Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
Acronym	ECHO
Number	830943
Type of instrument	Research and Innovation Action
Topic	SU-ICT-03-2018
Starting date	01/02/2019
Duration	48
Website	www.echonetwork.eu

D4.1 TRANSVERSAL TECHNICAL CYBERSECURITY CHALLENGES REPORT

Work package	WP4 Inter-sector Technology Roadmaps
Lead author	Notis Mengidis (CERTH)
Contributors	Andrea Guarino (ACEA), Andrew James Roberts (TUT), Antal Bódi (SU), Antonio Dan-Suteu (NDU), Boris Marinov (TBS), Bríd Davis (NUIM), Cagatay Yucel (BU), Christian Popov (TBS), Christina Todorova (ESI CEE), Csaba Krasznay (SU), Davide Ferrario (Z&P), Dragos Barbieru (NDU), Giuseppe Chechile (FNC), Gregory Depaix (NG), Harri Ruoslahti (LAU), Herman Fesenko (KhAI), Ioannis Chalkias (BU), Jan Derkacz (AGH), Julien Blin (NG), Jyri Rajamäki (LAU), Kornél Tóth (SU), Kristina Ignatova (BDI), Luis Galindo (TME), Marcin Niemiec (AGH), Marco Cammisa (EXP), Marco Dri (FNC), Maryna Kolisnyk (KhAI), Mascia Toussaint (ENQ), Monica Constantini (LCU), Notis Mengidis (CERTH), Oleg Illiashenko (KhAI), Pencho Vasilev (BDI), Petrisor Patrascu (NDU), PIoTr Bogacki (AGH), Ramón Cebrián (TME), Riccardo Feletto (FNC), Roberto Martínez (TME), Theodora Tsikrika (CERTH), Tiberiu Ion (NDU), Veselin Dobrev (BDI), Vyacheslav Kharchenko (KhAI),
Peer reviewers	Kristine Hovhannisyan (TUT), Nicola Zarra (VTCB), Kristiyan Popov (TBS), Boris Marinov (TBS)
Version	V1.0
Due date	30/04/2020
Submission date	18/06/2020

The work described in this document has been conducted within the ECHO project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830943

Dissemination level

x	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

Version history

Revision	Date	Editor	Comments
0.1	16/03/2020	Notis Mengidis (CERTH)	Table of Contents
0.2	20/3/2020	Notis Mengidis (CERTH)	Introduction
0.3	25/03/2020	Notis Mengidis (CERTH)	Section 3
0.4	05/04/2020	Notis Mengidis (CERTH)	Methodology
0.5	22/04/2020	Notis Mengidis (CERTH)	Integrated inputs from all contributors in Sections 4 and 5 – first version of the deliverable
0.6	02/05/2020	Notis Mengidis (CERTH)	Adjusted references
0.7	07/05/2020	Notis Mengidis (CERTH)	Internal QA Review
0.8	12/05/2020	Notis Mengidis (CERTH)	Executive summary
0.9	20/05/2020	Notis Mengidis (CERTH)	Added amended contributions to Sections 4 and 5
0.91	28/05/2020	Theodora Tsikrika (CERTH)	Updated content in Sections 1, 2 and 3
0.98	11/06/2020	Notis Mengidis (CERTH) & Theodora Tsikrika (CERTH)	Updated content in all sections. Fixed formatting issues.
0.99	17/06/2020	Tiago Nogueira (VisionSpace)	QA checks. Format corrections.
1.0	18/06/2020	Matteo Merialdo (RHEA)	Document closed

List of contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
1, 2, 3, 4, 4.4, 4.8, 5, 5.4, 6	Notis Mengidis (CERTH), Theodora Tsikrika (CERTH)
4.1, 4.3, 5.1, 5.1.2, 5.3, 5.7.7	Vyacheslav Kharchenko (KhAI), Oleg Illiashenko (KhAI), Maryna Kolisnyk (KhAI), Herman Fesenko (KhAI)
4.2, 4.10, 5.2, 5.9.5, 5.9.6	Giuseppe Chechile (FNC), Riccardo Feletto (FNC), Marco Dri (FNC)
4.5, 5.1.1.6, 5.5, 5.5.1, 5.7, 5.7.5, 5.7.6	Christian Popov (TBS), Boris Marinov (TBS)
4.6, 5.1.1, 5.4.7, 5.5.2, 5.5.3, 5.6, 5.7.2	Davide Ferrario (Z&P)
4.7, 5.1.1.1, 5.1.1.2, 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.8, 5.8.1, 5.8.2	Marcin Niemiec (AGH), Jan Derkacz (AGH), PIoTr Bogacki (AGH)
5.1.1.3, 5.1.1.4, 5.1.2.4, 5.1.2.6, 5.9.4	Harri Ruoslahti (LAU), Jyri Rajamäki (LAU)
5.1.1.5	Andrew James Roberts (TUT)
5.1.1.7	Andrea Guarino (ACEA)
5.1.2.1, 5.1.2.7, 5.4.5, 5.5.4	Veselin Dobrev (BDI), Pencho Vasilev (BDI), Kristina Ignatova (BDI)
5.1.2.2, 5.1.2.3	Mascia Toussaint (ENQ)

Section	Author(s)
5.1.2.5, 5.2.1, 5.2.2	Dragos Barbieru (NDU), Tiberiu Ion (NDU), Antonio Dan-Suteu (NDU), Petrisor Patrascu (NDU)
5.3.2, 5.3.3	Sorin Cernea (certSIGN)
5.3.4, 5.4.9, 5.9.1	Christina Todorova (ESI CEE)
5.3.1, 5.3.5, 5.3.6, 5.3.7, 5.9, 5.9.3	Julien Blin (NG), Gregory Depaix (NG)
5.4.6, 5.9.2	Antal Bódi (SU), Csaba Krasznay (SU), Kornél Tóth (SU)
5.1.2.8, 5.4.8	Cagatay Yucel (BU), Ioannis Chalkias (BU)
5.6.1, 5.6.2, 5.6.4	Marco Cammisa (EXP)
5.6.3, 5.7.4	Bríd Davis (NUIM)
5.7.1, 5.7.3	Luis Galindo (TME), Roberto Martínez (TME), Ramón Cebrián (TME)
5.7.8	Monica Constantini (LCU)

Keywords

CYBERSECURITY, TECHNICAL, RESEARCH DOMAINS, SECTORS, CHALLENGES, TRANSVERSAL

Disclaimer

Executive summary

The main objective of Work Package 4 (WP4) is the development of cybersecurity technology roadmaps as a result of analysis related to current and emerging cybersecurity challenges and associated technologies. These roadmaps will create the foundations for new industrial capabilities, and assist towards the development of innovative technologies that will aim to address these cybersecurity challenges. To this end, early prototypes research and development which will target specific, high-priority opportunities identified in these roadmaps will be performed.

To achieve these objectives, the roadmaps will be developed in accordance with the challenges identified in the analysis performed in T4.1 “Detailed analysis of transversal technical cybersecurity challenges” and its associated deliverables. This document is the first version of one of the two T4.1 deliverables that discusses and analyses a range of *transversal* technical cybersecurity challenges, i.e., technical cybersecurity challenges that are independent of sector or discipline; these challenges were identified through the following multistep process:

1. review and analysis of the latest cybersecurity reports from a variety of sources, including research articles and industry reports;
2. identification of threats and concerns based on the analysis of these reports which were subsequently converted into technical challenges (where appropriate); and
3. categorisation of these challenges based on already existing taxonomies, including the latest JRC taxonomy, which was published in 2019.

To avoid bias, the contributors of this deliverable were involved in all phases of the analysis, thus offering different perspectives on the most pressing technical challenges based on their experience and expertise. The variety of the sources that were analysed allowed for a comprehensive identification, since the reports that were gathered originated from organisations representing a wide variety of sectors and disciplines. The work presented in this deliverable also took into account the outcomes of WP2 “Multi-sector needs analysis” and specifically the threat and attack vectors described in deliverables D2.1 “Sector scenarios and use case analysis” and D2.4 “Inter-sector technology challenges and opportunities”.

Our analysis resulted in the identification of a total of 86 technical cybersecurity challenges: 57 transversal challenges (reviewed in this deliverable) and 29 inter-sector challenges (reviewed in the accompanying deliverable D4.2 “Inter-sector technical cybersecurity challenges report”). Each of the identified challenges is broadly presented across three dimensions: (i) the detailed description of each specific challenge, (ii) the mitigation techniques currently existing either as a commercially available product or as the state-of-the-art on a research level, and (iii) the opportunities that can be derived based on the availability of mitigation techniques and solutions. Based on these three pillars and also on the number of research and technological domains that each challenge covers, we performed an initial qualitative prioritisation in order to highlight the challenges with higher criticality that would need to be analysed by T4.2 “Inter-sector technology roadmap development”.

The current deliverable D4.1 “Transversal technical cybersecurity challenges report” will be updated on M45 to include the latest developments in the cyber threat landscape, enhance its study through questionnaires answered by cybersecurity practitioners and professionals, and also use the input of dedicated workshops specifically held for this purpose. Also, given the timeline of the second iteration of the technology roadmaps, the second version of D4.1 will shift its focus more on the emerging challenges, rather than the currently existing ones.

Table of contents

List of figures

List of tables

1. Introduction

1.1 Purpose and scope of the document

The vision of the European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO) is to provide an organised and coordinated view of the current cyber defence landscape of the European Union. One of the project's main enabling factors is the analysis of *technical cybersecurity challenges* and the subsequent development of technology roadmaps and early prototypes targeting high-priority opportunities identified as part of this analysis.

Cybersecurity is a highly multifaceted and often subjective discipline, and the absence of universally accepted definitions of used terms, along with the lack of a shared vision on what are the main challenges within the current landscape, make apparent the need for a more methodological approach to be considered for the identification and analysis of technical cybersecurity challenges. Therefore, in order to identify the most pressing technical issues that need to be addressed in the context of the activities of WP4 "Inter-sector Technology Roadmaps", a structured methodology was developed that enabled all consortium partners, with diverse expertise covering multiple domains, to provide their insights and shared vision.

In particular, Task 4.1 "Detailed analysis of transversal technical cybersecurity challenges" employed a technically focused approach for the identification, analysis, and categorisation of the most pressing current and emerging technical cybersecurity challenges with the goal to deliver two studies: one on *transversal challenges* (i.e., cybersecurity challenges that are independent of sector or discipline) and one on *inter-sector challenges* (i.e., cybersecurity challenges which are sector-related, but span across more than one sectors); the present deliverable D4.1 concerns the former, while the accompanying deliverable D4.2 concerns the latter. To perform this analysis, we reviewed and analysed in-depth the latest industrial reports and academic publications, covering multiple stakeholders' points of view, and highlighted challenges that span over different and multiple sectors. To classify these challenges, we examined some of the most widely accepted standards of taxonomies and then proposed one that better suited our needs, since it provides a more expressive and representative view of the task's given context based on appropriate research and technological domains.

Our analysis resulted in the identification of a total of 86 technical cybersecurity challenges: 57 transversal challenges (reviewed in this deliverable) and 29 inter-sector challenges (reviewed in the accompanying deliverable D4.2). Each of the identified challenges is broadly presented across three dimensions: (i) the detailed description of each specific challenge, (ii) the mitigation techniques currently existing either as a commercially available product or as the state-of-the-art at a research level, and (iii) the opportunities that can be derived based on the availability of mitigation techniques and solutions. Based on these three pillars and also on the number of research and technological domains that each challenge covers, the challenges with higher criticality that could be analysed by T4.2 "Inter-sector technology roadmap development" can be highlighted.

1.2 Structure of the document

This document describes first, in detailed steps, the process that was followed in order to collect reports, analyse them, and extract transversal technical cybersecurity challenges, as well as a detailed analysis of the identified challenges. The deliverable consists of the following sections:

- Section 2 presents the methodology that was used for the identification of the transversal technical challenges, including the taxonomy of cybersecurity research domains and technologies that was

employed for categorising the identified challenges. The same methodology and taxonomy were also used in D4.2.

- Section 3 provides an overview of the results of the analysis performed for the identification of transversal technical cybersecurity challenges.
- Section 4 describes the examined cybersecurity research domains and technologies, i.e., the categories of the taxonomy employed in this analysis.
- Section 5 analyses in depth the identified transversal technical cybersecurity challenges, i.e., technical challenges that affect all sectors, including the ECHO priority sectors of healthcare, transportation, energy, and defence.
- Section 6 discusses our conclusions and provides an outlook for the next steps.

1.3 Relation to other work in the project

This WP4 deliverable has been developed on the basis of WP2 “Multi-sector needs analysis” outcomes and will form a basis for further activities by other WP4 tasks and the ECHO project in general.

In particular, D4.1 used as input the outcomes of the following tasks and deliverables:

- T2.1 “Sector scenario use case analysis” and its associated deliverable D2.1 ”Sector scenarios and use case analysis” were used as an input in order to derive challenges from the developed cybersecurity sector scenarios, and also to identify threats based on known cyberattacks and cybersecurity threat trends.
- T2.4 “Technological challenges and opportunities” and its associated deliverable D2.4 “Inter-sector technology challenges and opportunities” were examined in order to identify the specifics of each sector and determine the cases where a technical-based approach was required.

The output of T4.1 will feed into the development of the inter-sector technology roadmaps conducted in T4.2 and also the subsequent early prototypes selection research and development in T4.3. Finally, it is worth noting that the methodology used in the current deliverable is applied also to D4.2.

1.4 Applicable and reference documents

The following documents contain requirements applicable to the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[GA]	Grant Agreement 830943 – ECHO	-	1.0	02/04/2019
[PH]	D1.1 Project Handbook	ECHO_D1.1_v1.41	1.41	02/05/2019
[PQP]	D1.3 Project Quality Plan	ECHO_D1.3_v1.1	1.1	31/05/2019

Table 1: Applicable documents

The following documents have been consulted for the generation of this document:

Reference	Document Title	Document Reference	Date
Abaimov & Bianchi, 2019	CODDLE: Code-Injection Detection With Deep Learning	Abaimov, S., & Bianchi, G. (2019). CODDLE: Code-Injection Detection With Deep Learning. IEEE Access, 7, 128617-128627.	2019
Acronis	How To Block Cryptomining Scripts	Acronis. How To Block Cryptomining Scripts In Your Web Browser. Retrieved 23 March 2020 from	n/a

Reference	Document Title	Document Reference	Date
	In Your Web Browser	https://www.acronis.com/en-eu/articles/how-to-block-cryptomining-scripts-in-your-browser/	
Agrawal, 2019	Cryptojacking: How Hackers Are Mining Cryptocurrencies Without Your Knowledge	Agrawal, H. (2019). Cryptojacking : How Hackers Are Mining Cryptocurrencies Without Your Knowledge. Retrieved 23 March 2020 from https://coinsutra.com/cryptojacking/	2019
Akamai, 2019	Web Attacks and Gaming Abuse	Akamai. (2019). Web Attacks and Gaming Abuse. Retrieved from https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-report-2019.pdf	2019
Alazab, Alazab, Shalaginov, Mesleh, & Awajan, 2020	Intelligent mobile malware detection using permission requests and API calls	Alazab, M., Alazab, M., Shalaginov, A., Mesleh, A., & Awajan, A. (2020). Intelligent mobile malware detection using permission requests and API calls. Future Generation Computer Systems, 107, 509-521.	2020
Alexandru, Morari, & Pappas, 2018	Cloud-based MPC with encrypted data	Alexandru, A. B., Morari, M., & Pappas, G. J. (2018). Cloud-based MPC with encrypted data. In 2018 IEEE Conference on Decision and Control (CDC) (pp. 5014-5019). IEEE.	2018
Alhindi, Traore, & Woungang, 2018	Data Loss Prevention using document semantic signature	Alhindi, H., Traore, I., & Woungang, I. (2018). Data Loss Prevention using document semantic signature. Proceedings of the International Conference on Wireless Intelligent and Distributed Environment for Communication.	2018
Allcott, and Gentzkow, 2017.	Social media and fake news in the 2016 election	Allcott, H. and Gentzkow, M., 2017. Social media and fake news in the 2016 election. Journal of economic perspectives, 31(2), pp.211-36.	2016
Al-rimy et al., 2018	Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions	Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.	2018
Australian Security Magazine, 2019	How to detect, mitigate and stop cryptomining malware	Australian Security Magazine. (2019). How to detect, mitigate and stop cryptomining malware. Retrieved 23 March 2020 from https://australiansecuritymagazine.com.au/how-to-detect-mitigate-and-stop-cryptomining-malware/	2019
Batchelder et al., 2014	Microsoft Security Intelligence Report	Batchelder, D., Blackbird, J., Felstead, D., Henry, P., Jones, J., Kulkarni, A., & Zink, T. (2014). Microsoft Security Intelligence Report. Microsoft Security Intelligence Report, 16, 1-19.	2014
Bauer, Dedhia, Skowyra, Streilein, & Okhravi, 2015	Multi-variant execution to protect unpatched software	Bauer, K., Dedhia, V., Skowyra, R., Streilein, W., & Okhravi, H. (2015). Multi-variant execution to protect unpatched software. Proceedings of the 2015 Resilience Week (RWS).	2015

Reference	Document Title	Document Reference	Date
Bay Area Rapid Transit, 2017	About BART	Bay Area Rapid Transit (2017). About BART. Retrieved 11 April 2020 from: https://www.bart.gov	2017
Bekara, 2014	Security issues and challenges for the IoT-based smart grid	Bekara, C. (2014). Security issues and challenges for the IoT-based smart grid. Proceedings of the FNC/MobiSPC	2014
Bertino & Ferrari, 2018	Big data security and privacy A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years	Bertino, E., & Ferrari, E. (2018). Big data security and privacy A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years (pp. 425-439): Springer	2018
Bhardwaj, 2017	Ransomware: A rising threat of new age digital extortion	Bhardwaj, A. (2017). Ransomware: A rising threat of new age digital extortion. In Online Banking Security Measures and Data Protection (pp. 189-221). IGI Global.	2017
Boeckl et al., 2019.	Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks	Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., . . . Scarfone, K. (2019). Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks: US Department of Commerce, National Institute of Standards and Technology.	2019
Brumley, Poosankam, Song, & Zheng, 2008	Automatic patch-based exploit generation is possible: Techniques and implications	Brumley, D., Poosankam, P., Song, D., & Zheng, J. (2008). Automatic patch-based exploit generation is possible: Techniques and implications. Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP 2008).	2008
Brundage et al., 2018	The malicious use of artificial intelligence: Forecasting, prevention, and mitigation	Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Anderson, H. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Retrieved 10 April 2020 from https://maliciousaireport.com/	2018
Buczak & Guven, 2015	A survey of data mining and machine learning methods for cyber security intrusion detection	Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.	2015
Chaabouni, Mosbah, Zemmari, Sauvignac, & Faruki, 2019	Network intrusion detection for IoT security based on learning techniques	Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications surveys & tutorials, 21(3), 2671-2701.	2019
Chen, Lai, Chang, & Lee, 2020	Detecting PE-Infection Based Malware	Chen, C.-M., Lai, G.-H., Chang, T.-C., & Lee, B. (2020). Detecting PE-Infection Based Malware. Proceedings of the Future of Information and Communication Conference.	2020
Chen, Wang, Wang, & Zhang, 2010	Side-channel leaks in web applications: A reality today, a challenge tomorrow	Chen, S., Wang, R., Wang, X., & Zhang, K. (2010). Side-channel leaks in web applications: A reality today, a challenge tomorrow. Proceedings of the 2010 IEEE Symposium on Security and Privacy.	2010

Reference	Document Title	Document Reference	Date
Chivers, 2019	What do we do about deepfake video?	Chivers, T., 2019. What do we do about deepfake video? The Guardian: The Observer - Artificial intelligence (AI) June 23 2019. Retrieved March 25, 2020 from: https://www.theguardian.com/technology/2019/jun/23/what-do-we-do-about-deepfake-video-ai-facebook	2019
Chung et al., 2019	Availability attacks on computing systems through alteration of environmental control: smart malware approach	Chung, K., Kalbarczyk, Z. T., & Iyer, R. K. (2019). Availability attacks on computing systems through alteration of environmental control: smart malware approach. In Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems (pp. 1-12).	2019
CISCO 2017 Midyear Cybersecurity Report, 2017	CISCO 2017 Midyear Cybersecurity Report	CISCO 2017 Midyear Cybersecurity Report (2017). Retrieved 11 April 2020, https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf	
CISCO 2018 Annual Cybersecurity Report, 2018	CISCO 2018 Annual Cybersecurity Report	CISCO 2018 Annual Cybersecurity Report (2018). Retrieved 11 April 2020 from https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf	
CISCO 2020 Benchmark Study, 2020	CISCO 2020 Benchmark Study	CISCO 2020 Benchmark Study (2020. Retrieved 11 April 2020 from https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html	
Constanze Dietrich, Krombholz, Borgolte, & Fiebig. 2018.	Investigating System Operators' Perspective on Security Misconfigurations	Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. 2018. Investigating System Operators' Perspective on Security Misconfigurations. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18). Association for Computing Machinery, New York, NY, USA, 1272–1289. DOI: https://doi.org/10.1145/3243734.3243794	2018
Conteh & Schmick, 2016	Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks	Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31.	2016
Corero 2019 Full Year DDoS Trends Report, 2019	Corero 2019 Full Year DDoS Trends Report	Corero 2019 Full Year DDoS Trends Report (2019). Retrieved 11 April 2020 from https://go.corero.com/corero-full-year-2019-ddos-trends-report-download?utm_campaign=TR-2020-03-02-2019-DDoS-Trends-Report&utm_source=pr	2019
Covington & Carskadden, 2013	Threat implications of the internet of things	Covington, M. J., & Carskadden, R. (2013). Threat implications of the internet of things. Proceedings of the 2013 5th International Conference on Cyber Conflict (CYCON 2013).	2013
Cser & Maxim, 2018	Top trends shaping IAM in 2018	Cser, A., Maxim, M.: Forrester - Top trends shaping IAM in 2018 (2018)	2018
D'Acquisto et al., 2015	Privacy by design in big data: an overview	D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y.-A., & Bourka, A. (2015). Privacy by	2015

Reference	Document Title	Document Reference	Date
	of privacy enhancing technologies in the era of big data analytics	design in big data: an overview of privacy enhancing technologies in the era of big data analytics. arXiv preprint arXiv:1512.06000.	
Darabian et al., 2020	Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis	Darabian, H., Homayounoot, S., Dehghantanha, A., Hashemi, S., Karimipour, H., Parizi, R. M., & Choo, K. K. R. (2020). Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis. Journal of Grid Computing, 1-11.	2020
Davie & Peterson, 2019	Computer networks	Davie, B. S., & Peterson, L. L. (2019). Computer networks: Morgan kaufmann.	2019
De Rango et al., 2020	Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks	De Rango, F., Potrino, G., Tropea, M., & Fazio, P. (2020). Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks. Pervasive and Mobile Computing, 61, 101105.	2020
Directive, 2008	identification and designation of European critical infrastructures and the assessment of the need to improve their protection	Directive, C. (2008). 114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union L, 345(75), 23.12.	2008
Directive, 1995	95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data	Directive, E. (1995). 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the EC, 23(6).	1995
Dodson, Souppaya & Scarfone, 2020	Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)	Dodson, D. F., Souppaya, M. P., & Scarfone, K. (2020). Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF).	2020
Dolhansky et al., 2019	The Deepfake Detection Challenge (DFDC) Preview Dataset	Dolhansky, B., Howes, R., Pflaum, B., Baram, N. and Ferrer, C.C., 2019. The Deepfake Detection Challenge (DFDC) Preview Dataset. arXiv preprint arXiv:1910.08854.	2019

Reference	Document Title	Document Reference	Date
Duchene, Rawat, Richier, & Groz, 2014	KameleonFuzz: evolutionary fuzzing for black-box XSS detection	Duchene, F., Rawat, S., Richier, J.-L., & Groz, R. (2014). KameleonFuzz: evolutionary fuzzing for black-box XSS detection. Proceedings of the Proceedings of the 4th ACM conference on Data and application security and privacy.	2014
ENISA, 2017	Cryptojacking – Cryptomining in the browser	ENISA. (2017). Cryptojacking – Cryptomining in the browser. Retrieved 23 March 2020 from https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser	2017
Farokhi, Shames, & Batterham, 2017	Secure and private control using semi-homomorphic encryption	Farokhi, F., Shames, I., & Batterham, N. (2017). Secure and private control using semi-homomorphic encryption. Control Engineering Practice, 67, 13-20.	2017
Floridi, 2018	Artificial intelligence, deepfakes and a future of ectypes.	Floridi, L., 2018. Artificial intelligence, deepfakes and a future of ectypes. Philosophy & Technology, 31(3), pp.317-321.	2018
Gallagher, 2016	Ransomware locks up San Francisco public transportation ticket machines: Some systems now restored; attacker demanded $73,000	Gallagher, S. (2016). Ransomware locks up San Francisco public transportation ticket machines: Some systems now restored; attacker demanded $73,000. Retrieved 11 April 2020 from: https://arstechnica.com/security/2016/11/san-francisco-muni-hit-by-black-fridayransomware-attack/	2016
Gordon, 2019	Better fact-checking for fake news	Gordon, R., 2019. Better fact-checking for fake news. MIT News October 17 2019. Retrieved March 26, 2020 from: http://news.mit.edu/2019/better-fact-checking-fake-news-1017	2019
Grill, Pevný, & Rehak, 2017	Reducing false positives of network anomaly detection by local adaptive multivariate smoothing	Grill, M., Pevný, T., & Rehak, M. (2017). Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. Journal of Computer and System Sciences, 83(1), 43-57.	2017
Gu et al., 2019	DIAVA: A Traffic-Based Framework for Detection of SQL Injection Attacks and Vulnerability Analysis of Leaked Data	Gu, H., Zhang, J., Liu, T., Hu, M., Zhou, J., Wei, T., & Chen, M. (2019). DIAVA: A Traffic-Based Framework for Detection of SQL Injection Attacks and Vulnerability Analysis of Leaked Data. IEEE Transactions on Reliability.	2019
Guilbeault and Woolley, 2016	How Twitter bots are shaping the election.	Guilbeault, D. and Woolley, S., 2016. How Twitter bots are shaping the election. The Atlantic, Retrieved March 23, 2020 from: https://www.theatlantic.com/technology/archive/2016/11/election-bots/506072/	2016
Gupta & Chaudhary, 2020	Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures	Gupta, B., & Chaudhary, P. (2020). Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures: CRC Press.	2020
Gupta, Govil, & Singh, 2014	Static analysis approaches to detect SQL injection and	Gupta, M. K., Govil, M., & Singh, G. (2014). Static analysis approaches to detect SQL injection and cross-site scripting vulnerabilities in web applications: A survey.	2014

Reference	Document Title	Document Reference	Date
	cross-site scripting vulnerabilities in web applications: A survey	Proceedings of the International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014).	
Gupta, Govil, Singh, & Sharma, 2015	Towards detection and mitigation of cross-site scripting vulnerabilities in web applications	Gupta, M. K., Govil, M. C., Singh, G., & Sharma, P. (2015). XSSDM: Towards detection and mitigation of cross-site scripting vulnerabilities in web applications. Proceedings of the 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI).	2015
Habibzadeh et al., 2019	A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities	Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society.	2019
High-Level Steering Committee, 2017	Quantum Technologies Flagship Intermediate Report	High-Level Steering Committee. (2017). Quantum Technologies Flagship Intermediate Report. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=42721	2017
Hirano & Kobayashi, 2019	Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained From Live-forensic Hypervisor	Hirano, M., & Kobayashi, R. (2019). Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained From Live-forensic Hypervisor. Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IoTSMS).	2019
Hitaj et al., 2019	Passgan: A deep learning approach for password guessing	Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2019). Passgan: A deep learning approach for password guessing. In International Conference on Applied Cryptography and Network Security (pp. 217-237). Springer, Cham.	2019
Holm, Karresand, Vidström, & Westring, 2015	A survey of industrial control system testbeds	Holm, H., Karresand, M., Vidström, A., & Westring, E. (2015). A survey of industrial control system testbeds. Proceedings of the Nordic Conference on Secure IT Systems.	2015
Humayed, Lin, Li, & Luo, 2017	Cyber-physical systems security—A survey	Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802-1831.	2017
IBM, 2013	Avoid the risks of cloud abuse. Reduce the risks of malicious cloud attacks perpetrated through social media avenues	IBM (2013), Avoid the risks of cloud abuse. Reduce the risks of malicious cloud attacks perpetrated through social media avenues. Retrieved from https://www.ibm.com/developerworks/cloud/library/cl-avoidriskscloudabuse/cl-avoidriskscloudabuse-pdf.pdf	2013
IEEE, 2017	IEEE Taxonomy	IEEE Taxonomy. Retrieved 20 March 2020 from https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/taxonomy_v101.pdf	2017

Reference	Document Title	Document Reference	Date
Internet Society, 2020	Enhancing IoT Security: Final Outcomes and Recommendations	Internet Society. (2020). Enhancing IoT Security: Final Outcomes and Recommendations Report | Internet Society. Retrieved 1 May 2020 from: https://www.internetsociety.org/wp-content/uploads/2019/05/Enhancing-IoT-Security-Report-2019_EN.pdf	2020
Jerkovic & Sinkovic, 2017	Vulnerability Analysis of most Popular Open Source Content Management Systems with Focus on WordPress and Proposed Integration of Artificial Intelligence Cyber Security Features	Jerkovic, H., & Sinkovic, B. (2017). Vulnerability Analysis of most Popular Open Source Content Management Systems with Focus on WordPress and Proposed Integration of Artificial Intelligence Cyber Security Features. International Journal of Economics and Management Systems, 2.	2017
Jiang, Gou, Shi, & Xiong, 2019	I Know What You Are Doing With Remote Desktop	Jiang, M., Gou, G., Shi, J., & Xiong, G. (2019). I Know What You Are Doing With Remote Desktop. Proceedings of the 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC).	2019
Kaloudi & Li, 2020	The AI-based cyber threat landscape: A survey	Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.	2020
Kirat et al., 2018	Deeplocker–Concealing Targeted Attacks with AI Locksmithing	Kirat, D., Jang, J., & Stoecklin, M. (2018). Deeplocker–Concealing Targeted Attacks with AI Locksmithing. Blackhat USA.	2018
Lazer et al., 2018	The science of fake news	Lazer, D.M., Baum, M.A., Benkler, Y., Berinsky, A.J., Greenhill, K.M., Menczer, F., Metzger, M.J., Nyhan, B., Pennycook, G., Rothschild, D. and Schudson, M., 2018. The science of fake news. Science, 359(6380), pp.1094-1096.	2019
Liu & Kuhn, 2010	Data loss prevention	Liu, S., & Kuhn, R. (2010). Data loss prevention. IT professional, 12(2), 10-13.	2010
Lomas, 2019	Fabula AI is using social spread to spot 'fake news'	Lomas, N., 2019. Fabula AI is using social spread to spot 'fake news', Techcrunch 6 February 2019. Retrieved March 27, 2020 from: https://techcrunch.com/2019/02/06/fabula-ai-is-using-social-spread-to-spot-fake-news/	2019
Maggi et al., 2017	Rogue robots: Testing the limits of an industrial robot's security	Maggi, F., Quarta, D., Pogliani, M., Polino, M., Zanchettin, A. M., & Zanero, S. (2017). Rogue robots: Testing the limits of an industrial robot's security. Trend Micro, Politecnico di Milano, Technical Report.	2017
Maras & Alexandrou, 2019	Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos	Maras, M.H. and Alexandrou, A., 2019. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. The International Journal of Evidence & Proof, 23(3), pp.255-262.	2019

Reference	Document Title	Document Reference	Date
McCallister, Grance, & Scarfone, 2010	Guide to protecting the confidentiality of personally identifiable information (PII)	McCallister, E., Grance, T., & Scarfone, K. A. (2010). Sp 800-122. Guide to protecting the confidentiality of personally identifiable information (PII).	2010
Microsoft, 2017	Cloud Services Due Diligence Checklist	Microsoft (2017), Cloud Services Due Diligence Checklist. Retrieved from https://www.microsoft.com/en-us/trust-center/compliance/due-diligence-checklist	2017
Mishra & Soni, 2019	A Content-Based Approach for detecting Smishing in Mobile Environment	Sandhya Mishra, Devpriya Soni (2019). A Content-Based Approach for detecting Smishing in Mobile Environment. Proceedings of International Conference on Sustainable Computing in Science, Technology & Management (SUSCOM-2019)	2019
Missaoui et al., 2018	Who is reusing stolen passwords? An empirical study on stolen passwords and countermeasures.	Missaoui, C., Bachouch, S., Abdelkader, I., & Trabelsi, S. (2018). Who is reusing stolen passwords? An empirical study on stolen passwords and countermeasures. In International Symposium on Cyberspace Safety and Security (pp. 3-17). Springer, Cham	2018
Nadeau, 2020	What is cryptojacking? How to prevent, detect, and recover from it	Nadeau, M. (2020). What is cryptojacking? How to prevent, detect, and recover from it. Retrieved 23 March 2020 from https://www.itworld.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html	2020
Nadji, Saxena, & Song, 2009	Document Structure Integrity: A Robust Basis for Cross-site Scripting Defense	Nadji, Y., Saxena, P., & Song, D. (2009). Document Structure Integrity: A Robust Basis for Cross-site Scripting Defense. Proceedings of the NDSS.	2009
Naffi, 2020	Deepfakes: Informed digital citizens are the best defence against online manipulation.	Naffi, N., 2020. Deepfakes: Informed digital citizens are the best defence against online manipulation. The Conservation January 8 2020. Retrieved March 25, 2020 from: https://theconversation.com/deepfakes-informed-digital-citizens-are-the-best-defence-against-online-manipulation-129164	2020
Nai-Fovino et al., 2018	A Proposal for a European Cybersecurity Taxonomy	Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G.-L., Figwer, M. & Lazari, A. 2019. A Proposal for a European Cybersecurity Taxonomy. EUR, 29868, 50.	2019
Narayanan, Toubiana, Barocas, Nissenbaum, & Boneh, 2012	A critical look at decentralised personal data architectures	Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H., & Boneh, D. (2012). A critical look at decentralised personal data architectures. arXiv preprint arXiv:1202.4503.	2012
NIST, 2019	CSRC Topics	Retrieved 20 March 2020 from https://csrc.nist.gov/topics	2019
Norton, 2018	What is cryptojacking? How it works and how to help prevent it	Norton. (2018). What is cryptojacking? How it works and how to help prevent it. Retrieved 23 March 2020 from https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html	2018

Reference	Document Title	Document Reference	Date
O'Dywer, G., 2016	Finnish Defense Ministry Hit by DDoS Cyber Attack	O'Dywer, G. (2016). Finnish Defense Ministry Hit by DDoS Cyber Attack. Defence News.	2016
Palo Alto, 2020	Unit 42 Cloud Threat Report: Spring 2020	Palo Alto. 2020. Unit 42 Cloud Threat Report: Spring 2020. Retrieved 10 April 2020 from https://unit42.paloaltonetworks.com/leaked-docker-code/	2020
Panja, Gennarelli, & Meharia, 2015	Handling cross site scripting attacks using cache check to reduce webpage rendering time with elimination of sanitisation and filtering in light weight mobile web browser	Panja, B., Gennarelli, T., & Meharia, P. (2015). Handling cross-site scripting attacks using cache check to reduce webpage rendering time with elimination of sanitisation and filtering in light weight mobile web browser. Proceedings of the 2015 First Conference on Mobile and Secure Services (MOBISECSERV).	2015
Perekalin, 2018	Why you should be careful with browser extensions	Perekalin, A. (2018). Why you should be careful with browser extensions. Retrieved 23 March 2020 from https://www.kaspersky.com/blog/browser-extensions-security/20886/	2018
Perrotta & Hao, 2018	Botnet in the browser: Understanding threats caused by malicious browser extensions	Perrotta, R., & Hao, F. (2018). Botnet in the browser: Understanding threats caused by malicious browser extensions. IEEE Security & Privacy, 16(4), 66-81.	2018
Ponemon Institute Research Report, 2018	Bridging the Digital Transformation Divide: Leaders Must Balance Risk& Growth	Ponemon Institute (2018). Bridging the Digital Transformation Divide: Leaders Must Balance Risk& Growth. Ponemon Institute Research Report	2018
Positive Technologies, 2019	Web application vulnerabilities: statistics for 2018	Positive Technologies (2019). Web application vulnerabilities: statistics for 2018. Retrieved 11 April 2020 from: https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019/	2019
Rajan, Ginkel, & Sundaresan, 2013	Expanded top ten big data security and privacy challenges	Rajan, S., Ginkel, W., & Sundaresan, N. (2013). Expanded top ten big data security and privacy challenges. Cloud Security Alliance, Apr.	2019
Ranjbar, Komu, Salmela, & Aura, 2016	An SDN-based approach to enhance the end-to-end security: SSL/TLS case study	Ranjbar, A., Komu, M., Salmela, P., & Aura, T. (2016). An SDN-based approach to enhance the end-to-end security: SSL/TLS case study. Proceedings of the NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium.	2016
Rathore, Sharma, & Park, 2017	XSSClassifier: An Efficient XSS Attack Detection Approach Based on Machine Learning Classifier on SNSs	Rathore, S., Sharma, P. K., & Park, J. H. (2017). XSSClassifier: An Efficient XSS Attack Detection Approach Based on Machine Learning Classifier on SNSs. JIPS, 13(4), 1014-1028.	2017

Reference	Document Title	Document Reference	Date
Richardson & North, 2017	Ransomware: Evolution, mitigation and prevention	Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10.	2017
Rubenfeld, 1989	The right of privacy	Rubenfeld, J. (1989). The right of privacy. Harvard Law Review, 737-807.	1989
Ruohonen, 2019	A Demand-Side Viewpoint to Software Vulnerabilities in WordPress Plugins	Ruohonen, J. (2019). A Demand-Side Viewpoint to Software Vulnerabilities in WordPress Plugins Proceedings of the Evaluation and Assessment on Software Engineering (pp. 222-228).	2019
Shahriar, Weldemariam, Zulkernine, & Lutellier, 2014	Effective detection of vulnerable and malicious browser extensions	Shahriar, H., Weldemariam, K., Zulkernine, M., & Lutellier, T. (2014). Effective detection of vulnerable and malicious browser extensions. Computers & Security, 47, 66-84.	2014
Sikos et al., 2019	Knowledge Representation of Network Semantics for Reasoning-Powered Cyber-Situational Awareness AI in Cybersecurity	Sikos, L. F., Philp, D., Howard, C., Voigt, S., Stumptner, M., & Mayer, W. (2019). Knowledge Representation of Network Semantics for Reasoning-Powered Cyber-Situational Awareness AI in Cybersecurity (pp. 19-45): Springer.	2019
Ştefăniţă, Corbu, & Buturoui, 2018	Fake news and the third-person effect: They are more influenced than me and you	Ştefăniţă, O., Corbu, N. and Buturoui, R., 2018. Fake news and the third-person effect: They are more influenced than me and you. Journal of Media Research, 11(3), pp.5-23.	2018
Stillwagon, 2018	Malicious browser extensions: What you should know	Stillwagon, A. (2018). Malicious browser extensions: What you should know. Retrieved 23 March 2020 from https://medium.com/redmorph/malicious-browser-extensions-what-you-should-know-cb7ecb477dbc	2018
Stouffer, Falco, & Scarfone, 2011	Guide to industrial control systems (ICS) security	Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST special publication, 800(82), 16-16.	2011
Sudhodanan et al., 2017	Large-scale analysis & detection of authentication cross-site request forgeries	Sudhodanan, A., Carbone, R., Compagna, L., Dolgin, N., Armando, A., & Morelli, U. (2017). Large-scale analysis & detection of authentication cross-site request forgeries. Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P).	2017
Thomas, Vijayaraghavan & Emmanuel, 2020	Adversarial Machine Learning in Cybersecurity	Thomas, T., Vijayaraghavan, A. P., & Emmanuel, S. (2020). Adversarial Machine Learning in Cybersecurity. In Machine Learning Approaches in Cyber Security Analytics (pp. 185-200). Springer, Singapore.	2020
Trend Micro, 2019	Root Account Misconfiguration Potentially Exposes 19% of the Top,	Trend Micro. 2019. Root Account Misconfiguration Potentially Exposes 19% of the Top, 1000 containers in docker hub. Retrieved 10 April 2020 from: https://www.trendmicro.com/vinfo/us/security/news/cyberc	2019

Reference	Document Title	Document Reference	Date
	1000 containers in docker hub	rime-and-digital-threats/root-account-misconfiguration-potentially-exposes-19-of-the-top-1-000-containers-in-docker-hub	
Trieu & Yang, 2018	Artificial intelligence-based password brute force attacks.	Trieu, K. & Yang, Y. (2018). Artificial intelligence-based password brute force attacks. In Proceedings of the 13thAnnual Conference of the Midwest AIS (MWAIS'18).	2018
Tzur-David, 2019	How Chrome extensions are making organisations vulnerable to attack	Tzur-David, S. (2019). How Chrome extensions are making organisations vulnerable to attack. Retrieved 23 March 2020 from https://www.information-age.com/chrome-extensions-123478016/	2019
University of Waterloo, 2019	New tool uses AI to flag fake news for media fact-checkers	University of Waterloo, 2019. New tool uses AI to flag fake news for media fact-checkers. ScienceDaily December 16 2019. Retrieved March 27, 2020 from www.sciencedaily.com/releases/2019/12/191216122422.htm	2019
Van Steen and Tanenbaum, 2017	Distributed systems	Van Steen, M., & Tanenbaum, A. S. (2017). Distributed systems. Maarten van Steen Leiden, The Netherlands.	2017
Vetterl & Clayton, 2019	Honware: A virtual honeypot framework for capturing CPE and IoT zero days	Vetterl, A., & Clayton, R. (2019). Honware: A virtual honeypot framework for capturing CPE and IoT zero days. Proceedings of the Symposium on Electronic Crime Research (eCrime). IEEE.	2019
W3Techs, 2020	Usage Statistics and Market Share of Content Management Systems	W3Techs. (2020). Usage Statistics and Market Share of Content Management Systems, June 2020. Retrieved 20 May 2020 from: https://w3techs.com/technologies/overview/content_management	2020
Westerlund, 2019	The Emergence of Deepfake Technology: A Review	Westerlund, M., 2019. The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review, 9(11).	2019
Woolley, 2020	We're fighting fake news AI bots by using more AI - That's a mistake	Woolley, S., 2020. We're fighting fake news AI bots by using more AI. That's a mistake. From: The Reality Game: How the Next Wave of Technology Will Break the Truth via the MIT Technology Review, 8th Jan 2020, Retrieved March 25, 2020 from: https://www.technologyreview.com/s/614810/were-fighting-fake-news-ai-bots-by-using-more-ai-thats-a-mistake/	2020
WP Whitesecurity, 2019	More Than 70% of WordPress Installations Vulnerable	WP Whitesecurity. (2019). More Than 70% of WordPress Installations Vulnerable | WP White Security. Retrieved 20 May 2020 from: https://www.wpwhitesecurity.com/statistics-70-percent-wordpress-installations-vulnerable/	2019
Wu et al., 2019	Misinformation in social media: Definition, manipulation, and detection	Wu, L., Morstatter, F., Carley, K. M., & Liu, H. (2019). Misinformation in social media: Definition, manipulation, and detection. ACM SIGKDD Explorations Newsletter, 21(2), 80-90.	2019

Reference	Document Title	Document Reference	Date
Xie & Aiken, 2006	Static Detection of Security Vulnerabilities in Scripting Languages	Xie, Y., & Aiken, A. (2006). Static Detection of Security Vulnerabilities in Scripting Languages. Proceedings of the USENIX Security Symposium.	2006
Yu, Sekar, Seshan, Agarwal, & Xu, 2015	Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things	Yu, T., Sekar, V., Seshan, S., Agarwal, Y., & Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. Proceedings of the 14th ACM Workshop on Hot Topics in Networks.	2015
Zhu, 2014	Resilient control and intrusion detection for scada systems	Zhu, B. X. (2014). Resilient control and intrusion detection for scada systems. California Univ. Berkeley. Dept Of Electrical Engineering and Computer Sciences. Technical Report No. UCB/EECS-2014-34.	2014
Zvelo, 2018	Cryptojacking Infection Methods: Identification and Prevention Tips	Zvelo. (2018). Cryptojacking Infection Methods: Identification and Prevention Tips. Retrieved 23 March 2020 from https://zvelo.com/cryptojacking-infection-methods-identification-prevention-tips/	2018

Table 2: Reference documents

1.5 Intellectual Property Rights

Based on the legal framework provided in the ECHO Grant Agreement and the Consortium Agreement, ECHO specific IPR procedures have been established to protect the innovations and knowledge developed within this deliverable.

1.6 Glossary of acronyms

Acronym	Description
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure
API	Application Programming Interfaces
AWS	Amazon Web Services
C2	Command and Control
CDN	Content Delivery Network
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
COMINT	Communication Intelligence
CPS	Cyber-Physical Systems
CSRF	Cross-Site Request Forgery
CyPR	Cybersecurity Professional Register
DDNS	Decentralised DNS
DDoS	Distributed Denial of Service
DGA	Domain Generation Algorithm
DKIM	Domain Keys Identified Mail
DLL	Dynamic Link Library
DLP	Data Loss Prevention

Acronym	Description
DLT	Distributed Ledger Technology
DMARC	Domain-based Message Authentication, Reporting & Conformance
DNS	Domain Name System
DoS	Denial of Service
ECDIS	Electronic Chart Display and Information System
E-MAF	ECHO Multi-sector Assessment Framework
FSP	Full-Scale Pilot
FTP	File Transfer Protocol
GA	Grant Agreement
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDaaS	Identity Access Management-as-a-Service
IDM	Identity Access Management
IDS	Intrusion Detection System
IMINT	Imagery Intelligence
IOC	Indicators of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention System
JOP	Jump-Oriented Programming
LAN	Local Area Network
MAC	Mandatory Access Control
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MNO	Mobile Network Operator
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
MSC	Maritime Safety Committee
MSP	Managed Service Provider
MSS	Managed Security Service
MT	Moving Target
NIDS	Network-based Intrusion Detection Systems
OSINT	Open-Source Intelligence
P2P	Peer-to-Peer
PaaS	Platform as a Service
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standards
PEB	Process Environment Block
PII	Personally Identifiable information
PKI	Public Key Infrastructure
RaaS	Ransomware as a Service
RBAC	Role-Based Access Control
ROI	Return of Investment

Acronym	Description
ROP	Return-Oriented programming
RDP	Remote Desktop Protocol
RSA	Rivest–Shamir–Adleman
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SDLC	Software development life cycle
SEB	Stakeholders Expert Board
SecaaS	Security-as-a-Service
SIEM	Security Information and Event Management
SIGINT	Signals Intelligence
SME	Small- and Medium-sized Enterprises
SMS	Short Message Service
SOA	Service Oriented Architectures
SOC	Security Operation Centres
SSL	Secure Sockets Layer
SSO	Single Sign On
TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top-Level Domain
TLS	Transport Layer Security
URL	Uniform Resource Locator
VAD	Virtual Address Description
VM	Virtual Machine
VoIP	Voice over IP
VPN	Virtual Private Network
WPA2	Wi-Fi Protected Access 2
WP	Work Package
WPA2	Wi-Fi Protected Access 2
XSS	Cross Site Scripting

Table 3: Glossary of acronyms, initialisms and abbreviations

2. Technical challenges identification methodology

An analysis of technical cybersecurity challenges requires a clear definition of what constitutes such a technical challenge. Since there does not exist, to the best of our knowledge, a universally accepted definition of a (technical) challenge in the literature, we adopted the following working definition by leveraging the well-defined notion of (cyber) threat:

a technical challenge refers to a threat or a set of threats that is difficult to mitigate/overcome using the technical means available in state-of-the-art research technologies or currently available industry solutions (products).

In particular, the following definitions of (cyber) threat are considered, listed in increasing order of specificity:

- **ISO 27000:2018**: Potential cause of an unwanted incident, which may result in harm to a system or organisation,
- **ENISA Glossary**: Any circumstance or event with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data, and/or denial of service.
- **NISTIR 7298 Rev. 3**: Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or the Nation through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.

Underpinned by the aforementioned definitions, the analysis performed both in this report (D4.1) and in the accompanying deliverable (D4.2) was organised in the following six phases (also illustrated in Figure 1): (i) Preparation, (ii) Report collection, (iii) Report analysis, (iv) Challenge identification, (v) Challenge categorisation, and (vi) Challenge analysis.

Figure 1: The six phases of the analysis

In the **Preparation** phase, the task leader proposed an initial approach/methodology based on the Description of Action and on the discussions that took place during WP4 kick-off meeting; this initial methodology was later refined based on the feedback received from all partners involved in T4.1. This refined methodology was subsequently presented during the WP4 progress meetings and it was finalised following several rounds of discussions with all involved partners, resulting in the five phases outlined below.

In the **Report collection** phase, all involved partners were requested to collect the latest relevant cybersecurity reports and also state-of-the-art scientific and academic surveys that could be used as a source for the identification of current and emerging technical cybersecurity challenges. This phase served as a step towards

having a better understanding of the cybersecurity landscape in various sectors, as well as creating a reference point of the current state of the art in the academic and industrial domains.

In the **Report analysis** phase, each partner was assigned a set of specific reports for analysis. During this assignment, the language of the report was taken into consideration (since not all of them were in English), along with the domain expertise of each partner. The main idea was to identify, in each report, *cybersecurity threats* that could potentially lead to the identification of *technical cybersecurity challenges*. Given the above definitions, the analysis of each such threat thus also required a state-of-the-art analysis regarding the currently available solutions either in the research domain or in industry-grade "off-the-shelf" products.

In the **Challenge identification** phase, the previous analyses were merged into a single matrix and were examined for duplicate reported threats. Each threat was examined separately in terms of mitigation techniques and impact, and was mapped to a specific challenge.

In the **Challenge categorisation** phase, the challenges were categorised into two broad categories, transversal and inter-sector, with the former being discussed in this deliverable (D4.1) and the latter in the accompanying deliverable (D4.2). A more fine-grained categorisation was performed afterwards in order to facilitate the multifaceted nature of cybersecurity and cover as many research and technology domains as possible. This was achieved by mapping the challenges to a taxonomy that combines two dimensions of the latest Joint Research Centre (JRC) taxonomy (Nai-Fovino et al., 2019).

In the final **Challenge analysis** phase, each challenge was analysed in depth through extensive literature review, partner's experience, and a more comprehensive report study. Also, a qualitative assessment was performed in order to highlight high priority areas that need to be addressed in T4.2 and T4.3.

Next, each of the latter five stages is described in more detail.

2.1 Report collection

The reports that were collected can be broadly classified in the following categories:

- Academic/Scientific papers
- EU Agencies reports
- Industry reports
- Law Enforcement Agencies reports
- National Organisations reports
- Other H2020 projects.

This phase resulted in the collection of a total of 123 reports which are distributed across the aforementioned six categories as shown in Figure 2. Half of the collected reports are Industry reports, followed by academic/scientific papers at 28%, reports by National Organisations at 11%, while the rest are below 5%.

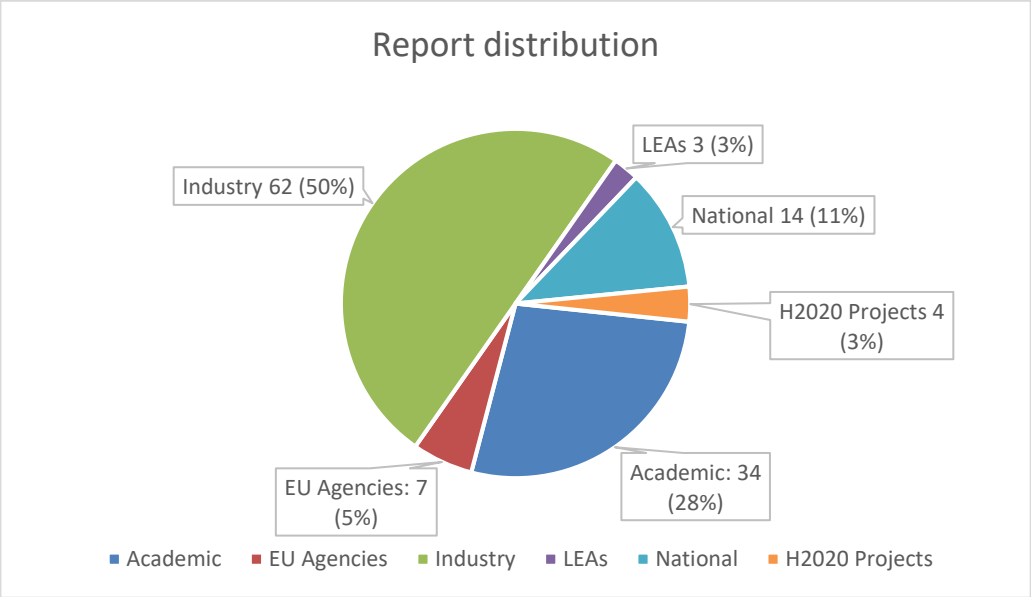

Figure 2: Distribution of the 123 collected reports

These reports were uploaded to the ECHO repository and were inventoried for easier and faster access using the information presented in Table 4; the full inventory of analysed reports can be found in Annex 1 – List of analysed reports.

Report information
Report title
Published by
Publication date
Country
Type of organisation
Abstract of the report
Keywords
Source

Table 4: Report inventory template

2.2 Report analysis

In this phase, the involved partners analysed the reports that were gathered during the collection phase. Each partner was assigned a predefined set of reports, selected by the task leader on the basis of each partner's expertise and also of the language of the report (since 13 were non-English reports).

For the purpose of this analysis and in order to achieve a more consistent outcome, a comprehensive matrix was created and was circulated to the involved partners, along with the list of each partner's assigned reports. The fields of this matrix are illustrated in Table 5 and aimed to describe and characterise the identified threat, including an initial categorisation into transversal and inter-sector, with the former being discussed in this deliverable (D4.1) and the latter in the accompanying deliverable (D4.2).

Report information	
Threat ID	
Name of the report	
Link to the analysed source	
Is the report relevant / In scope	Y/N
Threat specific information	
Identified threats (One per row)	
Threat description	
Sectors affected by the threat	Energy
	Healthcare
	Transportation
	Defence
	Other (Specify)
Type of threat	Transversal
	Inter-sector
Detailed description of the threat	
Impact	Short term (<2 years)
	Medium term (2-5 years)
	Long term (>5 years)

Table 5: Threat identification template

Out of the 123 reports that were considered during this phase, a total of 18 reports were deemed out of scope and were not analysed any further. In addition, the ECHO deliverables D2.1 and D2.4 were also analysed from a technical perspective in order to identify threats that could possibly lead to the identification of challenges relevant to the scope of WP4. This analysis resulted in the identification of **267 cyber threats**.

2.3 Challenge identification

Following the threat identification performed in the previous phase, the 267 threats were merged into a single matrix and were examined for duplicate reported threats; this resulted in a total of **189 threats**. Each contributing partner was then requested to perform a state-of-the-art analysis for each threat and examine whether the specific threat can be considered to constitute a challenge, given the adopted definition.

At this point, the analysed sources were not limited just to the collected reports, but also additional online sources could be used as well as academic and scientific surveys. Furthermore, at this point, 11 additional reports collected in the context of T9.4 “Innovation Management” which aim at offering a more long-term view of the cybersecurity landscape by covering a timeline 25-50 years from now, were also examined.

To enable the identification of challenges, the threat identification matrix (see Table 5) was expanded by adding the columns depicted in Table 6. This phase results in the identification of a total of **83 technical cybersecurity challenges: 57 transversal** and **26 inter-sector challenges**.

Challenge specific information
Detailed description of the challenge
Research/Innovation mitigation solutions
Industry mitigation solutions
References

Table 6: Additions to the threat identification template for supporting the identification of challenges

2.4 Challenge categorisation and analysis

A fine-grained categorisation of the identified challenges is beneficial towards achieving a better understanding and gaining insights into the current cybersecurity landscape; to this end, taxonomies are typically employed. A taxonomy serves two main purposes, one is to provide clear definitions in the cybersecurity domain thus overcoming language barriers, and the other one is to empower us with the capability of identifying and analysing challenges in grades of different granularity. A taxonomy that is better tailored to our needs, provides a structure that improves information sharing, risk assessment, challenge categorisation and high-level decision-making.

2.4.1 Examined taxonomies

There are several attempts and proposals for a universally accepted comprehensive taxonomy, however each one of them has its own goals and purposes. The taxonomies that we examined for the purpose of this document are the following:

1. National Institute of Standards and Technology (NIST) Computer Security Resource Centre (CSRC) taxonomy (NIST, 2019)
2. Institute of Electrical and Electronics Engineers (IEEE) taxonomy (IEEE, 2017)
3. Association for Computing Machinery (ACM) classification system (ACM, 2012)
4. JRC Taxonomy (Nai-Fovino et al., 2019).

All of these taxonomies use their own hierarchical structure, each with its own strengths and weaknesses, but some of them offer a very limited scope in terms of cybersecurity classification.

The NIST CSRC taxonomy, even though it is very precise and covers most of the traditional cybersecurity dimensions like cryptography, data security and identity management, it does not capture some of the categories of challenges that were identified by the consortium partners; examples of such categories include IoT, SCADA, and vehicular systems.

The IEEE taxonomy, on the other hand, is mainly focused on a more academically-oriented cybersecurity classification and lacks coverage of technical domains like data privacy, cloud computing, edge computing, and critical infrastructures.

The ACM classification system is also oriented towards scientific publications, hence severely lacks the operational aspect of cybersecurity. Furthermore, it was last updated in 2012 and, as such, emerging categories like artificial intelligence, IoT, and quantum technologies are missing.

Finally, the JRC taxonomy aims to offer more holistic view of the cybersecurity domain and is thus organised along the following three dimensions (illustrated also in Figure 3):

i. **Sectors** such as energy, healthcare, or transport, each with its own requirements and challenges.
ii. **Research domains** representing areas of knowledge related to technological, but also to human, legal, and ethical cybersecurity aspects.

iii. **Technologies and Use Cases** covering technological aspects, with particular focus on the so-called "technological enablers" that could be employed to enhance the development of different sectors.

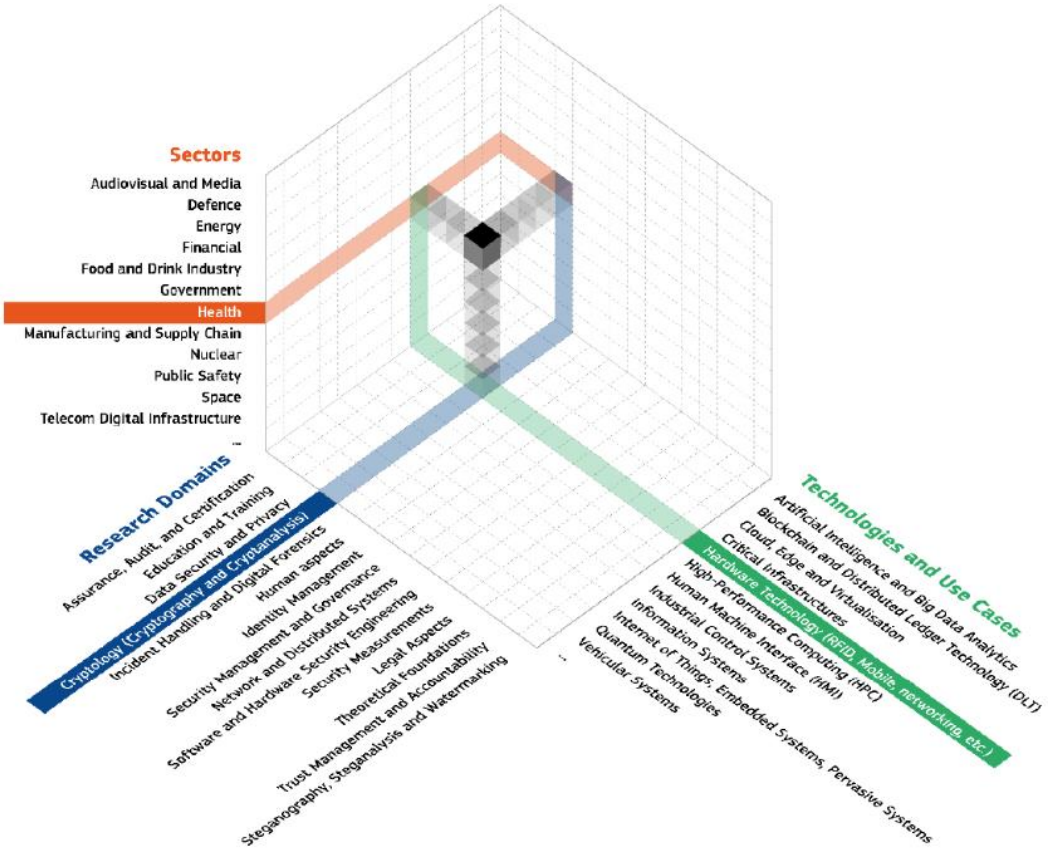

Figure 3: Three-dimensional JRC taxonomy (source: Nai-Fovino et al., 2019).

2.4.2 Technical cybersecurity challenges categorisation

Our study of the existing taxonomies concluded that the holistic taxonomy proposed by JRC was the most appropriate and precise to be used as a basis for our analysis. In particular, we focused on the two out of three dimensions of the JRC taxonomy, namely "Research domains" and "Technologies and Use Cases", by removing though categories that were either not relevant to our scope or were examined previously in WP2, i.e., the *Human Aspects*, *Legal Aspects*, and *Education and Training* categories which were examined in T2.3.

Moreover, we merged these two dimensions into a single list, since the categorisation of technical cybersecurity challenges requires a more holistic view of the affected research and technology domains, rather than their split into technological aspects and their enablers. This resulted in 24 categories listed in **Error! Reference source not found.**; this list is by no means exhaustive and future additions of new challenges will probably require the list to be revisited as T4.1, and the ECHO project in general, progresses.

Relevant categories extracted from the JRC taxonomy	
Assurance, Audit and Certification	AI and Big Data Analytics
Data Security and Privacy	Blockchain and Distributed Ledger Technology
Cryptology	Cloud, Edge and Virtualisation
Incident Handling and Digital Forensics	Critical Infrastructures
Identity Management	Hardware Technology (RFID, Mobile, networking etc.)
Security Management and Governance	High-Performance Computing (HPC)
Network and Distributed Systems	Human Machine Interface (HMI)
Software and Hardware Security Engineering	Industrial Control Systems
Security Measurements	Information Systems
Theoretical Foundations	IoT, Embedded Systems, Pervasive Systems
Trust Management and Accountability	Quantum Technologies
Steganography, Steganalysis and Watermarking	Vehicular Systems

Table 7: Initial taxonomy for technical cybersecurity challenges categorisation

Following this initial categorisation, it became apparent that the categories initially considered required a further refinement, because many challenges fell into multiple categories, thus a more coarse-grained approach was required and moreover many of these categories were either not relevant or contained a small number of threats.

Therefore, a further refinement was performed resulting in the following 10 newly created domains:

- Software and Hardware Security Engineering
- Critical Infrastructures
- IoT, Embedded Systems, Pervasive Systems
- Network and Distributed Systems
- Cloud, Edge and Virtualisation
- AI And Big Data Analytics
- Quantum Technologies
- Data Security and Privacy
- Incident Handling and Digital Forensics
- Vehicular Systems

which are aligned to the selected JRC categories as illustrated in Table 8, In some cases, a many-to-many relationship exists between some of the selected JRC categories and newly created domains; for example, it was deemed appropriate that “Theoretical Foundations” are relevant to a multitude of the considered domains.

These 10 newly created domains formed the basis of the analysis performed in the rest of this deliverable and also in the accompanying deliverable (D4.2)

	Assurance, Audit and Certification	Data Security and Privacy	Cryptology	Incident Handling and Digital	Identity Management	Security Management and	Network and Distributed Systems	Software and Hardware Security	Security Measurements	Theoretical Foundations	Trust Management and Accountability	Steganography, Steganalysis and	AI and Big Data Analytics	Blockchain and Distributed Ledger	Cloud, Edge and Virtualisation	Critical Infrastructures	Hardware Technology (RFID,	High-Performance Computing (HPC)	Human Machine Interface (HMI)	Industrial Control Systems	Information Systems	IoT, Embedded Systems, Pervasive	Quantum Technologies	Vehicular Systems
Software and Hardware Security Engineering								X		X							X	X			X			
Critical Infrastructures																X				X				
IoT, Embedded Systems, Pervasive Systems										X										X		X		
Network and Distributed Systems							X		X	X				X							X			
Cloud, Edge and Virtualisation															X									
AI and Big Data Analytics										X			X											
Quantum Technologies			X							X		X											X	
Data Security and Privacy	X	X			X	X			X	X	X													
Incident Handling and Digital Forensics				X															X					
Vehicular Systems																								X

Table 8: Categories mapped to the JRC aligned classification

2.5 Qualitative prioritisation

The prioritisation of the challenges aims to identify which challenges are more critical than others and thus motivate further analysis in the context of the technology roadmaps developed in T4.2 and the prototypes developed in T4.3.

To this end, we performed a qualitative prioritisation by calculating the number of domains affected by each of the 83 identified challenges. Even though this kind of assessment does not take into account quantitative parameters necessary for proper risk assessment, it can however highlight challenges that affect multiple research domains and technologies. In the next stages of the project, WP4 will be adopting the ECHO Multi-sector Assessment Framework (E-MAF) developed in WP2 as a framework basis and standardised methodology for the assessment and scoring of the identified challenges.

Next, an overview of the analysis performed using the methodology described in this section is provided.

3. Overview of the analysis of the transversal challenges

The analysis based on the methodology described in the previous section resulted in the identification of a total of 83 technical cybersecurity challenges: 57 transversal and 26 inter-sector; the rest of this deliverable focuses on the former, while the inter-sector challenges are analysed in the accompanying deliverable (D4.2).

The 57 transversal technical cybersecurity challenges that were identified are listed below and are also depicted in Figure 6. Once these challenges were identified, they were first categorised on the basis of the initial taxonomy consisting of the 24 categories derived from the JRC "Research domains" and "Technologies and Use Cases", and then on the basis of the final taxonomy consisting of the 10 categories proposed in this work. It should be noted that each challenge can be classified into more than one category, i.e., a multi-label classification is supported, with a single category though being considered as the "primary category" associated with each challenge.

Figure 4 and Figure 5 present the distribution of challenges per domain with respect to the 24 categories and the 10 newly created categories, respectively, on the basis of *all* the research and technological domains reflected in these categories that are affected by the threat(s) constituting the specific challenge. In both cases, the "Data Security and Privacy", "Network and Distributed Systems" and "Software and Hardware Security Engineering" are the categories with the most challenges associated with them. This is expected as these are among the core cybersecurity research and technological domains reflected in the 24 categories; in addition, they also encompass several categories in the final taxonomy based on the 10 categories and therefore they are more likely to further increase the number of challenges associated with them.

Overall, the following transversal technical challenges were identified and are listed with respect to their primary category. As a result, the category "Vehicular Systems" is not listed below as none of the identified transversal challenges considers this as their primary category.

- Software and Hardware Security Engineering
  - Application Security
    - Out-of-date security standards and protocols
    - Out-of-date and unpatched Windows systems
    - Attacks on RDP services and Remote Command Execution
    - DLL Injections
    - System misconfigurations
    - Mobile malware
    - Ransomware
  - Web Applications
    - Malicious Browser Extensions
    - CMS Hacking
    - Cross-site scripting / XSS Injection
    - Cross-Site Request Forgery (CSRF)
    - SQL Injection
    - JavaScript Injection
    - Cryptojacking scripts and extensions
    - Fileless and memory-resident malware
- Critical Infrastructures
  - Lack of cyber situational awareness in national critical infrastructure and gaps in defence-in-depth architecture hacking
  - Illicit access to critical infrastructures using IoT flaws and hacking
- IoT, Embedded systems, Pervasive systems
  - Access to IoT devices

    - IoT botnets
    - Traditional host-centric security solutions are inadequate at protecting IoT devices
    - Constantly increasing attack surface
    - Anomalous behaviour is hard to detect
    - Cross device dependencies
    - 0-day on CPS
- Network and distributed systems
    - Anomalous events of unknown origin in complex systems
    - Negative effects of complexity and connectivity
    - Obfuscation as IDS evasion technique
    - Encryption as IDS evasion technique
    - Man-in-the-middle attacks
    - Denial of Service attacks
    - Encrypted Malicious Web Traffic
    - Decentralised DNS
    - False positives in the detection of anomalies, attacks, and intrusion attempts
- Cloud, Edge, and Virtualisation
    - Abuse of Cloud Services
    - Vulnerabilities in cloud infrastructure
    - Content Delivery Network (CDN) manipulation
    - Data confidentiality and privacy in cloud environment
- AI and Big Data Analytics
    - Adversarial Machine Learning
    - Malicious use of AI
    - Disinformation, Fake News, and Deepfakes
    - Big data security
- Data security and privacy
    - Breaches and data leaks
    - Brute-force attacks
    - Credential theft
    - Unauthorised access
    - Smishing (SMS Phishing)
    - Vishing (Voice Phishing or VoIP Phishing)
    - Data loss
    - Data tampering
- Quantum technologies
    - Conditional security of asymmetric cryptography and fast development of quantum computers (Shor's algorithm)
    - Encryption based on symmetric ciphers with currently using keys can be broken by quantum computer (Grover's algorithm)
- Incident Handling and Digital Forensics
    - Attribution of cyberattacks
    - Lack of proper raw data collection
    - Lack of dedicated tools to manage cyber threats
    - Malware Anti-Analysis Techniques
    - Sandbox evasion techniques
    - Lack of adequate cyber risk mitigation frameworks

Figure 6 shows the number of categories associated with each of the identified challenges and thus can be considered to offer an indication of most critical among these, such as the “data confidentiality and privacy in

cloud environments" which reflect the current pressing concerns of users and developers alike, and the "out-of-date security standards and protocols" which is a long-standing issue in the cybersecurity community.

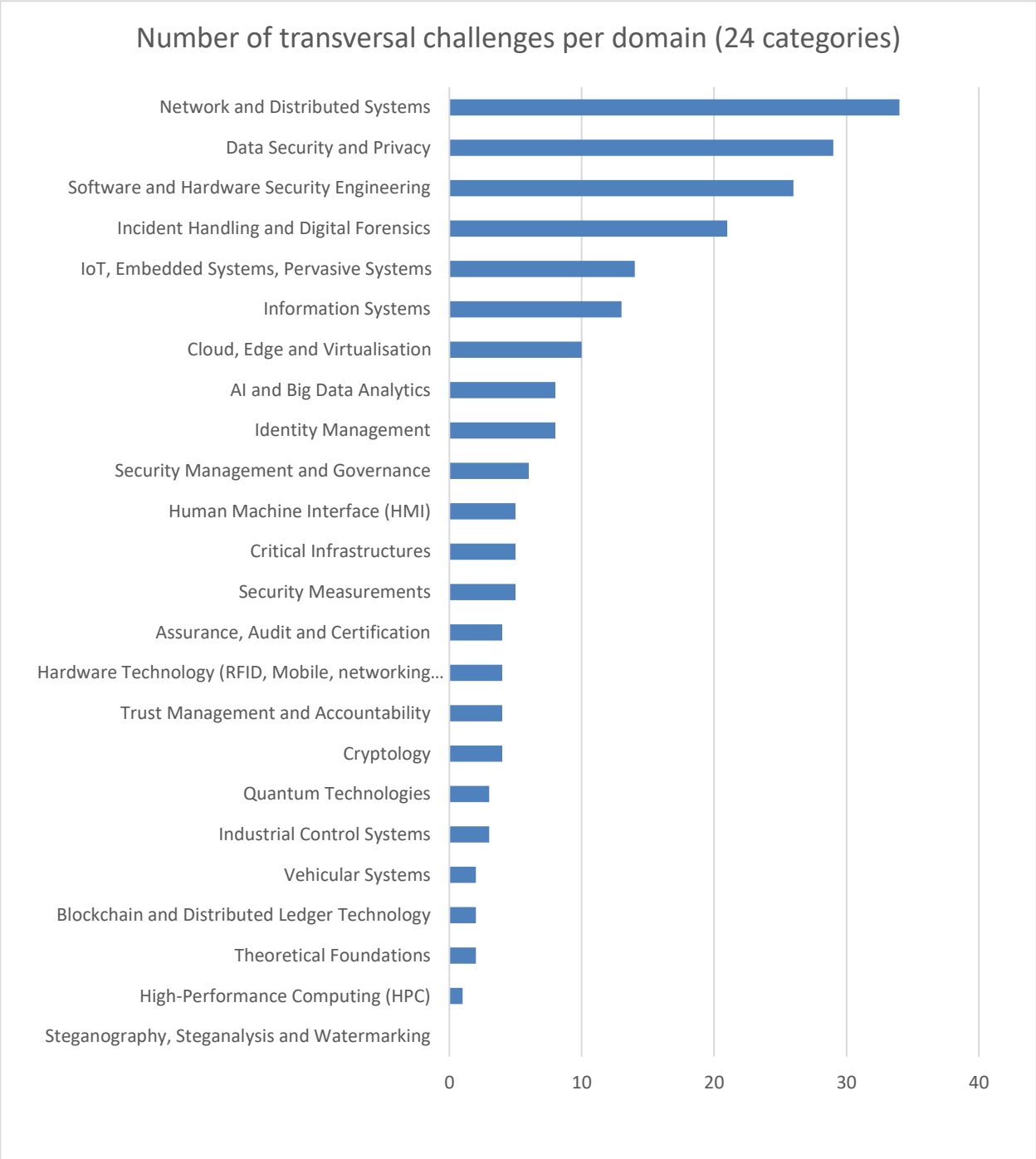

Figure 4: Numbers of identified challenges per domain based on the initial categorisation

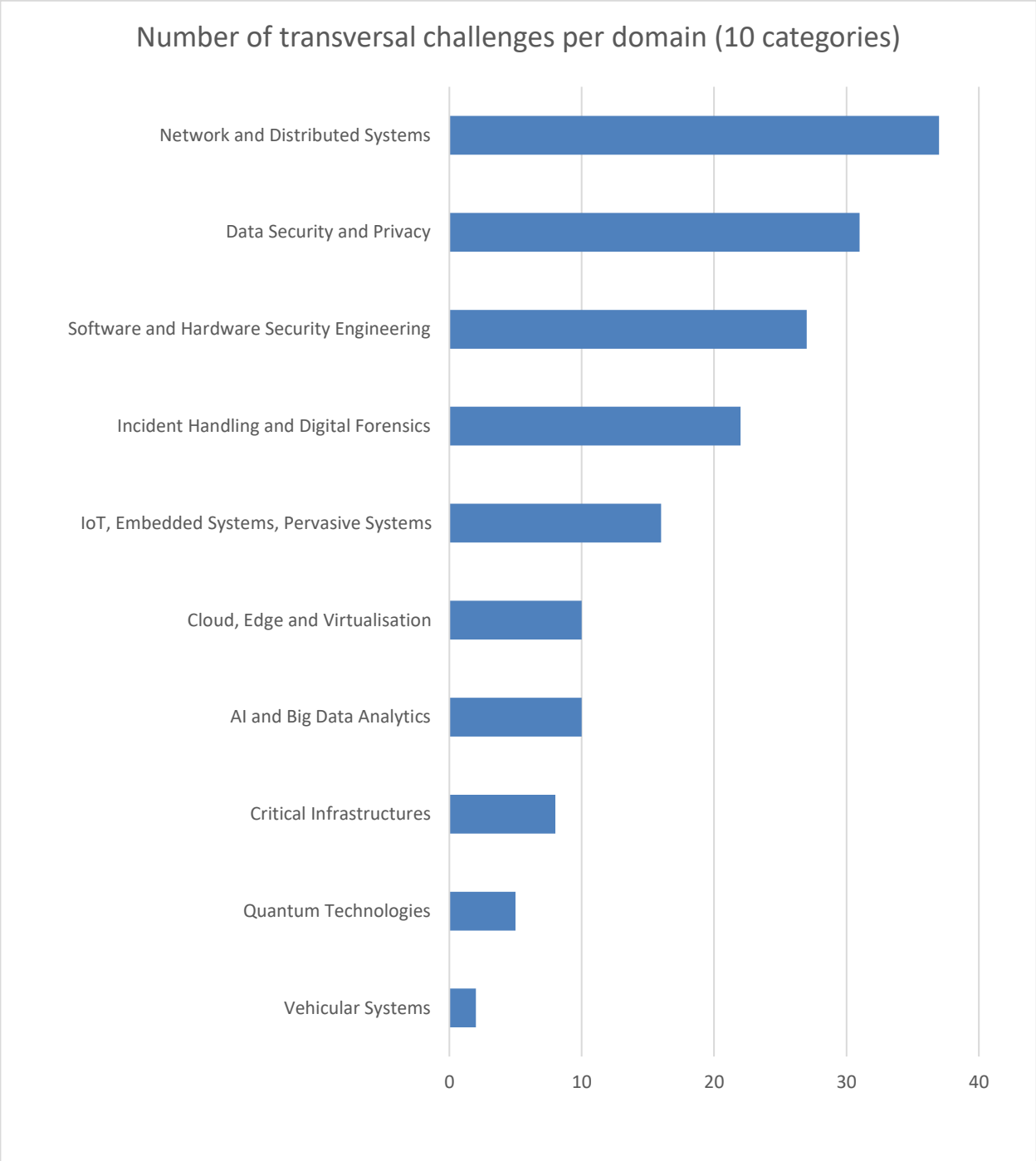

Figure 5: Numbers of identified challenges per domain based on the final categorisation

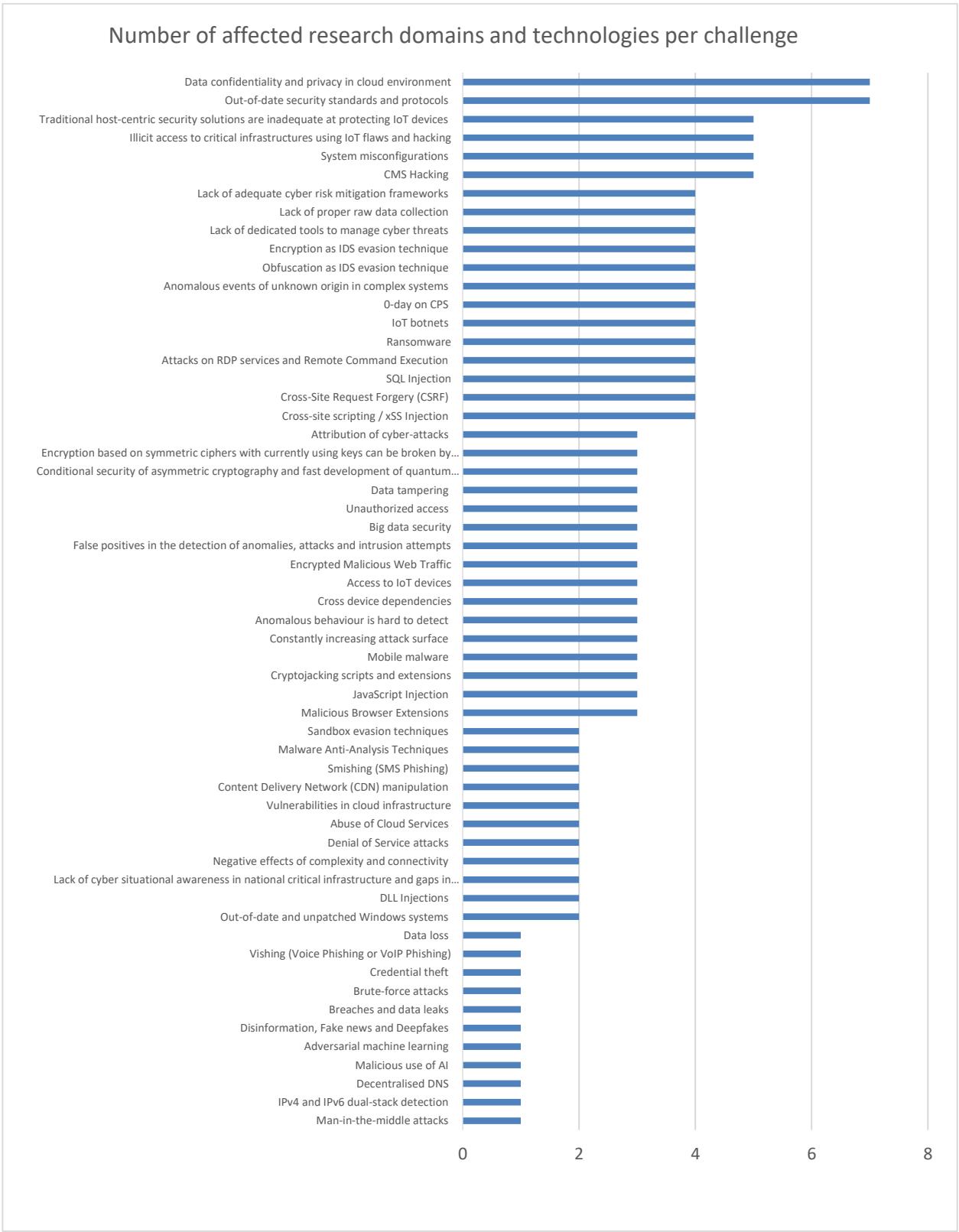

Figure 6: Number of affected research domains and technologies per challenge

Next, a description of each of the considered domains is provided (Section 4), followed by a detailed discussion on the identified transversal technical cybersecurity challenges as these are categorised to the domain that they primarily affect (Section 5).

4. Examined cybersecurity research domains and technologies

This section describes the scope of the cybersecurity research domains and technologies that were selected as the basis of the categorisation of the identified transversal technical cybersecurity challenges.

4.1 Software and hardware security engineering

The software development life cycle (SDLC) is a formal or informal methodology for designing, creating, and maintaining software (which includes code embedded in the hardware); there are many models for SDLC, including waterfall, spiral, agile development, and development and operation (DevOps). Regardless of which SDLC model is used for software development, methods for secure software development should be integrated in order to reduce the number of vulnerabilities in released software, to mitigate the potential impact of using undetected or unresolved vulnerabilities, and to eliminate root causes of vulnerabilities to prevent future recurrences. Most security aspects can be addressed in several places in the SDLC, but the sooner the protection is considered in the SDLC, the less effort and cost will ultimately be required to achieve the same level of security. This principle, also known as left shift, is critical regardless of the SDLC model.

Secure software development methods are well documented (Dodson, Souppaya, & Scarfone, 2020) and are based on principles and best practices on Secure Software Development Fundamentals (SSDFs):

- Prepare the organisation: make sure that the organisation's employees, processes, and technologies are ready for the secure development of software.
- Software protection:
    - Protect all software components from unauthorized access.
    - Produce well-protected software has minimal vulnerabilities in its releases.
    - Respond to vulnerabilities by identifying vulnerabilities in software releases and reacting accordingly in order to eliminate these vulnerabilities and also prevent other vulnerabilities from occurring in the future.

Hardware security refers to all actions necessary to identify equipment vulnerabilities, analyse their consequences, prevent their use by reducing, decreasing and (ideally) zeroing the risks caused by their presence, develop and implement appropriate remedies, and possibly avoid such risks by appropriate patches.

Hardware security — for both attack and defence — is different from software, network, and data security due to the nature of the equipment. Design and manufacture of equipment occur before or during software development, and as a result, the security of equipment should be considered in the early stages of the product life cycle. The hardware interacts with the software that controls a cyber-physical system, so the hardware is the last line of defence before the damage is done; if an attacker compromises the hardware, software protection mechanisms may be useless. Even if a piece of equipment has lost its usefulness, it is necessary to properly dispose of it or it may risk attacks as theft of data or software that is still on the hardware.

There are two aspects to hardware security: security in the processor supply chain, and also hardware mechanisms that provide software with a secure runtime. If the vulnerabilities are in the hardware and that the hardware attacks try to expose vulnerabilities through them to violate the security of the system, it does not necessarily mean that the means of protection against them must be implemented at the hardware level given that vulnerabilities are discovered when the equipment operates in the field, without the possibility of correction, as this can mainly be done for software. Therefore, any technique aimed at countering hardware attacks falls within the definition of hardware security, even if risk reduction measures are applied at the upper levels. Overall, hardware security refers to all solutions aimed at using equipment to protect the system from attacks that exploit vulnerabilities present also in other components of the system.

An attacker with access to the production process may make some changes to the final product. A hardware trojan is characterised by a payload, i.e., all the activity that the trojan performs when it is activated, and a trigger, which is a condition checked in the state of the circuit that activates the payload. In general, malicious trojans try to bypass or disable the system's security fence; they can leak confidential information from radio emission or other side channel signal. A trojan can also be used to disable, disrupt, or destroy the entire chip or its components and can be introduced at any stage of production (design, manufacturing, testing, assembly) and at any level (register transfer level, gate level, transistor level, and even physical level).

Among the common hardware security primitives, physical unclonable functions (PUFs) and true random number generators (TRNGs), as well as countermeasures, including anti-counterfeiting (DfAC) design, provide protection against various potential threats and vulnerabilities that arise at different stages of the life cycle and operation of the device. Some separation and degradation mechanisms can be effectively used to ensure hardware security.

4.2 Critical infrastructures

Critical infrastructures refer to the body of systems, networks, and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety. For various (political, economic, and technological) reasons, such infrastructures are becoming increasingly complex and interdependent, and although the evolution of such systems improves the quality of life and of the services that they deliver, it also introduces new vulnerabilities and risks that can be destructive for a nation and its people.

Although such infrastructures are similar across all nations due to the basic requirements of life, the infrastructures deemed critical can vary according to a nation's needs, resources, and development level. In Europe the following sectors are considered as critical: transport, energy, water, food, health, finance, information and communications technology, chemical industries, nuclear industries, and space.

In addition, the European Union also tried to define what a critical infrastructure is for a state member of the Union. With the *Council Directive 2008/114/EC* on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, the European Commission gave the following definition of critical infrastructure for Europe:

"'*European critical infrastructure' or 'ECI' means critical infra-structure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure.*"

In particular, the directive is based on the following key concepts:

- **Determination of ECI:** The directive defines a step-by-step process to identify a European Critical Infrastructure (ECI). It addresses single-sector and inter-sector criteria to select an infrastructure as critical for the European community. The final decision though belongs to the member state that holds the infrastructure.
- **Risk evaluation:** Every member state has to put in place specific procedures and processes to evaluate risks and threats about ECI located in their own territory.
- **Operator security plans:** Every owner or operator of ECI has to put in place a procedure to address the following points:
    - identification of important assets;
    - conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; and

- identification, selection and prioritisation of countermeasures and procedures; this kind of control can be split in two categories:
    - Permanent security measures, which identify indispensable security investments and means which are relevant to be employed at all times. This heading will include information concerning general measures, such as technical measures (including installation of detection, access control, protection and prevention means); organisational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.
    - Graduated security measures, which can be activated according to varying risk and threat levels.
- Every owner or operator of ECI has to nominate an officer to work as a point of contact between ECI and the competent national organisation for the protection of Critical Infrastructures.

The European directive for ECI also tries to address one of the major issues with modern critical infrastructure, i.e, despite that the security handling of such systems is provided by the nation that own them, a destructive incident that impacts such an infrastructure could become a problem also for other countries that use or buy that service.

4.3 IoT, embedded systems, pervasive systems

IoT devices generally face the same types of cybersecurity and privacy risks as conventional IT devices, though the prevalence and severity of such risks often differ. For example, data security risks are almost always a significant concern for conventional IT devices, but for some IoT devices, such data security risks may not exist because they do not have any data that needs protection (Boeckl et al., 2019).

Certain aspects of IoT security are so well-established that they were asserted as baseline actions that must be taken to enhance IoT security. Including but not limited to, some of these prerequisites are the following (Internet Society, 2020):

- No universal or easily guessed pre-set passwords.
- Data should be transmitted and stored securely using strong encryption.
- Data collection should be minimised to only what is necessary for a device to function.
- Devices should be capable of receiving security updates and patches.
- Device manufacturers should notify consumers if there is a security breach.
- Device manufacturers should ensure consumers are able to reset a device to factory settings in the event of a sale or transfer of the device

The IoT ecosystem is governed by the same system security principles as any other conventional IT system. However, the interoperability of IoT devices and the fact that their state and composition are hardly visible in a network, create some additional challenges such as the following:

- Protecting personally identifiable information (PII) at the network layer.
- Managing and updating IoT devices throughout their lifecycle.
- Managing and monitoring a large number of IoT devices is a hard task from an administrative perspective.
- Creating a common cybersecurity framework for all devices is difficult due to the lack of standardisation and the large number of IoT vendors.

In order to mitigate some of the risks associated with the heterogeneous nature of IoT devices, it is necessary to implement and maintain an accurate inventory throughout a device's lifecycle, which means that asset management is crucial. Furthermore, it is important to be able to update the software and firmware in order to reduce the likelihood of exploitation by known vulnerabilities. Prevention of unauthorised physical and logical

access is also vital, as well as monitoring and analysing IoT device activity in order to detect security incidents in a timely manner. Finally, decisions regarding the processing and interaction with PII should be based on informed decision-making that will enable individuals to understand the different aspects of privacy risks involved in having their data processed and collected by an IoT device.

Additionally, the inventorying of an IoT device can be a tedious task for an organisation's asset management system either because the device does not have a unique identifier that makes it easily distinguishable, or because the device cannot join a centralised asset management system (Boeckl et al., 2019). This creates an opportunity for employing physical unclonable functions (PUF) in order to generate identifiers uniquely created by specific physical attributes of a device. Additionally, a collaboration between the organisation and the manufacturer is highly encouraged in order to reach a mutual agreement on the provision of patches and upgrades throughout an IoT device life span. Finally, recent developments in intrusion detection systems create the opportunity for IoT devices to implement their own IDS, taking off course into full consideration the limitations imposed by the limited resources of these devices (Chaabouni, Mosbah, Zemmari, Sauvignac, & Faruki, 2019).

4.4 Network and distributed systems

In their simplest form, we can consider that the network consists of the following two building blocks: *nodes* and *links*. Nodes is a generic term that is used to describe a device connected to a network such as a general-purpose computer, a switch that routes network packages, or any other specific-purpose device, like a smart home appliance or a medical implant device which offers connection capabilities. Although it is outside the scope of this deliverable, it is useful to know a little bit about the inner architecture of each node and in particular, the fact that the resources of each node are finite, with memory and bandwidth being the most important ones; memory usually serves as a buffer for packets that are queued waiting to be transmitted, while on the other hand, bandwidth is essential for the timely transmission of the packets. Network links come in a variety of forms, including twisted pair, optical fibre but also space which is used to wirelessly connect nodes. Regardless of the type of the physical medium used, the main purpose of the link is as simple as the propagation of a signal.

In order to turn nodes and links into a network, a network adapter has to do the following:

Encode the data: The network adapter contains a signalling component that encodes data into signals at the transmitting part while it decodes signals the receiving end. Figure 7 illustrates the communication between two signalling components and their corresponding network adapters, while Figure 8 shows the most commonly used encoding schemes.

Frame the data: Modern computer networks use packet switching instead of bit streaming utilising blocks of data which are called frames. In simple terms, data transmission is a sequence of frames being sent by one network adapter to the other. Recognising the correct sequence in which the frames arrive and should be decoded is one of the main challenges that the network adapter has to deal with. In order to alleviate the framing problem, the following approaches are used: Byte-Oriented Protocols, Bit-Oriented Protocols, and Clock-Based Framing.

Detect and correct errors: Due to interference and noise, transmission errors are often introduced into frames. In order to address this problem, a lot of different techniques have been proposed and used, with the older one being Hamming code. Regarding error correction there are two approaches, the one is to ask the sender to transmit the corrupted frame again, and the other is to try and the reconstruct the methods using error correcting algorithms. The most commonly used error detection and correction codes are the following: Cyclic Redundancy Check (CRC), Internet Checksum Algorithm, and Two-Dimensional Parity.

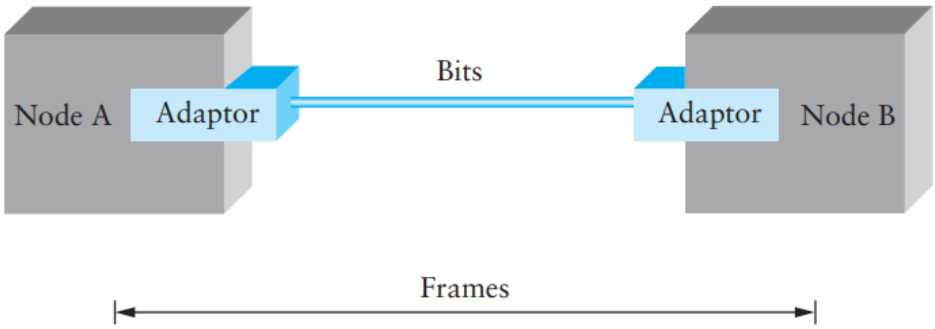

Figure 7: Signal flow between two network nodes (Davie & Peterson, 2019)

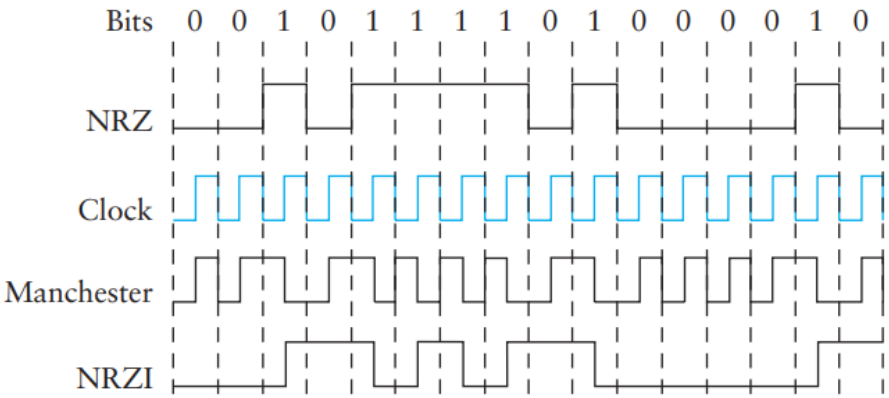

Figure 8: Most commonly used encoding schemes. (Davie & Peterson, 2019)

Distributed systems are generally regarded as complex pieces of software where the components are dispersed across multiple machines. The provision of a middleware layer is what makes distributed systems possible and its main purpose is to separate applications from the underlying platforms. The most important architectural styles for distributed systems are the following (Van Steen & Tanenbaum, 2017): (i) Layered architectures, (ii) Object-based architectures, (iii) Resource-centred architectures, and (iv) Event-based architectures.

When considering the cybersecurity aspects of a distributed system, regardless of the underlying architectural style, there are a number of design issues that need to be taken into consideration. The first one is the focus of control which as the name suggests, aims at the direct protection of the data associated with the application hence ensuring data integrity. The second design aspect that should be considered is how to layer the security mechanisms. The security mechanisms should be placed depending on the level of trust that a client has and also depending on the security level of a particular layer. Finally, another design issue related to distributed systems is simplicity. Even though simple security mechanisms are in some cases inefficient in applying strict security policies, in other cases introducing complex security protocol to an already complex system makes things worse. Furthermore, ensuring that the system has no security holes through an audit process is much easier in a simple and easy to understand security mechanism.

4.5 Cloud, edge, and virtualisation

New applications, services, and workloads increasingly demand a different kind of architecture, one that is built to directly support a distributed infrastructure. New requirements for availability and cloud capability at remote sites are needed to support both today's requirements (e.g., retail data analytics, network services, etc.) and also tomorrow's innovations (e.g., smart cities, AR/VR, etc.). The maturity, robustness, flexibility, and simplicity of cloud would thus need to be extended across multiple sites and networks in order to cope with evolving demands.

Recently companies have begun to apply the simplified administration and flexibility of cloud computing architectures to distributed infrastructures that span across multiple sites and networks. Organisations have an emerging need to take cloud capabilities across WAN networks and into increasingly smaller deployments out at the network edge. Though this approach is in its early days, it is becoming clear that many emerging use cases and scenarios would benefit from distributed architectures.

4.6 AI and Big Data analytics

Artificial Intelligence (AI), and in particular Deep Learning (DL) and Machine Learning (ML), are among the most active fields of research today, following concurrent advances in computer power and the ability to treat large amounts of data. As such, AI techniques have been successfully applied on the one hand to tackle many cybersecurity problems, while on the other hand they have been leveraged towards implementing stronger and hard-to-detect cyberattacks. Moreover, concerns have been raised over the security and stability of the AI algorithms used in cybersecurity applications.

Moreover, traditionally, cybersecurity has been struggling with the volume of data to be analysed, the high rate at which new threats emerge, the difficulties to predict the characteristics of the new threats, and the cost of prevention and mitigation actions. AI techniques offer several advantages when applied to cybersecurity: AI techniques scale well and can be applied to different domains; subtle changes in attack patterns can be dynamically discovered; it is possible to learn behaviour patterns from historical data and develop classifiers able to distinguish normal activity from anomalous one, thus detecting zero-day attacks; by balancing precision and recall it is possible to fine tune AI algorithms to reduce false alarms or increase the sensitivity of algorithms; and also Advanced Persistent Threat (ATPs) can be better observed in real-time and longer term.

4.6.1 Application of AI in cybersecurity

AI in cybersecurity can be used in malware detection, where the traditional blacklist-based methods are not able to detect new malware and/or lack exhaustivity.

Intrusion detection aims at monitoring network traffic and detecting any intrusions or misuse. Cybersecurity methods can be signature-based, anomaly-based, or hybrid, and usually analyse vast datasets of Packet-Level data and NetFlow Data. Artificial Neural Networks, Bayesian Networks, Decision Trees, Support Vector Machines, Hidden Markov Models (and many others) are AI techniques commonly used in this context. ML techniques have also been applied to filter phishing email, but their effectiveness has been questioned.

Advanced Persistent Threat is a category of sophisticated techniques that aim to obtain data without authorisation through attack cycles comprising target definition, accomplices research and management, tools building, deployment, initial intrusion, outbound connection, access expansion and credential theft, foothold strengthening, data exfiltration and tracks covering. Mitigation strategies presented in the literature are constructing ATP traffic patterns processing TCP/IP session information and building classification models.

AI has also been used in biometrical recognition, both for recognition-authentication processing and also towards securing platforms for biometrics applications. Other security domains in which AI solutions can be applied are cloud security, smart cities and cross domain information exchange.

4.6.2 Reliability and security of AI systems

The ubiquitous application of ML and AI tools makes very important to understand their vulnerabilities and how to mitigate them. For example, datasets can be “poisoned” by an adversary during the training phase in order to lower the accuracy of the algorithms, evasion or impersonating attacks may be performed during the testing phase inserting adversarial samples, thus deviating original samples from the distribution of training data, while machine learning outputs can be collected and reverse engineered to steal valuable information. Mitigation strategies range from data sanitisation (e.g., spam filters), to adversaries retraining, output smoothness, differential privacy and homomorphic encryption (thus allowing to perform operations directly on encrypted data).

4.6.3 Big Data security

Efficient processing of huge databases/logs for intrusion detection is a challenge. Such processing is important because of detection of anomalies and malware to prevent attacks which are not easy or even possible based on selected logs from one network device/system, given that sometimes only correlations across logs allow us to predict/detect network attacks or malware campaigns. Efficient processing of big data security can also help to identify security threats and vulnerabilities in protected systems/applications.

4.7 Quantum technologies

Quantum technologies are recognised as those technologies that rely on the principles of quantum physics, a special branch of physics which describes the behaviour of matter and energy at the atomic and subatomic levels.

Nowadays, some features of quantum mechanics are being used to design new methods of improving the cybersecurity and performance of modern communication networks. Quantum theory models have been successfully applied in many different contexts. Thanks to the unprecedented accuracy of modern techniques, we are able to manipulate quantum systems in micro scale which leads us to a variety of new technologies and solutions that have the potential to replace existing applications, thus quantum technology has the potential to change our society significantly.

Quantum technology uses the phenomena of quantum physics to make completely new effects possible. One of them is entanglement – a superposition that extends between two or more particles. Usually, the quantum state of a single particle is independent of others. However, we can produce pairs of particles which interact in a very interesting way: if we measure the state of one particle, then the state of the second particle can be fully determined. This means that we only need to measure one particle to know the states of both. Additionally, the states of the particles are completely random before measurement occurs. Another interesting effect is superposition. Quantum state can be represented as a sum of two or more other distinct states. However, when a measurement is made, the particle is forced into one of the possible alternatives; chance determines which one. For example, a unit of quantum information (qubit or quantum bit) can have two possible values (normally 0 or 1), however, it can also be a superposition of both. There is also one negative effect – decoherence. Quantum states of superposition are very sensitive to disturbances. This process is one of the greatest challenges to be faced in quantum technology.

The report of the High-Level Steering Committee (High-Level Steering Committee, 2017) indicates four main domains of quantum technologies: communication, computation, simulation, sensing and metrology (Figure 9). The development of these domains can produce transformative applications and has a real practical impact on ordinary people. Simulation can help to understand and solve a wide range of problems, such as chemical processes, the development of new materials, or fundamental physical theories. By sensing and metrology, we can achieve unprecedented sensitivity, accuracy, and resolution in measurement and diagnostics. However, the two remaining domains are the ones that directly influence cybersecurity: quantum communication and quantum computation.

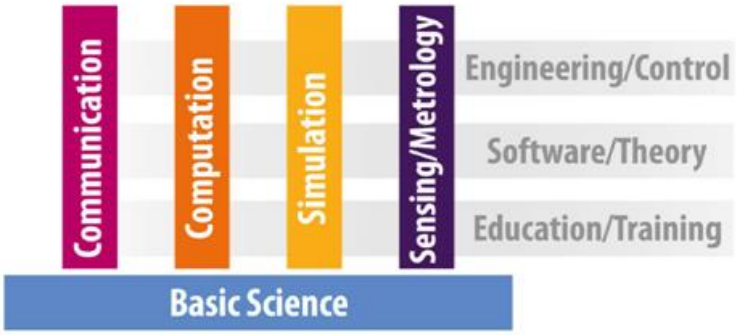

Figure 9: Vertical domains of quantum technologies and three considered aspects of them

The idea of *quantum communication* can guarantee secure data transmission in public networks. Also, it should be able to develop long-term security for end-users by using communication protocols. The most well-known example of quantum communications methods is quantum key distribution, a solution that ensures a very high level of data security. The security is ensured because it is not possible to eavesdrop the communication between two users in a passive way. If an eavesdropper tries to read the exchanged data (distributed key), he/she will change the quantum states of the photons and will thus be revealed. This kind of protection is possible because in the quantum world, measurements influence the quantum state. Additionally, it is not possible to clone an unknown quantum state and thus obtain the quantum state from a copied quantum particle. Popular quantum key distribution protocols, such as BB84 (proposed by Charles Bennett and Gilles Brassard in 1984), are based on the polarisation of single photons, which carry information from a sender to a receiver. This information is coded using quantum states, i.e., different polarisations: vertical, horizontal, diagonal. In this way, the recipient (and also potential eavesdropper) does not know which detector should be used to measure the polarisation to obtain precise value of quantum bit.

However, this is not a problem for the intended recipient; when the right user announces the configuration of the detectors which are used during the measurement of a received photon, the sender confirms that the obtained result is correct (then such a bit can be a part of final key) or asks for this bit to be deleted from the final key because the obtained result is not certain. However, if the eavesdropper chooses the wrong detector, then the polarisation of the photon changes and the quantum bit can be received incorrectly. The sender and recipient uncover the eavesdropper if they compare a part of exchanged bits (established key). Thanks to this mechanism, passive eavesdropping is not possible in quantum key distribution systems. However, it is only a part of the total key establishment process. For example, the sender and recipient must estimate errors in the distributed key by computing the value of Quantum Bit Error Rate (QBER). The QBER is the ratio of the number of wrong bits to the total number of bits. It is worth emphasising that not only eavesdropper can be responsible for errors; these may occur because of disturbance in the quantum channel, noise in detectors, optical misalignment, and others.

These protocols usually involve two steps: key reconciliation (the sender and recipient must find and correct/delete occurred errors) and privacy amplification (the sender and recipient should improve confidentiality of string of bits and construct the final key by deleting a part of distributed bits or shorten this key using a hash function). Currently, quantum cryptography is developing from the point-to-point systems towards the quantum-based solution over many-node networks that are running in various places worldwide (sometimes called quantum network). Serious technical problems limit the distance of quantum key distribution service to approximately 100-150 km over the point-to-point optical connections and a few hundreds of kilometres for free-space systems. However, the long-distance communication with high bit rates still is a serious challenge.

Quantum computation – the fourth dimension of quantum technology – is able to solve problems beyond the reach of classical processors by using programmable quantum gates. Quantum computer is the device where a quantum algorithm is implemented. Based on quantum bits, the quantum computer acts as a massive parallel device with large number of computations taking place at the same time. Therefore, quantum computers can break current key encryption methods, especially those based on asymmetric ciphers. Unfortunately, these vulnerable methods are widely used for key exchange, data confidentiality, and authentication throughout the world. When quantum computers become powerful enough, the services based on these methods will not be secure. Many researchers and engineers expect that quantum computers will reach this level of power in about twenty to thirty years. It is worth mentioning that modern symmetric ciphers are not so vulnerable as asymmetric algorithms. Probably, it will be necessary to increase key length as computers became more powerful. However, quantum computers also influence them and current authentication and encryption schemes which rely on symmetric-key encryption methods will also need to be updated.

4.8 Data security and privacy

The main objective of data privacy is to ensure that information cannot be accessed by individuals or parties that are not authorised to do so, while at the same time personally identifiable information (PII) remains under the control of the custodian. Traditionally, when data protection is discussed three main properties are the main security concerns: data confidentiality, integrity, and availability, commonly referred to as the CIA triad. However, privacy has begun to emerge as another very critical aspect of data protection. As technology progresses, so does the necessity to protect and properly handle personal information.

One of the first studies that actually discussed and defined privacy was by (Rubenfeld, 1989) where he defined privacy as someone's right to be left alone. Nowadays, the most commonly used definition of data privacy is the one provided by Allan Westin who defined data privacy as the right to control when, how, and to what extent information about them is communicated to others (Bertino & Ferrari, 2018). This definition is particularly comprehensive given the fact that due to the spread of the Internet, the collection of information about individuals was made possible without however these individuals having any knowledge about who has, owns, or is accessing this information (Narayanan, Toubiana, Barocas, Nissenbaum, & Boneh, 2012).

Ensuring data privacy is a task that requires more than just applying a predefined set of techniques or technologies. In many cases, data privacy is considered as a subset of data confidentiality which is just focused on personal data. However, this is not the correct approach since there are fundamental differences between these two requirements. Data privacy indeed has data confidentiality as a prerequisite, since there is no way to guarantee privacy without first protecting the data against unauthorised access, but it also has additional requirements, such as legal regulations and individual privacy preferences. Therefore, every system that is handling sensitive data should also collect and record the privacy preferences of the individual to whom the data refers to, also known as data subjects. Data privacy is by no means a new challenge, after all the European Data Protection Directive which introduced terms like processing, sensitive personal data, and consent, dates back to 1995 (E. Directive, 1995). However, big data has created an additional privacy problem by allowing the extraction of information through the correlation of large datasets.

Whereas data privacy is mostly governed by policies and procedures, data security primarily focuses on the use of physical and logical strategies in order to protect information from cyberattacks, data leaks, and data loss. More specifically, examples of measures that ensure data security include resilient data storage, access controls that prevent unauthorised access, and encryption of data both at rest and in motion. These techniques are complemented by disaster recovery plans and solid backup policies.

However, traditional approaches to data security cannot be easily applied to big data because their intended design was to address small-scale static data (D'Acquisto et al., 2015). According to (Rajan, Ginkel, & Sundaresan, 2013) some of the top high priority challenges of security and privacy in the big data can be organised into the following four categories: (i) Infrastructure Security, (ii) Data Privacy,(iii) Data Management, and (iv) Integrity and Reactive Security.

4.9 Incident handling and digital Forensics

Computer security incident response has become an important component of information technology programs. An incident response capability is necessary for rapidly detecting incidents, minimising loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. The basic steps of incident handling and digital forensics reviewed in this section consist of building a monitoring infrastructure able to identify attacks attempts and prevent spread over the internal network, as well as the training of teams to collect evidence.

4.9.1 Identification

Logs Collection: Most of the equipment, operating systems, and services making up a corporate network are able to produce event logs (e.g., Firewall, IDPS, DNS, Proxy Active Directory, Antivirus, EDR, Web and Mail services, Sysmon, etc). Each of these logs must be collected, processed, standardised, and centralised in a SIEM (Security Information and Event Management), such as Splunk, ELK or Graylog. Moreover, in order to make any future analysis work relevant, the time of all equipment must be synchronised using an NTP server.

Hunting and Detection: The detection phase consists of identifying suspicious activities, lateralisation attempts, or data exfiltration using collected logs, while the risk analysis identifies hazards that may occur. Based on these results, it becomes possible to tune the SIEMs in order to raise an alert when dreaded events are detected. Detection teams can be assisted by innovative technologies such as Artificial Intelligence (AI), capable of analysing data stored in the SIEM. AI techniques operate by learning "normal" activity and warn when a deviation is detected. Concerning OT (Operational Technology), turnkey solutions such as “CISCO Cybervision” rely on industrial equipment already in production to analyse industrial protocols and detect anomalies.

Cyber Threat Intelligence (CTI): Some highly skilled hackers groups target certain companies and specific sectors of activity by using use publicly unknown or unpatched vulnerabilities to infiltrate corporate websites and networks. The more collected and stored logs there are, the more chances a defender team have to find the specific malicious activities linked to these groups. A CTI team is in charge of tracking these specific attackers, listing the tools and exploits used, understanding lateralisation and persistence techniques. They are also able to track an infrastructure used by a group of attackers (command & control server, domain name, certificate), sometimes even anticipating future actions. CTI teams also produce Indicators of Compromise (IOCs) based on information collected and technical analysis. IOCs are then injected into the SIEMs for live detection and must be searched in previous months logs; sharing IOCs with partners reduces the chances of them being compromised.

4.9.2 Evidence collection and acquisition

When a detection is reported and qualified as relevant, several actions can be taken depending on the threat. In the case of a ransomware attack, it should be stopped immediately by disconnecting the affected machines as well as vital services in order to limit its spread to the network. On the other hand, when an advanced persistent threat (APT) has been present and introduced for some time in the network, a more refined approach may be recommended. Indeed, when hackers feel hunted by the incident response teams, they may be tempted to the erase evidence of their activity by destroying all or part of the network, as was the case during the attack on "TV5 Monde". Concerning the collection of one or more computers, it is advisable to dump the RAM before switching off the machine and then do a bit-for-bit copy using for example a write blocker such as the "Tableau® TD3".

As part of a hunting campaign, bit-for-bit collection of hundreds of machines is not an option due to time waste. The most relevant artefacts will be harvested, such as memory dumps, registry databases, prefetches, event logs, files listings and fingerprints, pagefile.sys, hiberfile.sys, or browsing history. Most of EDR and some DFIR tools such as “DFIR ORC” can handle this task remotely.

Whether it is bit-for-bit copying or targeted artifacts collection, a timeline of machine activity should be established with tools such as Plaso, Autopsy, X-ways or Encase. Resulting timeline should then be injected into a software like Splunk. Pre-programmed dashboard can then look for abnormal patterns and behaviours (e.g., weird entry in registry, newly created and launched services, remote failed administrator connection, brute-force attempts, senseless internal computers communications, etc).

Once the digital forensic analysis is finished, for either as part of a detection or hunting operation, these timelines should then be stored in SIEM, so that they can be compared with the IOCs that will be imported over the next few months/years in order to detect any compromise that may not have been seen during analysis.

4.10 Vehicular systems

Vehicular Systems include aerial, ground, and water transports of all kinds, both for people and for goods, such as aircrafts, trains, metro, cars, buses, ships, and submarines. Vehicular systems are highly interdependent with electrical power generation and transportation, telecommunications, satellite localisation, the petrol industry, and so on. Vehicular Systems also generate and exploit large quantities of data, and thus many data-driven services are available (e.g., public transport apps, traffic monitoring, smart payments, connected cars, remote diagnostics, and preventive maintenance). Moreover, due to the nature of human beings, transportation transcends the pure physical dimension of moving people and goods from point A to point B, because it is the enabling technology that makes people meet each other, send and receive presents, go out for a trip or make the journey of a lifetime, have the possibility to know other cultures and breath the air of exotic places.

According to (Habibzadeh et al., 2019), public transport and electric vehicles are also much very interconnected to Smart Cities and their underlying infrastructure (e.g., recharging stations, traffic control, and telecommunications). In case of an attack to the transportation infrastructure, such as a denial of service or data, consequences can be critical. An attack to a public transportation system can target either the industrial control system networks and infrastructure or it may aim to disable ticket machines and payment infrastructure, as well as computer systems that are used to manage the infrastructure (Gallagher, 2016). Such systems may be vulnerable to a ransomware able to paralyse the transportation infrastructure of an entire city for a long period of time; also in case the ransom is paid, there is no assurance that the data will be unencrypted and that the systems will become available again. In this scenario, the importance of incident handling, backup and

restore procedures, as well as of offline backups is crucial. (Bay Area Rapid Transit, 2017) reports the case of Bay Area Regional Transit system did in California that was targeted by ransomware. In this case, the public transport system allowed the riders to travel for free, resulting in loss of revenue.

If we analyse the Vehicular Systems from a maritime perspective (one of the priority sectors in ECHO), we see that the concept of cyber-enabled, interconnected ships, arises. In the recent years, ship-owners (including Navies) are required to optimise operational costs, thus reducing on-board crew to operate the ships towards completely unmanned vessels, either autonomous or remotely-controlled. Unmanned ships are likely to have a greater array of digital infrastructure than traditional ones, in order to ensure that ship owners and operators are able to control and track their ships remotely. However, it is probably worth mentioning that the maritime industry as a whole has been criticised for being a bit slow in reacting to existing cyber threats, including fully crewed vessels, and that the biggest threat to any organisation's cyber-security posture is still, in fact, human error. It is therefore possible that a transition to unmanned ships might actually reduce an organisation's profile and exposure to cyber risks. The cyber threat should certainly be taken seriously, but it should not put the brakes on further exploration of the viability of unmanned ships.

Indeed, ships are cyber-physical systems where IT and OT have equal importance in terms of safety of ship conduction and security of the assets. The growing need of interconnection, exposes ship systems to malicious agents that may exploit vulnerabilities for money extortion or to cause physical damages. Cybersecurity incidents have been experienced by large companies such as COSCO Shipping, Maersk A/S and SAIPEM. There are still lot of unknown specific vulnerabilities to cyberattacks of today's marine transportation systems and equipment. Modern ships are more and more dependent on integrated IT and OT, and on sophisticated equipment such as ECDIS (Electronic Chart Display and Information System), AIS (Automatic Identification System), Radar/ARPA (Radio Direction and Ranging) (Automatic Radar Plotting Aid), Compass (Gyro, Fluxgate, GPS and others), Steering (Computerised Automatic Steering System), VDR (Voyage Data Recorder – "Black Box"), GMDSS (Global Maritime Distress and Safety System), and numerous other advanced units and systems. All these systems are potentially open to cyberattacks.

As an example, we can consider the Electronic Chart Display and Information System (ECDIS), a computer-based navigation system that is an alternative to paper navigation charts. ECDIS integrates a variety of real-time information and serves as an automated decision aid, continuously determining a ship's position in relation to land, charted objects, navigation aids, and unseen hazards. ECDIS includes electronic navigational charts and integrates position information from GPS and other navigational sensors, e.g., radar, fathometer, and automatic identification systems (AIS). ECDIS may also display additional navigation-related information, such as sailing directions.

ECDIS vulnerabilities could allow an attacker to access and modify files and charts on board or on shore. The result is that the crew has unreliable and misleading navigation information, that may induct wrong manoeuvres leading to collision or grounding of the vessel, thus impacting security of the assets, safety of the crew and reputation of the ship-owner.

In January 2014, the NCC Group performed a penetration testing onto an ECDIS product from a major OEM. Security weaknesses found include the possibility to read, download, replace or delete any file stored on the computer hosting the ECDIS. Once the ECDIS is compromised, the attacker may also perform lateral movement ant compromise other navigational systems, such as ARPA, AIS or even the VDR (the ship black-box) causing damage to the ship, the transported goods and the crew while having the possibility to clear or alter logs and VDR recordings. The attack vectors are multiple in this case, it can be brought via infected USB key, by downloading a malicious email attachment, and eventually it can also be conducted from remotely by exploiting SatCom channel.

Maritime security is a key topic in maritime since the beginning of 2000s. In 2004, the U.S. presented a national maritime security policy. The increase in piracy attacks in 2008 and 2011 outside the coast of Somalia also contributed to increased attention to global maritime security. In 2011, maritime security became one of the objectives in NATO Alliance Maritime Strategy. In 2014, UK, EU and the African Union proposed maritime security strategies, while the Maritime Safety Committee (MSC) in the International Maritime Organization has recently published guidelines on maritime cyber risk management. Classification Societies such as Bureau Veritas, DNV-GL and Lloyd Register have issued cybersecurity guidelines taking into consideration the state of the art of international standards (i.e. ISO 27001, NIST SP800-53, IEC 62443) that will be used by shipbuilders, ship systems OEMs and ship-owners to design, build, deliver and operate secure, interconnected, cyber-enabled ships.

5. Transversal technical cybersecurity challenges

The exponential increase in threats and vulnerabilities and the sudden growth of interconnectivity create the need for a technical assessment of the most important challenges, as there were identified by our analysis. This assessment is based on three pillars: (i) challenge description, (ii) mitigation, and (iii) opportunities; i.e., for each identified transversal technical cybersecurity challenge, the following are provided: (i) a detailed description of each specific challenge, (ii) the mitigation techniques currently existing either as a commercially available product or as the state-of-the-art on a research level, and (iii) the opportunities that can be derived based on the availability of mitigation techniques and solutions.

Next, the 57 transversal technical cybersecurity challenges belonging to nine of the previously defined research and technological domains are analysed.

5.1 Software and hardware security engineering

Engineering-based solutions, both at the software and hardware levels, are essential for managing the growing complexity, dynamicity, and interconnectedness of today's systems, in order to develop more secure and defensible systems, ranging from cyber-physical systems to systems-of-systems (including IoT). The overall objective is to address security issues and use established engineering processes so as to ensure that all stakeholders' requirements are addressed appropriately throughout the life cycle of the system.

A large percentage of the security incidents that take place can be attributed to vulnerabilities existing in an application's source code. Evidently, it is necessary to prevent such vulnerabilities existing the first place which makes software developers as the first line of defence against these software bugs and their subsequent exploitation. In most cases, distinguishing security auditing from development adds an additional overhead primarily, but also increases the development cost since detecting vulnerabilities late in the project development lifecycle creates additional costs both in terms of money and time.

In the following section, we examine the cybersecurity challenges related to application security by dividing them into desktop applications and Web applications.

5.1.1 Application Security

Out-of-date security standards and protocols

Using old versions of firmware/applications can easily jeopardise the entire information system; the same of course applies for email protocols, web servers, operating systems, and communication channels. This is especially true for smaller businesses and home users where devices and systems connected to the internet have become more affordable.

Challenge:

TCP/IP was created in the early days of the Internet when security was not a priority (as there were far fewer threats than today). Since then, the situation has changed significantly, so it is worth making sure that the organisation uses the best possible secure Internet communication. TLS is a cryptographic protocol designed to provide secure communications over a computer network, while its predecessor was SSL. Several versions of the protocols are broadly used in applications such as web browsing, messaging, and voice over IP (VoIP); websites can also use TLS to secure communications between web browsers and servers. To protect Web

traffic, it is important to use up-to-date and more secure versions of the TLS protocol. The deprecated TLS 1.0 and 1.1 versions account nowadays for a very small percentage of Web traffic today, and various vulnerabilities have been found in these legacy versions in recent years.

Mitigation:

Experts recommend, among other things, switching from SSL and older versions of TLS to at least TLS 1.2; it is worth noting that the PCI DSS standard that is used to handle online financial transactions no longer recognises SSL and older versions of TLS as meeting sufficiently high-security requirements.

Opportunities:

With the increased number of devices that rely on encryption for their secure communications, the volume of devices which become exploitable due to their use of exploitable encryption algorithms and protocols also increases. In many cases patching and updating existing systems is challenging either because it is not technically possible or because the number of vulnerable systems is too large, making the update procedure uneconomical.

One of the most promising approaches, which still remains though on a research level, is to use a centralised software-defined networking architecture which exploits the negotiation before the handshake that many security protocols perform. This negotiation usually contains, in plaintext, parameters such as protocol version, encryption algorithms, and certificates. Even though this approach can be extended to many protocols, its primary usage is to detect outdated protocols in SSL/TLS sessions. In this approach, the handshakes are monitored by a network controller, without having a significant impact on the latency, which instructs devices like switches on how to handle these flows. In case a TLS handshake that uses outdated protocol version is found, the controller either allows or rejects the connection based on a defined security policy, thus achieving policy compliance (Ranjbar, Komu, Salmela, & Aura, 2016).

Out-of-date and unpatched Windows systems

Older and unpatched Windows systems are particularly vulnerable because attackers do not need to exploit a zero-day vulnerability to successfully compromise them; they simply need to exploit known vulnerabilities that are publicly documented in open source databases.

Challenge:

Different versions of MS Windows undoubtedly dominate when it comes to operating systems used on personal computers and, although the latest version of this operating system, Windows 10, has exceeded 50% market share, older versions (such as Windows 7) are still in use and Microsoft directly recommends the transition to Windows 10; unfortunately, though, the process of free upgrades to the latest version of the system was completed in 2016, and therefore such a transition will require a substantial license fee. To upgrade to Windows 10, you have to thus purchase a license, download the appropriate tool from Microsoft's official website, and follow the on-screen instructions. Even an average computer-acquainted user should be able to handle the process, and in case of problems, Microsoft support (present, of course, during the transition process from the old system to the new one) will certainly prove useful. Full instructions for upgrading to the latest version of the system can be found on the official website of the manufacturer.

Mitigation:

Windows 10, which is more stable and secure than other systems, made a large part of users switch to them. Microsoft is releasing new system security updates frequently, and this makes it possible for users to be safe on their computer network. The main incentives to keeping the MS Windows operating system up-to-date are

obvious. An up-to-date version of the software is a guarantee that we have access to the latest security improvements and technologies that support us in the fight against cyber threats. Windows 10 features an improved Windows Defender service, which is even better at detecting and combating malware.

Opportunities:

For a variety of reasons, mainly economical and practical, Windows systems remain unpatched for extensive periods of time. This delayed deployment of critical Windows updates gives cyberattackers a strategic advantage since studies showed that there is very short window between the release of a patch and the automatic generation of an exploit (Brumley, Poosankam, Song, & Zheng, 2008). Even when a Windows system is timely patched, a Microsoft report showed that malicious actors are still able to infect systems by developing new advanced techniques (Batchelder et al., 2014).

One of the most interesting approaches to provide resilience to unpatched systems is through the use of a Moving Target (MT) technique. More specifically, in an effort to detect and protect unpatched software, a study created a detection engine using a dynamic software-based MT technique called *multi-variant execution.* In this study, the authors relied on running two variants of the same application (patched and unpatched) and performed differential analysis in order to detect deviations in the execution traces (Bauer, Dedhia, Skowyra, Streilein, & Okhravi, 2015). This work creates an interesting opportunity for protecting Windows systems which cannot be immediately patched.

Attacks on RDP services and Remote Command Execution

BlueKeep, otherwise known as CVE-2019-0708, is a remote desktop remote code execution vulnerability in Window OS that Microsoft has patched. Essentially BlueKeep allows hackers to exploit this vulnerability by infiltrating the target's Remote Desktop Protocol (RDP) services in their computer and transmitting customised crafted code request. Because this vulnerability is accessible pre-authentication and does not require user involvement, it allows non-authenticated users to easily place arbitrary code in the target's computer to his/or her bidding. BlueKeep also has the potential to be "wormable" and allows malware to spread autonomously from one vulnerable system to another. An unauthenticated user can connect to a vulnerable system via Microsoft's proprietary RDP and take control of it to steal credentials and data or plant ransomware and other malware.

Challenge:

As Bluekeep has the potential to become a wormable event, it allows the malware to self-propagate and infect multiple vulnerable computers without user interaction, similarly to the WannaCry worm. Microsoft has even made patches to non-Windows operating systems to combat this vulnerability. Bluekeep is no longer wormable, but it is being distributed to target computers and installing cryptomining malware. Sectors affected by the threat are both the public and private sectors, as well as personal computer usage.

Mitigation:

BlueKeep is a reminder that organisations need to secure RDP services. Best practices for mitigating risk include disabling RDP on systems that do not require it, using strong passwords and account lockout to protect against brute-force attacks, applying available patches and updates to address known vulnerabilities, and enabling network-level authentication.

Opportunities:

The real-time interactive work that is provided by RDP can lead to some serious security issues and side-channel privacy leakage (Chen, Wang, Wang, & Zhang, 2010). Also, the experimental results demonstrated in (Jiang, Gou, Shi, & Xiong, 2019) showed that the currently used encryption mechanisms are unable to protect a user's activity, something that should be further researched in order to provide stronger resilience against side-channel attacks.

DLL Injections

DLL injections are injection attacks in applications that can manipulate the functionality of a running process in a manner that was not intended by the creator behind the DLL file. This means that the application is injected with malicious code, which is initiated as soon as the application's DLL entry point is called.

Challenge:

DLL injections are attacks that manipulate the execution of a DLL file for a running process in an application. In essence, the attack transmits the DLL into the RAM of the system. The challenge in these types of injections is that even though they look benign on the surface, they perform actions that are invisible to the user.

Mitigation:

System tools like PowerShell and command prompt should be restricted to administrators, and tools capable of executing scripts should be locked down or removed. Additionally, to prevent DLL injection, we need to ensure that no untrusted process gets elevated access to an application.

Opportunities:

A dynamic signature model, proposed in (Chen, Lai, Chang, & Lee, 2020) creates an interesting opportunity for detecting injections during runtime. In this study, the authors managed to create a signature, based on the API call sequence. They also took into account other attributes such as the process name and the parent process, and used this as an input to their API hooking process. The extracted behaviour is then compared against an existing dataset of signatures, creating what the authors call a *behaviour analyser*.

System misconfigurations

Misconfiguration of applications and infrastructure present opportunities for adversarial cyber actors to achieve their objectives. Microservices are transforming application architectures, breaking the dependence of applications on back-end infrastructure. Popular microarchitectural platforms like docker allow an application to be virtualised and housed in a container which shares OS and libraries and binaries with other applications. These containerised applications should be configured to communicate securely within the docker host. Misconfiguration of a docker host would allow an adversarial cyber actor to compromise the host and use its administrative permission to exploit or disrupt the communication channel with other docker container applications (Dietrich et. al, 2018).

Challenge:

From post-incident response and threat intelligence reports the misconfigurations have been identified as default container names, default service ports and unsecure or no encryption of Docker Daemons. An investigation from Palo Alto security threat intelligence team, Unit 42 identified over 40,000 Kubernetes and Docker containers were misconfigured and vulnerable to exploitation. Once the attacker has managed to gain

access to the docker host they can deploy malicious payloads on the host or obtain sensitive information such as credentials and configurations from the docker log (Palo Alto, 2020).

Mitigation:

The optimal mitigations for docker misconfigurations have been identified as:

- Always enforce mutual authentication when configuring TLS on Docker daemon socket
- Docker can make use of a Linux feature called user namespace which, when enabled, allows for container isolation by limiting container access to system resources. Setting applications to run as regular users can stop privilege escalation attacks from accessing the critical parts of the container.
- Mandatory access control (MAC) tools such as SELinux (Security-Enhanced Linux) and AppArmor can help prevent attacks that compromise application and system services by limiting access to files and network resources.
- Minimising the use of third-party software and using verifiable ones ensure malicious software is not inadvertently introduced to the container environment.
- Mounting the host's root file system in read-only mode will restrict write access for applications, limiting the chances of an attacker being able to introduce malicious elements to the container.
- The UNIX socket is a two-way communication mechanism that allows the host to communicate with the containers. Disabling this socket can thwart attacks that exploit it — for example, an attacker abusing the API from inside a container (Trend Micro, 2019).

Opportunities:

Cloud computing environments and virtualised application and infrastructure technology are a prime-target for cyberattacks. The architecture of the internet is changing, new protocols are being developed to support the mass-scale required by content delivery networks and internet services are transforming to micro-services that are more architecturally efficient. Greater research in the areas of systems security, privacy and cryptography to understand the existing flaws in docker implementations will provide users more understanding of the requirements for secure micro-services architecture.

Mobile malware

Traditional security techniques like host-based intrusion prevention and detection, internet activity monitoring, and others are falling short when it comes to securing mobile devices. There are some mobile security frameworks (e.g., Google Play Protect and Apple iOS application store security) that review and validate apps to substantiate if they are legitimate by comparing versions to known bad repackaged apps or malware, before allowing them to go to their respective application stores.

Challenge:

The mobile devices present in today's home and work environment are practically mobile computers and may include anything from mobile phones, game consoles, personal assistants, thermostats, video cameras, even washing machines and dryers. With every new convenient feature or functionality, new code is added to a device. With every new line of code, new potential security risks are introduced. Devices once considered secure can now be exploited for nefarious goals, while the information that is stored in such devices comprises a sizeable portion of an individual's Critical Information Infrastructure (CII).

Some of the main reasons why attackers are shifting their attention to mobile devices are:

- the diversity of smart mobile devices, both IoT and smartphones;
- the increased software applications and features with lacking secure coding practices;
- the lack of user awareness of the existing threats and the overall lack of monitoring for said threats;
- the ability to track a user's physical and online interactions;
- the use of open-source application platform (like Android) makes it easier to develop malware; and
- the lack of mature security controls or systems to detect or prevent malicious activity on mobile devices.

The weakest link in any IT security chain is the user awareness and training of the users. Therefore, the responsibility for securing mobile devices should mainly land on the service providers to secure the medium or the network these devices are operating on, the marketplaces where mobile applications can be acquired, and also on the developers to secure the software running on the devices.

A worrying development is the ability of cyber-criminals to tap into and use the vast resources of mobile device networks and turn them into zombies as part of botnets that can be used to launch cyberattacks. Malwares like DroidJack, Dendroit, GMBot and others had integrated thousands of mobile devices into extensive botnets. Some of these malware strains are developed to exploit vulnerabilities on either the operating systems (OS), installed applications, or just to change or steal user information. Advanced mobile botnets like Geost and ADB.bot have also been on the rise. These botnets have turned their attention to Android mobile devices and at its peak Geost recorded to have over 800,000 infected android devices. The use of specific to mobile botnets C2 creates additional challenges that differentiate them from well-known PC-based botnets.

Mitigation:

It is essential for users to be aware of the security measures of their mobile device and the overall advice to users includes:

- Keeping the device software up to date is crucial in preventing exploitable software vulnerabilities.
- Installing anti-malware applications will protect and notify the user if malware installation is attempted.
- Installing applications from trusted sources (Google and Apple app store) only will ensure the installed application has passed rigorous testing against malware before it is installed on the device.
- Install only applications from the official developer.
- Before installing an application check the permission it requires. If the application requires access to sensitive information like contact and SMS lists be weigh the risks involved.
- Install remote locate, track, lock, wipe, backup and restore software to retrieve, protect or restore a lost or stolen mobile device and the personal data on the device.

Opportunities:

Mobile malware is continuously evolving with new functionality and updated distribution methods. However, the most difficult part in detecting new malware is their use of detection avoidance techniques such as obfuscation and repackaging. Anti-malware scanners are not very effective against these evading techniques, which was the main motivation behind the work presented in (Alazab, Alazab, Shalaginov, Mesleh, & Awajan, 2020). In their work, they were able to identify commonalities among different malware families and determined that API calls and permissions are an efficient classification for detecting malicious behaviour, thus identifying mobile malware. Even though this frequency analysis was empirical and was applied to a subset of all available android apps, the results suggest that this proposed method is promising and worthy of further exploration.

Ransomware

Ransomware is a general term used to encompass malware used for digital extortions. We recognise the existence of two major forms of ransomware: the first, and most common, that aims to hide, encrypt, or deny access to files, and the second that locks the victims out of their systems. Hybrid forms exist, where the ransom is not paid with money (e.g., to unlock the PC or the encrypted data, the victim must execute specific orders or complete a task) or there is no request at all. However, in most situations, victims are required to pay a fee (generally using cryptocurrencies) or accept some kind of loss, such as access to files or database, access to the infected devices, or other unwanted consequences.

Challenge:

With the availability of cryptocurrencies and RaaS (Ransomware as a Service) through anonymous TOR channels, the Ransomware encryption malware became dominant and much more diffused, due to the high ROI and the low risks for the attackers, and the basic skills necessary to launch a successful RaaS campaign. Due to extensive press and media coverage, most of the people know or heard about the WannaCry Ransomware. In 2017, it spread like wildfire in many countries due to a (largely unpatched) Microsoft Windows vulnerability exploitable remotely through the “Eternal Blue” vector. The very first version of WannaCry included a kill-switch that was incidentally activated by a security analyst, who was studying its inner working, so damages were initially contained. Another version of the malware was released, this time without the kill-switch, and more than 200.000 computers and many corporations were hit worldwide. Even though the WannaCry creators did not earn much money, this ransomware was crucial for the development of new strains and raised awareness about cybersecurity.

Mitigation:

The most common recommendations for businesses and individuals in order to minimise the damage or even prevent it is the following:

Understand the risk: The risks that ransomware presents are very high and have the potential of totally disrupting an organisation’s functions. Understanding the full extent of this risk can help an organisation make decisions regarding the prevention of such kind of attacks and prioritise accordingly.

Create a stricter security policy: Organisations should make sure that their employees understand their role in protecting against ransomware while at the same time the use of privileged accounts should be minimised following the principle of least privilege (Richardson & North, 2017).

Train the users to follow best practices: Proper password management and continuous security awareness training should be part of every organisation’s employee training programme.

Opportunities:

A novel machine learning based ransomware detection method was presented in (Hirano & Kobayashi, 2019) which was able to detect a significant number of 0-day ransomware attacks. The proposed scheme used a behavioural model based on storage I/O requests on a hardware level and was able to distinguish ransomware from other benign programs with an F-measure rate of 98%.

5.1.2 Web Applications

Malicious Browser Extensions

Browser extensions are basically software modules used by web browsers to provide additional functionality and improve user experience. Malicious browser extensions are usually presented as legitimate and helpful extensions and even though they sometimes provide their claimed functionality, they can damage the computer, steal data or perform unauthorised actions on the user's behalf. If an extension has access to all the web pages someone is visiting, it can do practically anything. It could function as a keylogger to capture someone's passwords and credit card details, insert advertisements into the pages they view, redirect their search traffic elsewhere, track everything they do online – or a combination of the above. Even though they are in most cases small pieces of software, they have an elevated level of access to someone's web browser, and that makes them dangerous. Even an extension that only provides a minimal functionality, may require access to a substantial amount of information stored in a web browser (Tzur-David, 2019).

Challenge:

Unsafely coded browser extensions can compromise the security of a browser, making them attractive targets for attackers as a primary vehicle for conducting cyberattacks. Among others, the main factors making vulnerable extensions a high-risk security threat for browsers and the main challenges to overcome (Shahriar, Weldemariam, Zulkernine, & Lutellier, 2014):

- The wide popularity of browser extensions.
- The similarity of browser extensions with web applications.
- The highly privileged access level of browser extension scripts.
- The most popular marketplace for extensions, the Google Chrome Web Store, does not screen extensions before they are published. This makes extremely easy to publish malicious browser extensions.
- Extensions are not an application all on their own – their code runs as part of someone's browser. Because a browser is considered a trusted application, it is hard for antivirus software to catch malicious extensions.
- Though extensions require permissions to work, most browsers grant them permissions by default. Even if a browser asks for an elevated access confirmation, many extensions – Including safe and legitimate ones – will not install without the permission to "view and change all your data on the websites you visit."
- Mechanisms that specifically target to mitigate browser extension-related attacks have received less attention as opposed to solutions that have been deployed for common web security problems, such as SQL injection, XSS, logic flaws, client-side vulnerabilities and drive-by-download.

Mitigation:

A range of countermeasures exists, some of which can be easily applied but some others require fundamental changes in the underlying extension architecture. Some of the most popular ones are:

Iframe-Based Phishing: An iframe that contains sensitive information can be easily detected, especially if the iframe content is provided over an HTTPS connection, and for every attempt to modify that content the user must be notified.

Restricting Cross-Site Requests: Several approaches for detecting cross-site requests are available with the most popular one being a privilege schema that resides between the browser core and the scripts. The extension core is granted explicit cross-site access privileges via the manifest file, whereas any attempt to bypass this via the use of a malicious content script is prevented by having it explicitly declare any remote origins added to the webpage (Perrotta & Hao, 2018).

Opportunities:

Future research activities should mainly focus on information flow analysis to capture suspicious data flows, privilege restriction on API calls by malicious extensions, digital signatures to monitor process and memory level activities, and allowing users to specify their own security policies in order to restrict the operations of extensions.

CMS Hacking

Content Management Systems (CMS) play a major role in the content that is available online. According to (W3Techs, 2020), 63% of all the websites are based on CMS, with WordPress being the most popular one with a market share of 37.2%. Other popular platforms are Joomla and Drupal with a market share of 2.4% and 1.6% respectively. Regardless of the underlying CMS platform, all these systems are affected by attackers, exploiting various vulnerabilities such as website owners not keeping their CMS, plugins up to date, using plugins with malware or not using some kind of application firewall.

Challenge:

The fact that more than 73.2% of all WordPress installations are vulnerable (WP Whitesecurity, 2019), creates a great concern regarding the general situation with CMS security. Although hosting companies are usually informed in time, many hosts are left uninformed about how to protect their web servers in case their clients use an outdated and vulnerable version of WordPress. There is a lack of a warning system that will alert in an organised way web hosting companies about the seriousness and the impact of a newly found security flaw. As an example, in 2017 a vulnerability in version 4.7.2 of WordPress allowed hackers to deface around 2 million websites (Jerkovic & Sinkovic, 2017). Even though the disclosure about the vulnerability was timely, there was no publicly released information about how someone could protect their web server.

Mitigation:

Countermeasures for attacks on CMS platforms can be categorised in different ways, but the one proposed by (Gupta, Govil, & Singh, 2014) is the more structured one. It should be noted that the predominant type of attacks against CMS is SQL injection and cross-site scripting; thus the mitigation techniques presented in this deliverable in their respective sections also apply to CMS.

Defensive coding guidelines: Guidelines for CMS plugin developers should instruct how to write the application code in a secure manner. However, human errors cannot be completely avoided; that is why guidelines alone cannot guarantee the security of the code.

Vulnerability detection approaches: Static analysis and dynamic analysis are to of the most popular testing methods for source code. In static analysis, the code is examined for vulnerabilities without however actually running the code. It offers the advantage of covering all application parts but at the same time, it creates a lot of false positives. On the other hand, in dynamic analysis, the code is executed, and the behaviour is analysed.

Attack prevention approaches: In this approach, monitor daemons are installed both on the client and server-side and analyse data traffic for patterns known to be associated with attacks.

Opportunities:

The majority of the attacks against CMS are based on SQL injection and cross-site scripting, hence the opportunities that are described in Sections 0 and 0 also apply in this case. The study performed by (Ruohonen, 2019) showed that WordPress deployments with a large user base are more prone to vulnerability exploitation and suggested the use of a vulnerability-based metric to calculate the quality of a WordPress plugin.

Cross-site scripting / XSS Injection

Cross-Site Scripting (XSS) enables attackers to inject malicious code into website content viewed by visitors/users. A web page or web application is vulnerable to XSS if it uses unsanitised user input in the output that it generates. The web page or web application becomes then a vehicle to deliver the malicious script to the user's browser and gain access to sensitive data, webcam, microphone, files, etc. It can also change the content of the website or even redirect the browser to another web page, for example, one that contains malicious code.

Challenge:

According to a study conducted by Positive Technologies (Positive Technologies, 2019), 88% of all known web application vulnerabilities are related to XSS. Modern web applications accommodate for a wide range of end-users providing them with features relying on client-side technologies such as JavaScript and ASP. The variety of technologies and platforms that web developers have in their disposal nowadays, introduce the challenge of applying proper defensive security measures. Taking into account that the key objective of XSS attacks is the web browser's credentials theft, highlights the importance in the impact that such incident could have in organisations that operate in sectors like healthcare, finance, and energy.

Mitigation:

The most commonly used mitigation techniques can be classified into four categories (B. Gupta & Chaudhary, 2020):

Client-side approaches: In this approach, mitigation techniques are implemented on the client-side and usually come in the form of an extension or as a base functionality of a browser

Server-side approaches: In this approach, mitigation techniques are implemented on the server-side in order to defend against XSS attacks. Examples of such implementations are the *black box detection-based technique* (Duchene, Rawat, Richier, & Groz, 2014) and the *context-sensitive sanitisation* (M. K. Gupta, Govil, Singh, & Sharma, 2015).

Combinational approaches: In this approach, mitigation techniques are implemented both on server and client-side. Examples of such implementations are the *buffer-based cache technique* (Panja, Gennarelli, & Meharia, 2015) and the *runtime tracking and randomisation* (Nadji, Saxena, & Song, 2009)

Proxy-based approaches: In this approach, mitigation techniques are implemented in a proxy server which resides between the user's browser and the server.

Opportunities:

Alongside the increase in cross-site scripting attacks, a few mitigation approaches have been proposed to detect them. Some of them were presented in the previous section; however, all of them rely on string comparison and payload signatures. In order to detect obfuscated XSS attacks, the most promising approach is the one suggested by (Rathore, Sharma, & Park, 2017) where the detection relies on machine learning classifiers.

Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated. These executions involve changing the functionality of a state change request produced by the web application server, such as changing the victim's password, email address, or transferring funds from a bank account. CSRF is often initiated through social engineering in through email or chat hyperlink attached with the malicious script request. So, if clicked, the CSRF exploit is executed with certain specific commands that force the unsuspecting victim into performing the unknown action on the attacker's behalf.

Challenge:

CSRF is based on target state requests from the web application. What this means is that because most web browser applications collect credentials such as cookie session IDS, IP addresses, and other browser information the web application assumes that through access the end user is the authenticated one. Therefore, when a CSRF attack is executed, it is initiated while the authenticated user is logged, which makes the request execution hard to differentiate between a forged one from some script or from an authenticated user. Websites that do not setup their applications with the right validation input leave themselves vulnerable to these attacks by people with unauthorised access. CSRF scripts have the potential to be stored in web applications without the need of social engineering by editing the HTML content in a web page. These vulnerabilities can be devastating because a user who might already be authenticated can be susceptible to an immediate attack upon entering the site. In addition, if the CSRF affects users with elevated privileges, like an administrator, the entire web application can be compromised.

Mitigation:

There are plenty of documented solutions to help thwart CSRF, such as the use of CSRF tokens whether built in from the website's framework or customised for all state changing requests per session and validated these request on the backend of the server. Utilising SameSite, a cookie attribute that is now being distributed in desktop web browsers and mobile browsers, helps mitigate CSRF attacks by instructing browsers whether or not to send cookie sessions along with cross site requests (GET/POST) depending on the attribute (Lax, Strict, or None) attached to Samesite. Creating custom headers, along with verifying the source of standard request headers and using double submit cookies can be effective in CSRF mitigation. Lastly, it is recommended to not use GET request for state changing requests on a web application.

Opportunities:

An interesting approach that attempts to solve the problem of CSRF attacks is the one presented in (Sudhodanan et al., 2017). The concept of the proposed tool examines the HTTP requests that contain the security token and then asks the requester to provide the URL of the Identity Provider (IdP) and provide an input just before authenticating.

SQL Injection

The growth of SQL injection (SQLi) as an attack vector over the last two years (Akamai, 2019) should concern website owners. In the first quarter of 2017, SQLi accounted for 44% of application-layer attacks

Challenge:

SQL Injection is a vulnerability that allows an attacker to interfere with queries that a web application makes in the database. This can allow an attacker to obtain data from other users or modify and delete data, causing changes in the app's behaviour. This technique exploits vulnerabilities in the application web interface. Vulnerability is present when user entries are not correctly verified by web applications, and requests are sent to database servers in the back-end.

A web application is hosted by a web server that can send a form to the client's browser. The client communicates through the HTTP/HTTPS protocol and transmits the data entered by it to the web server. The web server provides this data to the application that communicates with the database server, usually via SQL.

An SQL Injection attack usually follows the next steps:

1. The attacker enters the web server address into the browser and sends an HTTP/S request to the hosted application.
2. The web server receives the request and sends it to the hosted application. The server-side application generates a form and with the help of the web server sends the HTTP/S response to the attacker.
3. The attacker enters malicious data and sends it to the app.
4. The application does not filter input data and accesses the database server with SQL queries made up of this data.
5. The attacker gets remote control.

SQL injection attacks usually occur when input data is from a non-trusted source, and SQL queries are dynamically built; a technique that enables developers to build SQL statements dynamically at runtime.

The effects of this vulnerability affect the CIA model (Confidentiality, Integrity, Availability). Databases contain confidential data and their integrity can be exploited by modifications or deletions. An attacker can get the names of the system users and the password-associated hash.

SQL Injection can be classified into three major categories: In-band, Inferential/Blind and Out-of-Band. In-band SQL uses the same communication channel to both launch the attack and gather information. Out-of-Band injection exfiltrates data through an outbound channel, either through DNS or HTTP protocol.

Mitigation:

There are three main internal measures to protect against SQL injection: filtering, encoding and separating code and data. The filtering or escaping procedure does make the code more secure. The only solution to thwart SQL injection is to separate data from code.

Internal measures:

- input validation on the client-side;

- input validation on the server-side;
- separate code from data;
- data sanitisation;
- parameterised SQL statement;
- using stored procedures;

External measures:

- error handling to avoid displaying detailed error information;
- implementing a security mechanism likes Intrusion Prevention System and Web Application Filter;
- monitoring for anomaly and proper incident response;
- improve network and security architecture design;
- third party authentication;
- strong password hashing using salt;
- principle of least privilege regarding access of databases, secure the database and privileges;
- update and patch software components; and
- test web applications.

Opportunities:

Through the analysis of the syntax and the behaviour of web-based applications, some studies were able to detect SQL injection attacks. For example, the work of (Xie & Aiken, 2006) presented a method that utilised static taint analysis to detect vulnerabilities in PHP code. However, the work of (Gu et al., 2019) follows a completely different approach and instead of relying on the detection of SQL injection attacks, it actually tests the robustness of newly deployed applications against the aforementioned type of attack. Another novel idea presented in the work of (Abaimov & Bianchi, 2019), detects not only SQL injection attacks, but code injection attacks in general, using Deep Neural Networks (DNN) and more specifically Convolutional Neural Networks (CNN).

JavaScript Injection

JavaScript Injection is an injection attack that threat actors use to insert their malicious JavaScript code into web pages with input code vulnerabilities. Typically, this attack unleashed on the client-side when a user visits the web site. Once the script is enacted is upon the user's viewing of a web page, the JavaScript can allow the attacker to perform activities like cookie theft, keylogging or phishing where they steal sensitive information such as passwords or financial info, for their gain.

The main purpose of JavaScript Injection is to change the website's appearance and manipulate the parameters. Consequences of JavaScript Injection can be very different – from damaging a website 's design to accessing someone else's account. There are three common ways that JavaScript injections are executed either by inserting the malicious scripts in the developer's console interface, entering the code directly in the URL address bar of the web page, or through XSS, placing <script> syntax into web page forms or comment fields.

Challenge:

JavaScript code can be injected into a client-side server or address bar to manipulate web pages like phishing techniques. Website owners that do not set up their applications with the right input validation and sanitisation leave themselves vulnerable to these attacks.

The attacker has injected code into a page served by the website, the malicious JavaScript is executed in the context of that website. This means that it is treated like any other script from that website: it has access to the victim's data for that website (such as cookies) and the hostname shown in the URL bar will be that of the website. For all intents and purposes, the script is considered a legitimate part of the website, allowing it to do anything that the actual website can.

Mitigation:

Check website files to see that no unfamiliar files have been uploaded, along with patching plugins and bugs, along with reviewing validation input syntax to minimise the vulnerabilities that can be exploited.

Remove HTML tags for comments, forums, feedback: Before saving to the database, replace all < with < (HTML symbol lesser than), and all > with > (HTML symbol greater than). It will prevent XSS, and any people trying to insert HTML into a website.

Server-side checks: As a rule, validation of forms and inout restrictions should be applied.

Opportunities:

Given the similar nature of SQL injection attacks and JavaScript injection attacks, the opportunities described in Sections 0 and 0 also apply to this section.

Cryptojacking scripts and extensions

Cryptojacking is the act of unauthorised use of someone else's computer power resource to mine cryptocurrency. Cyber criminals are able to do that by tricking the victim to click on a malicious link (usually send via an email), that installs cryptomining software onto the victim's computer, or by executing JavaScript code on an infected website, once this website is loaded on the victim's browser. The cryptomining code starts working in the background, and usually the only sign of its presence is the slower performance and/or lagging.

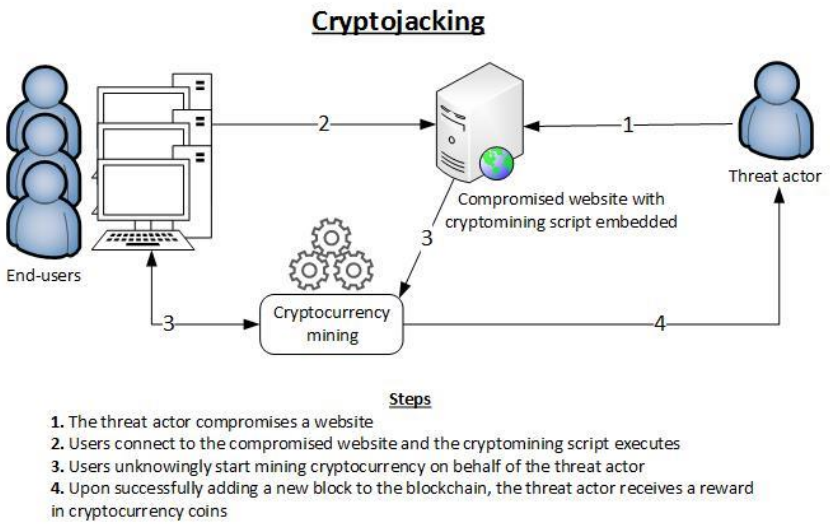

Figure 10. Cryptojacking (source: ENISA, 2017)

Challenge:

Cyber criminals are always on a lookout for cheaper way to mine cryptocurrency, since the process is long and expensive to run (e.g., higher electricity bills, expensive computer equipment). The more computer equipment and devices the user has working for him, the faster the "mining" of coins can be. This is the main reason why cryptojacking is so popular among cybercriminals.

Cryptojacking is typically performed through using malicious phishing emails, which install cryptomining code on the victim's computer, upon clicking on a link in the email or downloading and running an attachment, containing the harmful cryptomining script, or through using a web browser miner whereby the cyber criminals inject cryptomining script on a website or a harmful ad, which can be placed on various websites. If the user, visits such website or clicks on such an ad, the harmful script is automatically executed and the cryptomining starts to work in the background, usually, even though the harmful code itself is not stored on the user's computer. In both these cryptojacking methods, the cryptomining is done without the victim's knowledge, but there may be some signs to look for, such as high processor usage, unusually slow response times and lagging, overheating of user's hardware, and fast battery draining on mobile devices.

Mitigation:

To minimise the risk of cryptojacking, the following recommendations should be followed:

- Since the main method of malware delivery are the phishing attacks, it is recommended to organise security training in each organisation; however, these trainings will not be effective against auto-executing cryptomining scripts, executed by visiting infected websites.
- Antivirus software and ad-blocking or anti-cryptomining extensions (all obtained from reputable providers) should be installed on web browsers. Some of the antimalware solutions on the market have excellent capabilities to detect cryptomining scripts. Scans should be run regularly on all mobile and desktop devices.
- Antivirus software should be kept up to date. Once an infected web page is identified, it should be blocked also for other users in the organisation.
- Even though mobile devices are not the primary attack target for such cyber criminals, due to their limited processing power, it is recommended to also use a mobile device management (MDM) solutions so as to better manage what is on the organisation's mobile devices in terms of apps and software; this solution is usually applicable for larger organisations.
- For complete protection against Javascript attacks, JavaScript can be disabled altogether, even though this will prevent the use of also legitimate websites.
- Domains that are suspects of cryptomining should be blocked.

None of those practices can guarantee defence against cryptojacking, however, keeping strict security policies and good sense, can minimise the risk.

Opportunities:

Even though cryptojacking scripts do not directly damage the victim's hardware or data it is still a significant threat that causes all sorts of problems, such as loss of CPU power, wear on the hardware, and high electricity bills. The advances in AI/ML techniques are generating opportunities also for developing more effective cryptomining malware detection method using AI-based static and dynamic analysis e.g., on sequences of opcodes and system call events (Darabian et al., 2020).

Fileless and memory-resident malware

As the malware authors make their own advancements against malware analysis techniques and antivirus technologies, a new avoidance technique called memory-resident, fileless malware has come into existence. These types of malware do not require an executable file and they are downloaded and run on the victim's computer directly from the source and into the memory. Their attack vectors start with exploiting a vulnerability in a browser or an online plugin and reside on the memory to do the malicious work. Since they do not need a file to run, general malware scanners and detection methodologies become useless.

Challenge:

This type of malware is very hard to detect as it works only on the memory, leaving no traces on the storage spaces, and steals other processes' address space to do their malicious work. Fileless malware is typically utilised by:

- **Trusted applications:** Fileless malware uses trusted applications in the memory, injects its malicious scripts using process hallowing, DLL & code injection, while also using the code of legitimate processes to create malicious actions with ROP and JOP chains.
- **Lateral movement:** The fact that fileless malware does not leave a trace on the file system, makes it even harder to detect in the kill-chain phases of lateral movement. As an example, injecting malicious code into powershell scripts can automate the lateral movement on a network.
- **Phishing emails and fraudulent websites:** Regarding the phishing techniques of the attacks, instead of utilising a malicious attachment, the attack can be conducted by providing a malicious link. Clicking on the link will result in running some malicious code on a vulnerable browser extension.

Mitigation:

Behavioural anomalies of plugins and browser activities, and the memory activities of such tools should be monitored. Unusual communications for these plugins are also needed to be logged and tracked for the identification of C2 servers and attackers. On a more theoretical level, a rule of thumb approach for understanding memory operations is to check the Process Environment Block (PEB) structure and cross-reference with the Virtual Address Description (VAD) structure of the kernel space of the memory. Tools that utilise the VAD structure and make comparisons with PEBs can be integrated as part of security measures. Scripts can be produced to take regular memory dumps and also to analyse those dumps for the mentioned comparison even with open source tools such as 'volatility.py'[1].

Opportunities:

This challenge has the potential to lead to novel detection techniques that work only on memory and on the behavioural characteristics of malicious codes.

[1] https://github.com/volatilityfoundation/volatility

5.2 Critical infrastructures

5.2.1 Lack of cyber situational awareness in national critical infrastructure and gaps in defence-in-depth architecture hacking

Legacy architectures in critical infrastructures not built for digitalisation are being connected to TCP/IP which is allowing the risk of cyberattacks. Lack of education and training, and difficulty in the implementation of security in critical operational environments is compounding the ability of national critical infrastructure operators to protect against sophisticated offensive campaigns. StuxNet, TRISIS, CrashOverride, Ekans are all examples of ICS malware that security controls have failed to mitigate.

Challenge:

In the past 20 years, a number of events, held in different regions of the world, had a devastating impact on essential and vital services required by the population. Unconventional threats, such as terrorist attacks, cyberattacks, natural disasters, and hybrid warfare actions are the main reasons that determined the development of a new critical infrastructure protection concept. Critical infrastructures were delimited from the ordinary infrastructures, through a procedure of identification and designation, supported by a phased legal framework implementation.

Nowadays, cyberattacks on critical infrastructures are on the rise; they are both more numerous and more sophisticated. These cyberattacks are aimed at vital sectors of activity, such as the energy sector, the transport sector, the financial-banking sector, etc., where attackers are exploiting technical, human, production, and security vulnerabilities. Deficiencies identified in the cybersecurity of critical infrastructures have drawn the attention of decision-makers and specialists to find solutions in several areas of interest, through a holistic security model.

The model below might be beneficial for the analysis of the critical infrastructures.

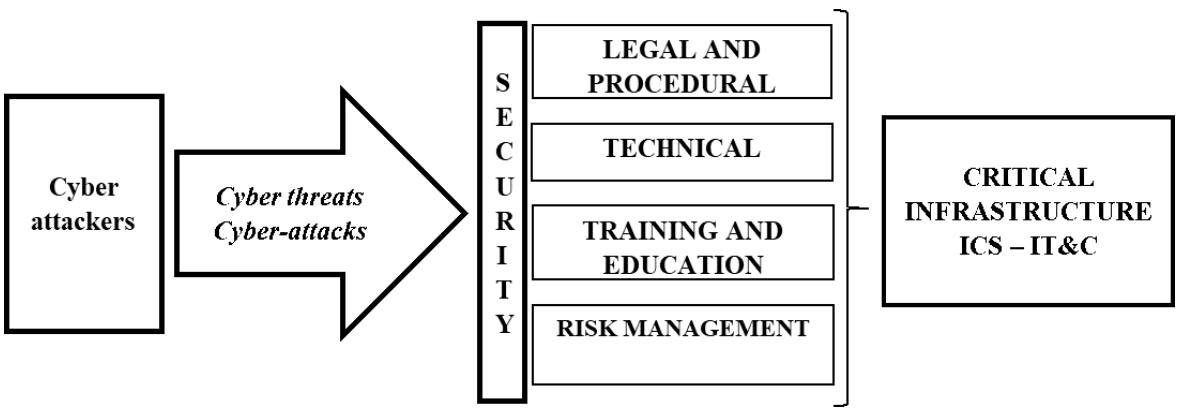

Figure 11: Cyberattack model

Cyberattackers targeting critical infrastructures are highly trained, experienced, and motivated individuals that might be supported by organised crime groups, terrorist groups, and even state actors. Usually, they do not act independently, but within an organised group that holds important information about the targeted critical infrastructure. There are several means of gathering information for a cyberattack, from disciplines such as HUMINT (Human Intelligence), OSINT (Open-Source Intelligence), SIGINT (Signals Intelligence), COMINT (Communication Intelligence), IMINT (Imagery Intelligence), etc.

Cyberattacks are offensive campaigns against critical infrastructure, aimed at disrupting or shutting down the respective infrastructure. *Communications infrastructure vulnerabilities* are the most common vulnerabilities of SCADA systems because they involve interruption, interception and modification of data traffic. The real-time operating systems are very susceptible to Denial of Service (DoS) attacks because minor interruptions can lead to significant loss of system availability. Attacks exploiting these vulnerabilities are performed on the stack of protocols that use the TCP/IP model (Zhu, 2014), in particular on the following layers

Network Layer

- Attacks of servers on the UDP port: attackers have access to the same debugging tools that RTOS developers have access to;
- Inactive scanning: MODBUS and DNP3 industrial protocols have scan functions that are prone to such attacks when encapsulated to run on TCP/IP;
- Smurf: In SCADA systems, if a PLC acts on receiving a modified message, it may be destroyed or send incorrect commands;
- Address Resolution Protocol (ARP) spoofing/poisoning: by sending fake ARP messages that contain false MAC addresses in SCADA systems, an attacker can confuse network devices, such as switches when frames are sent: to a fake node (packets can be intercepted), to an unreachable host (DoS attack), to another destination.

Transport Layer

- SYN flood: SCADA protocols have vulnerabilities that could be exploited by the attacker through methodologies as simple as injecting modified packets to cause the receiving device to respond or communicate in inappropriate ways and thus lead to loss of visibility or control of the device.

Application Layer

- At the level of the industrial protocols used in SCADA systems, there is no strong security control, such as DNP3, Modbus, InterControl Communications Protocol (ICCP), IEC 60870-5-101/104, and IEC-61850. Practically, there is no authentication on the source and the generated data. The write access and diagnostic functions of these protocols are particularly vulnerable to cyberattacks.

In addition, software and hardware vulnerabilities are also important. *Software vulnerabilities* are defects or errors in software products that, if exploited by attackers, can distort the initial purpose for which they were designed. Most of these vulnerabilities are exploited by buffer overflow attacks and SQL Injection attacks. The effect of these attacks can include resetting passwords, changing content and running malicious code. *Hardware vulnerabilities* are specific to different SCADA components (master servers, RTUs, IEDs), an example being the *hardware backdoors,* far harder to be detected because they are embedded in the circuits of the product and can be activated using some data sequences received on the communication channel. By exploiting these vulnerabilities, the attacker can gain unauthorized remote access to devices and can change their configuration settings, causing the devices to transmit erroneous values or disrupting the alarm management system, so that when an alarm actually occurs, the human operator is not aware of it.

Mitigation:

Training and education: The training of cybersecurity specialists in IT&C and ICS infrastructures (SCADA) laboratories needs to be performed by carrying out threat scenarios and exercises on critical infrastructure (red team-blue team), with the participation of security professionals from several critical infrastructures, with the same activity profile. Threat scenarios are an integral part of the *Operator Security Plan (LSO)* (C. Directive, 2008) of European and national critical infrastructure. Based on these scenarios, the risk analysis for the protection of the respective infrastructure is carried out. The education of personnel might be performed

through various methods, to include good practice guides for cybersecurity implementation, periodic training, information campaigns, online and offline courses, etc.

Legal and procedural: Compliance with European and national legislation (where critical infrastructure is located) needs to be ensured regarding both the protection of critical infrastructures and the cybersecurity of the embedded systems.

Protocols: Standardised protocols used in the field of IT&C (TCP / UDP), but especially industry-specific protocols (ICCP, Modbus, Fieldbus, DNP3, PROFIBUS, IEC 60870-5-101, IEC 60870-5-104, IEC 61850, OLE for Process Control Data Access (OPC DA), etc. need to be applied. These are standardised protocols and recognised by all major SCADA vendors.

Risk Management: The risk management process is underlying the Operator Security Plan. Once the threats have been identified and the threat scenarios are outlined, the risk assessment is made, based on one of the analysis methodologies. A proper and complete risk assessment must take into account the complex interdependencies of critical infrastructures, be comprehensive and holistic, addressing the institutional, organisational, managerial, and functional hierarchical structures, together with other determining factors.

Because the impact of a cyber incident in an ICS environment may include both physical and digital effects, risk assessments need to incorporate those potential effects, requiring a more in-depth examination of the following (Stouffer, Falco, & Scarfone, 2011): (i) impacts on safety and use of safety assessments, (ii) physical impact of a cyber incident on an ICS, including the larger physical environment, effect on the process controlled, and the physical effect on the ICS itself, and (iii) the consequences for risk assessments of non-digital control components within an ICS. Risk analysis for ICS might include methods such as Bayesian Networks (BN), Hierarchical Holographic Modelling (HHM), Tree Analysis (TA), etc.

Technical cybersecurity: The security of the automation, protection, and control systems, which serve critical infrastructures, must be efficient and strong. Cybersecurity solutions and services might include Firewall, IDS/SIEM, DMZ, antivirus, anti-malware, Honeypot, DLP, and DHS. A common practice encountered in critical infrastructure cybersecurity is to make a testbeds (Holm, Karresand, Vidström, & Westring, 2015) by creating a virtual copy of IT and ICS configurations and place them in isolated environments.

Opportunities:

Proactive network security is highly dependent on the quality and accuracy of the network data. While the attempts of malicious actors to compromise critical infrastructures are expected to increase constantly, the developments in the field of intelligent systems can aid in reducing their impact of cyber-attacks. In the big data era, we can no longer rely on the manual filtration and transformation of raw data into valuable information, but we need to shift to automated reasoning-based frameworks. Such frameworks will improve the cyber situational awareness of complicated and highly volatile environments such as the ones present at critical infrastructures.

Towards this end, a technique that can enable the automation of data processing, is the syntactic and semantic interoperability through the use of formal knowledge representation. The formal representation of raw data allows information to be indexed, hence optimised for queries, but also facilitates the use of reasoning algorithms to infer new statements (Sikos et al., 2019).

5.2.2 Illicit access to critical infrastructures using IoT flaws and hacking

The widespread of IoT devices and the migration of their use from the domestic user to industrial entities, including several types of infrastructures, brings new challenges to the field of securing critical infrastructures.

IoT devices typically include components that have limited resources, are connected to the Internet (usually wirelessly), and run limited software dedicated for the tasks they have to perform. The large number of devices and their limited functionality make them an attractive target for possible attacks.

Challenge:

It is within reach for anyone with access to the internet and relevant skills and motivation to use OSINT technology to collect information about connected IoT devices in critical infrastructure sectors. Open source search engines (e.g., Shodan, Censys) are able to find exposed and unprotected IoT that can be used to mount more complex attacks on the internal networks, turn on/off devices, or compromise the privacy of individuals.

The emergence of IoT devices in the fields of SCADA systems causes new challenges to be considered (Bekara, 2014):

- *scalability*: difficult to provide a reliable security solution (key management, authentication) for a very large number of objects spread over very large geographical areas;
- *interoperability*: interconnection of devices that have different communication protocols/stacks or the same communication protocols/stacks but with different characteristics: one with fully support, the other with partial support (example: DTLS with/without certificate support);
- *trust management*: creating a trusting relationship (necessary in the communication process) between different devices spread widely and managed by different entities;
- *mobility*: different mobile devices (e.g., smart transportation, smart grid devices, etc.) that need secure communications in different environments;
- *deployment*: devices installed in unsafe (remote) spaces easily accessible by anyone require the implementation of solutions capable of ensuring their physical and logical security;
- *legacy systems*: maintaining of legacy devices in IoT infrastructure, that cannot be replaced or cannot be updated with modern security measures;
- *constrained resources*: the limited resources of IoT devices generate challenges in the application of cryptographic security solutions;
- *heterogeneity*: adapting already existing solutions to obtain the communications security for various IoT devices, devices that have limited resources and different implementations protocols and communication stacks;
- *bootstrapping*: efficiently bootstrap devices with initial cryptographic security parameters (cryptographic keys, cryptographic functions/algorithms, etc.); and
- *latency/time constraint*: time-consuming operations (public key operations) might affect negatively fast, real-time data transmission (smart grid sector).

Mitigation:

Mitigation of IoT-based attacks to critical infrastructures can be achieved by:

- *incorporating "security by design"*: this solution could prevent some potentially fatal flaws; manufacturers must consider the challenges and possible vulnerabilities and apply adequate security techniques to all the components of their products (i.e., software, hardware, and communication components);
- *investigating optimal IoT-based system configurations*: the monitoring, control, software update/patching of the devices must be performed permanently; and
- *effective management of security incidents*: expanding the implementation of detection or prevention technologies to help decrease the number of security incidents; creating structures that can enhance the organisation's abilities to respond and dramatically reduce the Mean Time to Identify (MTTI) and

the Mean Time to Respond (MTTR); the organisation preparing itself for managing security incidents using various exercises and scenarios.

Opportunities:

One particularly popular line of IoT security research is IoT context-aware permission models, where collaborative models are designed to secure IoT environment from malicious actors. For instance, initial research (Yu, Sekar, Seshan, Agarwal, & Xu, 2015) proposed a policy abstraction language that is capable of capturing relevant environmental IoT factors, security-relevant details, and cross-device interactions, to vet IoT specific network activities. Further, the authors proposed a crowdsourced repository where IoT operators can share derived attack signatures, which deviate from the captured benign policies.

5.3 IoT, embedded systems, pervasive systems

The Internet of Things (IoT) is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. Many organisations are not necessarily aware of the large number of IoT devices they are already using and how IoT devices may affect cybersecurity and privacy risks differently than conventional information technology (IT) devices do. The cybersecurity and privacy risks associated with their individual IoT devices vary throughout the devices' lifecycles.

5.3.1 Access to IoT devices

The lack of security in many IoT devices allows access to many devices over the world. With more and more devices controlling several tasks and with the current trend of implanting IoT devices in human bodies, the problems and the possibility for cybercrime is growing exponentially.

Challenge:

For decades, the Internet has forged the world by connecting people. But for a few years now, this network has extended to objects thanks to IoT (Internet of Things). It is a transformation that concerns all areas of our life in society including the professional, public and private fields. The IoT promotes the emergence of new fields that were not connected to each other until now, such as smart sensors (e.g., water, gas, steam, electricity), mobility / ITS (Intelligent Transportation System), industry, manufacturing (production, factories), robotics, aeronautics, maritime, improving daily life / well-being (Well Being, Aging Well, Smart Living), health (eHealth), agriculture and food, energy, intelligent buildings, the environment, smart cities…

Examples of compromised connected objects include:

- Various sellers of connected locks whose equipment can be opened by capturing and replaying authentication sequences.
- Connected car models allowing varying degrees of control of certain remote functions, for example Jeep vehicles.
- Various appliances, from the refrigerator to washing machine.
- Different versions of IP cameras, connected baby monitors, and other recorders open on the Internet or by keeping the manufacturer's default password.

Beyond such anecdotal evidence, IoT devices offer an interesting playground for several reasons:

- Unlike traditional platforms which are much more heterogeneous, they have very stable and identical software platforms on all objects of the same type (same brand and models); this makes writing a hack

much more efficient, since it will be able to run on all vulnerable devices without much effort. The same vulnerability can therefore make it possible to take control of several thousand devices very quickly.
- Security is not a priority for many equipment manufacturers, who do not follow basic best practices by leaving default passwords and open ports on their devices without justification for the service rendered to user.
- There is little or no security supervision on these devices which are connected and then forgotten, as long as they provide the desired service.
- The difficulty of updating the systems and software of many connected objects makes infection, and therefore control by the attacker, much more durable over time.

This apparent ease of hacking for attackers can be explained in several ways. The economic pressure on companies to be the first on the market and to present real innovation often comes at the expense of a certain number of controls. Security is considered as a brake on innovation and development, and relegated to a later version. Moreover, the tendency to develop new objects based on market components, sometimes devoid of security, may also explain this lack of consideration of security in the manufacturing of objects.

Overall, the security problems encountered by IoT devices are explained by the lack of integration of security during the design phase, the lack of culture on the IT security of the design teams, but also by the lack of standards and solutions proposed by IT security specialists, which could allow security principles to be applied in a simple manner to all projects, from design to manufacture and production.

Mitigation:

IoT are complex heterogeneous environments, requiring the implementation of a security covering the whole ecosystem which includes the connected device, the cloud service platform which retrieves data, and the connectivity between devices. Securing IoT devices must therefore rest on 5 pillars which are: (i) Protection of the device, (ii) Protection of communications, (iii) User protection, (iv) Equipment management, and (iv) Ecosystem supervision.

Protection at device level: IoT are devices with closed environments. The customer is often unable to add a layer of security if this has not been provided by the supplier. For this reason, security must be thought of from the design of the object (secure by design) and no longer be seen as a complementary, but rather as an integral part of the project. The security industry must bring a new approach by bringing in technologies allowing integrity, encryption, authentication, intrusion prevention, security updates, etc. In addition, IoT devices are sometimes deployed in places without the possibility of strong control over physical access. This opens the door to reverse engineering attacks. It is therefore advisable to harden the system by including for instance a white list of the authorised applications, partitioning these applications, restricting the communications in entry and exit, setting up a concept of secureboot, etc.

Protection of communications and authentication: This protection involves data encryption and authentication of communications. The implementation of a trust model based on certificates allows the interoperability of the various components of the architecture of an IoT service through the use of strong certificates managed by perennial certification authorities. The implementation of mutual certificate-based authentication is now facilitated by many existing standards, such as SCEP, or OCSP allowing OTA management of certificates.

User protection: The General Data Protection Regulation aims to enforce the protection of personal data within the European Union, with the stated objective of giving citizens back control of their personal data, while simplifying the regulatory environment for businesses. This new regulation provides a clear answer to consumers worried about the use of this data.

Equipment management: These devices will have to be updated via OTA (Over The Air) processes. The benefits of good update management go beyond simple security.

Ecosystem supervision: A complete threat control strategy requires the implementation of a security analysis module to add detection functions to the protection functions described above. These analysis modules can rely on the telemetry retrieved from the IoT devices and network equipment deployed in the infrastructure to give visibility on what is happening throughout the ecosystem.

Opportunities:

Despite the measures described above, IoT environments require exploring new ways to offer better guarantees of security, particularly in order to allow connection to critical environments.

Declaration of objects: One of the emerging paths to ensure better cohesion of connected objects and their security would be an approach based on the obligation for each object connecting to the ecosystem to go through a declaration step to announce the services used and interactions expected with the rest of the infrastructure. This vision today requires the development of standards and a commitment from industry which has yet to be created.

Detection of anomalies: Since IoT environments are constrained environments, deviations from what has been implemented can be quickly identified. The idea of anomaly detection is to include dedicated analytical modules capable of detecting all these deviations as quickly as possible. The wide variety of industrial environments and IoTs protocols can make this problem difficult, but new techniques based on machine learning offer promising avenues.

User education: At the consumer level, restoring confidence requires better education and better information. The education must be done on the precautions of use to be taken in the installation of connected objects and can be done during the activation of the service by imposing precautions of use like the modification of the default password. It can also be done through the development of a solution bringing visibility to all of the objects connected to the system in order to guide the users in taking control of the data and services used by these objects; this also requires better information on the data used by these services. Here, standards are to be developed so that each IoT service, particularly those intended for the general public, can communicate in a homogeneous manner on the use made of personal data.

5.3.2 IoT botnets

There was a multitude of IoT devices already on the market far before the discussion on IoT security even started. These devices had a stealthy entrance since, in the early days, they were devices with minimal communication capabilities limited to “local applications". In this case, the threats were mainly highly motivated actors targeting specific installations and industrial sites. The breakthrough to mass-market happened when the devices became IP-enabled, essentially converging these micro-systems, micro-services, and the Internet. This enablement has been done on top of existing hardware architectures and code-bases and coincided with the development of malware and exploitation tactics.

An IoT botnet is a group of compromised IoT devices such as generic sensors, home appliances, wearables, medical, security and industrial devices which are being used as attack vectors. They are controlled by command and control software which makes possible directed and synchronised targeted behaviour.

Challenge:

Organisations do not typically consider IoT botnets as an imminent threat. IoT devices are mostly low-cost devices, scattered inside the networks, which makes them pass under the radar of organisations. These devices lack of basic security and privacy functionalities, sometimes have clear text protocols and unnecessary open ports, and often lack of maintenance support from vendors for fixing issues. More than often, IT departments do not even have an inventory of IoT devices deployed in their network and do not have the proper tools to monitor and maintain them since the traditional IT ecosystem is not suitable for this use case. A specific threat is counterfeiting when measures against physical tampering are not in place with no encryption and integrity checks.

Application DDoS: Application layer attacks or layer-7 DDoS attacks refer to a type of malicious behaviour designed to target specific systems, servers or services so that they become unavailable. By exploiting the aforementioned IoT devices' vulnerabilities, attackers inject malware into IoT devices to turn them into botnets. The challenge here, different from a "classic" botnet, is the sheer number of diverse IoT devices which can be relatively easily enrolled in the botnet army and used for the massive scale attacks. Notably, there is a market for creating and selling IoT botnets. Therefore, the number of DDoS attacks based on IoT botnets has seen a surge in the last years. One of the most famous IoT malware is Mirai, responsible for a massive 1.2 Tbps attack on OVH and Dyn in 2016. This malware is not very sophisticated because it uses default, weak configured Internet accessible devices. Other malware such as BASHLITE, LuaBot, Remaiten exploit specific issues with technologies used by devices.

DDOS burst attacks (hit-and-run DDoS): Hit-and-run DDoS is an DDoS attack in which the attacker generates, using command and control software, via the botnet devices, non-legitimate traffic in short bursts over a period of time. It could span to days, and even weeks, and it tries to reduce, restrict and prevent accessibility to systems and services by bandwidth depletion, consuming connection state tables (protocol attacks) or application layer resources (HTTP GET/POST and slowloris attacks).

This type of attack aims to work around anti-DDoS software and techniques which are used to mitigate persistent DDoS. Anti-DDoS software works by implementing complex detection techniques, such as activity profiling, change point detection (changes in network traffic statistics and flow rate), or wavelet-based signal analysis (in terms of spectral components). The job of such software is made even harder when the attack bursts are varied in time by changing characteristics or attack types. This is not specific to IoT botnets, but this kind of networks are increasingly being used as attack vectors. According to Corero 2019 Full Year DDoS Trends Report (2019), in 2019, the duration of attacks which lasted less than 10 minutes accounted for 85% of attacks and only 9% lasted more than 20 minutes. Also, there is a 25% chance that an organisation will be attacked again within 24 hours.

Reflection (spoofed) amplification attacks: The attacks are getting more and more complicated and this type of attack is proof to that. Reflection or spoofed DDoS is performed by using multiple intermediary, usually legitimate, machines that contribute to the actual attack against the target server or application. The attacker directs intermediary victims to send packets (TCP) to non-compromised machines or reflectors with the target's IP address so that they try to establish legitimate connections. This triggers the reflectors to send large amount of traffic to the target as they believe it was the target who initiated the connection thus depleting its resources. It is a complex attack which involves exploitation of vulnerabilities of knows protocols (e.g., DNS, NTP, SNMP) and makes it very difficult to identify the attacker when the application protocols are combined in a simultaneous attack. The DDoS reflection is a multi-hop attack because it uses a number of intermediary machines until it reaches the reflectors and then the target machine. The primary target seems to be attacked by the reflector servers and not the actual attacker.

Mitigation:

Organisations do not typically consider IoT botnets as an imminent threat: The mitigation of such threats starts with applying the security best practices, which nowadays to some degree exist in most responsible organisations, also to IoT devices. The first level of defence has to be established internally, since it is very difficult, and it takes time to impose stricter regulations to the IoT device vendors. This could be done by having an account of all IoT devices deployed in an organisation's infrastructure, by adding them in the infrastructure diagrams (usually omitted from them) and limiting (or cutting considering the risks) access to and from external world (to Internet services). Organisations also have to design their own regulations to cover maintenance of IoT devices, which are not very different from the classic resources (network devices, operating systems, applications); the same activities have to be performed, e.g., changing default configurations, install security patches and updates (if any), monitoring and profiling the traffic to and from them. There are, of course, specifics, but these are mainly related to the application ecosystem utilised to accomplish this. Another specific item is the special attention to the acquisition process since the IoT devices are easier to counterfeit or tamper with. These generic advice could become a compliance framework or updates to existing security regulations enforced by governments and public institutions.

Application DDoS: The classic approach to mitigate application DDoS includes increasing bandwidth to absorb the traffic, load balancing, throttling at domain boundary (on routers), so that the servers can handle the traffic, and ultimately dropping requests. Another technique is to make the requester solve a difficult puzzle (similar to a CAPTCHA) that require a lot of memory or computing power before sending the actual request. It may determine the bot to stop making the request. All these strategies require planning, additional resources or voluntarily (temporarily) reducing the service level; of course, this will include also legitimate users.

DDOS burst attacks (hit-and-run DDoS): As seen in the previous sections, the classical countermeasures to DDoS are more and more outpaced by new attack methods, as it is the case with hit-and-run DDoS which not only can vary the duration and load of the attack, but it can also change the DDoS attack types. Even if the firewalls at the network boundary do have profiling capabilities, it is still very difficult to detect it and filter it. Novel technologies must be employed and machine learning is a valid option, which has started being applied also in this field. Advanced web application firewalls are using Behavioural DoS modules (BDoS) to detect attacks, try to identify attack sources and filter the bad traffic. The basic idea behind it, is to detect traffic anomalies by constantly learning the traffic behaviour and comparing it to an evolving baseline. This is done by machine learning algorithms or by calculating traffic signatures which aim to isolate traffic characteristics deviations from the current control baseline.

Reflection (spoofed) amplification attacks: The same measures apply also to reflection amplification attacks. Combined techniques based on filtering and BDoS make possible the containment of these attack which otherwise are very hard to deal with in the same time with maintaining business continuity.

Opportunities:

There are two non-concurring paths for opportunities related to IoT botnets threat: (i) improve the overall security of IoT devices by regulations, new standards, and new technical approaches for low-resource, cheap devices, and (ii) develop and improve behavioural protection based on Artificial Intelligence. The first path seems to be natural and it is the path that most technologies have taken before. The security architecture has to be improved by vendors by effectively balancing the cost and simplicity. The second path is a more complex approach, but which provides a wider coverage of attack types. This path is driven by the need of protection against ever-evolving threats which are more and more complex. The latter opportunity is also driven by the normal expectation that AI technologies will be used in conducting the attack itself. It is very easy to imagine the malicious actors deploying such technology to test and learn the response of systems which try to mitigate DDoS and then to develop new ways to work around them.

5.3.3 Traditional host-centric security solutions are inadequate at protecting IoT devices

Considering the challenges related to IoT botnets in which actors are increasingly using IoT devices for their DDoS attacks, it is obvious that it is relatively easy to build such an army of bots and hence that current security solutions are inadequate at protecting IoT devices.

Challenge:

While traditional IT systems have well-established policies and tools ecosystem, the IoT world is yet to be in the same position. Moreover, the translation of the same policies and tools from the traditional IT to IoT is not straightforward and it is often not suitable. Host-centric security solutions (e.g., antivirus software, firewall, update and patch clients) are not suitable for hardware constrained devices which do not offer the minimum security support. Security by design principle is not, still, part of the development process of a large part of today's deployed IoT infrastructure. This is mostly due to the way the IoT devices have evolved as cheap, low-power, even disposable devices.

The following concern areas are challenges for the current IT security ecosystem when applied to the IoT domain:

- IT security policies definition: many IoT devices cannot be directly contacted unless using a dedicated gateway which IP-enables them.
- Monitoring: the IoT world is very diverse which makes it very hard to compile traffic signatures or profiles.
- Policy enforcement for deployed systems: IoT devices (including IoT gateways) are low-resource devices and usually run pseudo-operating systems; such an enforcement would have to be external to these devices.
- Requirements to have standard compliant network devices, such as PCI-DSS (The Payment Card Industry Data Security Standard) or GDPR (General Data Protection Regulations): this would require most IoT devices to be excluded.

Mitigation:

Any mitigation strategy would have to start with the IoT manufacturers. Security cannot be external to the IoT world; you cannot fix the problem only by deploying new security devices, probes or sophisticated traffic inspection. Security features have to be embedded in the IoT infrastructure and this can be enforced by required compliance to a minimal dedicated security framework.

A new method to approach these matters (but not yet fully developed) is using Software Defined Networking (SDN) and Network Functions Virtualization (NFV) technology. Essentially, SDN aims to make network configuration dynamic by separating network control plane (routing process) from the data plane (forwarding of network packets). NFV aims to have entire network functions virtualised (e.g., firewalls, WAFs, IDSs) and run in virtual machines which can be chained to create complex communication services.

Based on these concepts already used in current networking, the idea is to create "micro-boxes" to cover the data plane, specifically configured for types of IoT devices. These micro-boxes can be rapidly instantiated and reconfigured for the necessary forwarding rules. The control plane is centralized and in this way a better control of IoT traffic could be performed.

Opportunities:

The opportunities for innovation are open since there is a lot of room for improvement along two complementary paths: (i) one is *internal* to the IoT world, based on developing dedicated software infrastructure, such as operating systems, libraries, protocols, micro-firewalls, and re-utilisable hardware with security features by design, and (ii) the other one is *external* to the IoT world, based on developing micro-security functions, routing capabilities which can be deployed on top of existing IoT infrastructures.

5.3.4 Constantly increasing attack surface

The cybersecurity aspects, related to the Internet of Things (IoT) devices and networks are gaining further importance, following several high-profile hacks during the last couple of years. Connecting services and devices can have unexpected consequences, especially against the backdrop of industries with no established traditions in terms of mitigation of cybersecurity risks. A stark example of this was the Finland 2016 denial-of-service attack (DoS attack)[2], which managed to disable residential automated heating systems in apartment blocks for more than a week. In any case, attacks against IoT devices, embedded systems, networks and applications are commonly used to exploit existing vulnerabilities in the IoT paradigm, in order to infiltrate and attack a larger network.

Connected devices include a wide variety of devices and diverse applications, which offer a plethora of competitive advantages; however, IoT devices and applications are not primarily designed with consideration of common cybersecurity issues or aspects. Therefore, the likelihood of an increase in high profile incidents, security and privacy problems rises exponentially, with a prominent focus on data and network confidentiality, integrity and availability, as well as issues, related to the authentication, access control and accountability of the IoT devices, networks and applications.

What we currently witness, as a prominent issue, is the multi-layered expansion of the attack surface of the IoT paradigm. The increased prominence of IoT devices, along with their, heterogeneity, complexity, interoperability, mobility, and distribution of entities (smart objects, controller, user, and services) expand the attack surfaces in the interconnected things' networks (Covington & Carskadden, 2013).

Challenge:

Multiple challenges arise in terms of cybersecurity in consideration with the ever-increasing attack surface of the IoT paradigm. Some of those challenges stem out of the resource constraints of the IoT devices, software and networks, which makes the application of standard cybersecurity mechanisms inherently difficult or even impossible. Furthermore, the heterogeneity of the IoT devices presents an enormous challenge in terms of coming up with standardised approaches to ensuring the confidentiality, integrity, and availability of IoT devices, applications and networks. Some IoT devices perform as a hybrid configuration and act as collectors, processors and controllers of data, whilst others perform only one of those functions and a standard solution will not be able to fit the diverse context of the devices.

Considering IoT devices, the challenges leading to an increase of the attack surface are mainly the by-design limitations, which produce a complex environment for the deployment of standard cybersecurity mechanisms. Such challenges, for example, are the IoT devices inherent m*emory and computational power constraints*. In comparison to traditional computation systems, such as PCs, IoT devices are designed with limited memory, which makes the traditional security schemes and algorithms, which are not designed with memory efficiency

[2] https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/

as main priority, difficult to apply. Furthermore, security algorithms need to be further customized per IoT device, as their standard scheme and configuration is in general not applicable to the IoT paradigm.

Additionally, having into consideration the inherent mobility and the discussed scalability and variety of the connected devices, the attack surface constantly expands with issues, such the by-design connection to networks with no prior security configuration. Furthermore, more and more IoT devices are designed to connect and exchange packages in proximal networks, through non-IP protocols, while at the same time using the IP protocol to communicate those packages to a cloud service or another application. Most traditional security paradigms are proven to be unsuitable for such multi-protocol communications and increase the attack surface by leaving a communication protocol possibly unprotected. By the same token, most security paradigms for communication protection do not envisage, or are too resource-exigent to deal with the topology dynamic of the IoT paradigm, which further multiplies the possible attack vectors of the IoT ecosystem.

Mitigation:

The mitigation techniques, against the backdrop of the complex diversity of the IoT security challenges, are diverse, extensive, and not standard for all IoT solutions. Several critical mitigation strategies, however, could be drawn out as generic guidelines for securing IoT systems.

The first strategic decision to mitigate the impact of the constantly increasing attack surface is to embrace the security-by-design principles when developing new IoT technologies. Following such an approach, the alternate security tactics and patterns are first being considered, and among them, the best practices are selected and enforced by the architecture design, and then used as guiding principles for the IoT developers. Besides the security-by-design principles, there are several strategies for security hardening for IoT that are widely recognised as successful and impactful.

- End-to-end security: IoT devices generate huge amounts of sensitive information, which is shared, communicated, potentially analysed, and stored by external entities. In IoT, the two major connection points, where the security of this sensitive information is absolutely a paramount are the point of contact between the “user” and the “thing”, and the point of communication between that “thing” and another “thing”.
- Dynamic security patching: A definite must for the in-time mitigation of potential vulnerabilities and a shield against the exploitation of known vulnerabilities.
- Identity management: Along with the topics of authorisation and authentication, an effective identity management scheme is paramount for the protection of the IoT devices against adversaries, while still providing access, or proving identity to trusted users, networks or nodes.
- Key management: Key management systems, designed with the power and memory constraints of the IoT devices and the device protocol stack, are crucial in order to maintain a safe key and to distribute it between trusted nodes.
- Energy efficient security model implementation: Although still this field is heavily under research, several energy-efficient cryptographic methods have been implemented specifically for IoT devices. Other security algorithms and systems are also being designed with the intention to harden the security of the IoT paradigm.
- Intrusion prevention and intrusion detection, monitoring and control: Establishing mechanisms for the monitoring and control, as well as the reporting of deviation from standard behaviour and possible attacks. For industrial systems, such as SCADA, the reliable handling of the alarms generated by the control system monitors and sensors and the triggering of the response and mitigation actions consequently to current requirements might be a matter of national security.

There is currently a number of IoT security guidelines and security standards available, which discuss the above-mentioned issues in depth and are a recommended literature, when it comes to mitigating the increasing attack surface and ensuring reliable and resilient usage and development of IoT devices and applications.

Opportunities:

Multiple opportunities for research and innovation are available when it comes to shrinking the attack surface for IoT and embedded systems. Such include, but are not limited to:

- Development of lightweight security schemes, that take into consideration the parameters of IoT devices and applications or embedded systems.
- Development of mobility resilient security algorithms for IoT devices.
- Security for both wired and wireless medium properties.
- Forensics: The field of digital forensics is currently facing a number of challenges when it comes to the IoT paradigm. Firstly, within the IoT, a number of forensics schemes are employed, such as device forensics, cloud forensics, and network forensics, which requires a vast plethora of skills, knowledge, and capabilities. Combined with the enormous data sets, which are primarily handled by data centres and external entities, digital forensics specialists have to overcome multiple hardships to be able to obtain evidence and investigate.
- Security for handling big data: Embedded systems and IoT devices alike, generate huge amounts of heterogenous data, which needs to be securely handled, including during transfer and at rest, without compromising the performance of the system. Such systems are still under development and standardised solutions and governance models are at a generic level and are not applicable to multiple contexts.

Most of the critical security issues, related to cyber-physical systems, are still not widely addressed, not only in terms of awareness, but also through unified efforts among developers, engineers and architects of such systems. Prominent security issues related to the expansion of the attacks surface, as well as opportunities for research in the field are further structured and thoroughly discussed in the previous and the following chapters of this document.

5.3.5 Anomalous behaviour is hard to detect

Challenge:

IoT are present in our daily lives. They are connected to our private networks and our businesses (e.g., video surveillance, thermostat, watches, alarms, medical devices, etc). Unfortunately, many manufacturers focus on innovation to the prejudice of robust security. Some malwares therefore use the security weaknesses present in these ubiquitous devices to build botnets or infiltrate a company. Following the example of the Mirai bonet, released in 2016, a botnet of approximately 145,000 connected cameras launched DDOS-type attacks against OVH, the European leader in cloud hosting or the DNS service "Dyn". Mirai and the new generations of botnets inspired by it, regularly scan the Internet to connect to IoT's administration interfaces which are left open, protected by weak passwords, or vulnerable to unpatched / 0days exploits.

Hackers having taken control of the equipment, can easily do lateral movement within internal network or use this resource to compromise new equipment or target other victims. Traditional approaches in IT consist of setting up a defence in depth and multiplying detection and collection tools. Installation of antivirus and EDR (Endpoint Detection & Response) on workstations and servers, Intrusion Detection System in network outage, uploading of all logs to a SIEM for analysis and correlation.

Unfortunately, the deployment of antivirus software on connected objects is not easily feasible due to their low computing power. In addition, antivirus editors rely on detection bases that are not easily maintainable due to the large number of manufacturers and the heterogeneity of the IoT ecosystem. Learning of a normal activity should, in theory, make it possible to detect a deviant behaviour, however IoT evolves and integrates a certain adaptive "intelligence" which will change its behaviour according to events detected or actions carried out by users. Machine learning does not appear to be the best weapon to detect abnormal behaviour in IoT.

Mitigation:

Faced with these problems, traditional techniques are not adapted. The implementation of an open honeypot on Internet, able to emulate an IoT equipment and to record all the actions and attacks carried out against the emulator could be the beginning of a solution, however, a private individual or a company would not have the means to set up and maintain an infrastructure emulating thousands of equipment. The solution could therefore come from sharing patterns with community. The solution called "Honware" could facilitate the implementation of this infrastructure by using the original firmware applications and their configurations which means that every phase of an attack can be monitored and fully understood (Vetterl & Clayton, 2019). From malware capture and analysis, YARA and IOC rules can be written and easily shared with partners or publicly. The more sharing there is, the more mature the detection of abnormal behaviour will be.

Opportunities:

As firmware is not systematically made available publicly by manufacturers, a database could be created to bring them all together, requesting the contribution of manufacturers. A tool, dedicated to the sharing of detected rules dedicated to the IoT could be developed or adapted from existing frameworks.

5.3.6 Cross device dependencies

Like typical network devices, IoT devices can communicate explicitly with each other. For example, a networked thermostat (e.g., NEST) can control the air-conditioning system in a smart home. However, unlike traditional devices, IoT devices can also be coupled through the physical environment leading to implicit dependencies. For instance, a temperature sensor can be connected to a service like IF-This-Then-That (IFTTT) to open windows to cool down a space when the air-conditioning is not active. Thus, an attacker could compromise the smart plug (e.g., Belkin Wemo) to turn off the air-conditioner in a room and trigger a temperature increase, which would, in turn, cause the windows to open and create a physical security breach. Such cross-device dependencies are quite common.

Challenge:

Automation and dependencies applications (e.g., IFTTT) are widely implemented to make interactions with IoT devices simpler and more convenient for the user. These applications provide an interface allowing a user to control their networked smart devices through the use of triggers and events. The use of these applications becomes more frequent as the IoT becomes more easily accessible with the number of devices that a user can have. These devices can be door bells, lights in your home, central heating devices such as HIVE, as well as your social media accounts, which can be linked to these apps to help make tasks repetitive and tedious on these less difficult platforms. These applications make tasks easier and help control many monotonous events on a daily basis, but they do not have sufficient security to secure the data and devices of their user databases. This interdependence between IoT devices can be exploited by attackers to gain access to the entire ecosystem. Many IoT devices (e.g., smart locks, CCTV cameras, perimeter security sensors) are installed outside the home, exposing them to illegal manipulation. Therefore, it is very important to limit these device-to-device interactions and dependencies in the IoT ecosystem in order to reduce the possibilities for an attacker to cheat the entire system.

Mitigation:

Today's IT security ecosystem, which relies on a combination of static perimeter network defences (e.g., firewalls and intrusion detection / prevention systems), a pervasive use of defences based on the end host (for example, antivirus) and vendor hotfixes (for example, Patch Tuesday), is basically ill-equipped to handle IoT

deployments. Specifically, the scale, heterogeneity, use cases, devices and IoT provider constraints mean that traditional approaches do not respond well to the security principles that should be in place.

To use the IFTTT example, there are undoubtedly many advantages to using it and integrating it into the daily use of IoT, but there are potential areas of vulnerability. When it comes to security, IFTTT uses Secure Socket Layer (SSL) to encrypt information transmitted on their website, which is an industry-approved way to protect information transmitted while in transit over the internet. To use the IFTTT, you must grant it numerous authorisations, such as camera control, coordinates, location data, access to your applications (authentication tokens), etc. The fact of storing and having so much information in one place opens the door to hackers. Thus, if a hacker were to access this database, he would have access to all the platforms and services to which a user has registered to use the IFTTT application, without having to hack each of them. Also, there is no way to check or control the triggers before they happen.

In order to reduce dependencies between devices, protection countermeasures must be applied, such as access control, information flow control, 2-factor authentication / validation, etc. Access control and information flow can be based on the applet principle (in the IFTTT convention but the concept is found in competition) exclusively private or public. This segregation of accesses and flows thus makes it possible to break private flows towards public environments which are often poorly controlled.

Security zones can also be defined, e.g., (i) trusted network for internal devices in the immediate environment of use (home, business), (ii) limited trust network for devices external to the environment of use but whose flows do not pass over the internet (external cameras, doorbell, proximity sensor, etc.), and (iii) public network for devices whose flows pass through the internet and whose physical proximity is not possible. Without reducing security measures between environments, we can then consider that the more we move away from the physical zone of presence, the more security must be increased, and the less the flows will be trusted.

As indicated previously, a device-to-device dialogue from a weak (so-called public) security environment to a trusted environment should only be possible if the latter is explicitly approved either upstream or through real-time 2-factor validation. In addition, it can also be interesting to build a network of trust between the devices. So when adding a device, its authenticity or legitimacy on the network must be able to be validated by another counterpart before establishing a communication link. This proof of authorization provides assurance that a peer has the power to communicate with another peer and can take action.

Opportunities:

In order to ensure consistent security for all connected devices at all times, networks should be able to identify connected devices. Using device information, gateways and access points (APs) should be able to automatically retrieve and apply the required set of traffic filtering rules to secure all connected devices. For example, reconfigure the network to ensure that a Smart TV cannot send video and audio streams from the microphone and webcam to an arbitrary server at all times. In the near future, machine learning could apply to this type of security context. Indeed, automatic learning algorithms can analyse network traffic to form traffic classification models using a large number of connections and contextual parameters.

5.3.7 0-day on CPS

CPS (Cyber-Physical Systems) are going to be massively deployed in the near future in businesses and even in critical sectors, such as transportation (railway, aeronautical), energy (power plants, power grids) and health industry. Thus, all these new components are the object of new and active attention from hacktivists. The mirroring side is the urgent need to detect and protect the businesses. A zero-day attack is an attack when the

vulnerability is exploited before or at the time the vulnerability is published. Regarding the importance and the number of deployed CPS, it appears those components contain a critical potential impact on the global system.

Challenge:

CPS components embody a direct link between the real world we are living in and computing systems and therefore a failure in that type of component will then consequently have an impact on our environment. It could be an electric disruption in factory premises, airports, hospital. It could be an integrity failure in a medical device. It could be a configuration change in a railway switching system. Through all these examples, it could lead to potentially fatal issues. A 0-day exploit combines the high potential impact and the lack of defense against the vulnerability.

Examples of applications where CPS components are deployed and associated with likely attacks include the following:

Medical Devices: One of the security flaws comes from the fact that some manufacturers allow interaction between a smartphone and the CPS equipment. An insulin pump, for example, exchanges data and instructions using unencrypted wireless technology. Some researchers have demonstrated the ability to take control of the equipment within a radius of about 10 meters and change the dose of insulin to be delivered, which could be lethal to the patient.

Smart Cars: Intelligent vehicles have on-board computers capable of collecting and analysing data from thousands of sensors. They are able to decide and react to an unexpected event in order to avoid an imminent accident (e.g., emergency braking, pedestrian avoidance, etc.). Intelligent vehicles also have a high level of connectivity (WiFi, Internet, GPS). This connectivity then opens up opportunities for hackers who would like to take control of the vehicle remotely. As a matter of fact, the vulnerabilities of several car manufacturers have been demonstrated. For example, two hackers managed to hack a Jeep vehicle remotely. After hacking the WiFi, they were able to access the multimedia management system theoretically not connected to the CPS. By patching a firmware they were able to access the CAN bus, giving them the means to act on any equipment and CPS in the car (brake, accelerator, steering wheel, etc.). This type of attack could be used to steal vehicles, injure or even kill the occupants of the vehicle or run over pedestrians (Humayed, Lin, Li, & Luo, 2017).

Mitigation:

Several avenues can be set up to limit or detect 0 days exploitation, including (but not limited to):

- Use of VPN to access field devices;
- Segmenting the network by restricting lateral communication to necessary and expected traffic in order to reduce the impact of a breach;
- Installing sensors on network, storing, and monitoring every single log available into SIEM; AI and ML may help to learn normal network traffic and detect deviation;
- Setting up honeypot to identify 0 days exploitation and sharing signatures through IOC / YARA rules;
- Changing all default password if possible;
- Applying security patches; and
- Disabling wireless technology or input port (e.g., USB, Firewire, etc) if it is not necessary.

Opportunities:

CPS devices manufacturers could consider several features, such as use of encryption to communicate with device, enabling authentication mechanisms, implementing protection against replay attacks, use of hardware-

based solutions such as Trusted Platform Module (TPM) to maintain privacy and integrity of device software and firmware, and data storage encryption.

5.4 Network and distributed systems

5.4.1 Anomalous events of unknown origin in complex systems

Detection and analysis of abnormal behaviour in network and other complex systems is among the highest priorities of intrusion detection and prevention systems. They typically work by monitoring the network/system and apply certain rules according to previous attack patterns given to them.

Challenge:

Supervision and control of complex systems, such as these related to industrial processes, is usually based on different proprietary technologies, used in different scenarios, ranging from control processes, transport, power generation, water distribution, environmental controls and others, become very vulnerable to current cyber threats. The key to implementing such complex systems, like SCADA, is to design and define robust and reliable handling of the alarms generated by the control system monitors and sensors and to trigger the response and mitigation actions consequently to current requirements. In many of these cases, defence against cyberattacks and threats was not considered as an important issue, and as a matter of fact, the proprietary nature of the implemented technologies and protocols, together with their niche application and the inherent protection against critical failures, were considered to be sufficient to counter cyberattacks, especially given the additional physical isolation of the critical infrastructure networks from the Internet and the physical access protection systems.

Contemporary digital systems are very often required to process in (near) real-time a large amount and variety of data, the sources of which can be distributed to a large extent since monitoring and logging processes are often dispersed in complex systems. The load on the system, especially in response to attacks, will vary significantly over time. Distributed, agile computing platforms are thus required to provide the computing power needed to counter attacks on the complex systems. These requirements can be met through the integration of cloud computing technologies and, in particular, by hybrid cloud technology.

In the last several years, many boundary conditions have changed dramatically. On the one hand, for obvious cost and market reasons, industrial control processes systems have taken a significant step towards the gradual introduction of common low-cost hardware. Furthermore, the massive deployment of low-cost and flexible IoT technologies is considered to have an unprecedented impact on industrial processes and critical infrastructure. Such devices and technologies are based on the same standard Internet protocols and ICT solutions and systems used in regular networks and systems. As such, they are already thoroughly investigated and targeted by attackers who may introduce into a complex system the same vulnerabilities and attacks that are widely used in the Internet.

Increased connectivity and integration with office and corporate systems, as well as the combination of devices, including personal devices owned by employees, have opened the door to many infiltration paths, from direct connections to the Internet to more subtle and insidious use of side penetration channels.

Finally, business interests (and in some cases even governmental interests) have made industrial processes and critical infrastructure key targets for intrusion and espionage and destructive attacks.

Mitigation:

A holistic approach is required to counteract threats in complex systems which should comprise of (i) a cautiously designed multi-layered security monitoring architecture, clearly differentiating a multi-source, multi-technology, and multi-purpose threat monitoring layer, from an upper control layer responsible for protection and managing the collection and classification of identified events, (ii) deeper inspection or mitigation actions, from the higher decision level in charge to correlate events, detect behavioural changes in the system as a whole, and perform mitigation decisions, and (iii) sufficient scalability of protection systems must be assured in order to fit the reliability and scaling needs of the deployment, so as to enable faster deployment and integration, and plug-and-play provisioning.

Opportunities:

New methods are constantly emerging for analysis of heterogeneous data and cyber-physical information gathered in complex systems and the security monitoring framework (system logs, physical security alarms, surveillance alarms, network events, etc.). These new methods exploit extremely advanced statistical algorithms (e.g., dynamic Bayesian network inferences) on the events that were not yet detected as attacks to determine if they most probably correspond to “normal” behaviours or to outliers and behavioural deviations.

5.4.2 Negative effects of complexity and connectivity

Organisations operate in chains and depend on other organisations. Monitoring the entire supplier chain in terms of its cybersecurity is a complex challenge and can be seen as a negative effect of the complexity and connectivity of contemporary IT solutions.

Challenge:

As businesses undergo technology-based transformations, including cloud, IoT, and high-speed wireless access, the area of potential attacks on them increases. Securing this complex environment becomes more difficult when using different technologies that do not work together. The CISCO 2020 Benchmark Study (2020), conducted by CISCO among 2800 security professionals, found that 28% of those surveyed found it very difficult to manage the environment of many suppliers, an increase of eight points compared to the previous survey.

In addition, almost one third (31%) of organisations base their monitoring and protection of cyberspace on over 50 different security products. This not only increases costs and complexity, but also makes it difficult to detect and respond to timely cybersecurity incidents. The cybersecurity industry has been flooded with plethora of single-function products to help customers, but instead created an unmanageable environment with tools that do not work together. This has led to gaps in the approach to business security. In addition to the activities of cybercriminals, the complexity of cyberspace environments has become another risk that security teams must overcome.

Mitigation:

Integrated IT security technology platforms have the potential to address these economic, technical, and resource challenges, providing more comprehensive threat detection, automated incident response and ease of use. What is needed are easy-to-use (cloud-based) platforms unifying the management of the entire security solution range. Such solutions for automated security processes, including investigation of violations and corrective actions, should provide new possibilities of threat detection based on the expert knowledge.

A comprehensive use of integrated security group and existing customer security infrastructure is required. Such platforms should identify unknown threats and automate workflows to enhance users’ security on the

network, endpoints, cloud, and applications. Because simplicity is essential to secure today's wave of digital transition a unified approach would be expected.

A fundamental change in the approach to customer security could be removing the complexity and providing a consistent view of customer security services and alarms. In this way, security teams could make better use of their available resources and become at the same the business advisors introducing the digital transformation within companies.

Opportunities:

Adoption of solutions from different sectors could be considered such as modern technical systems which are also characterised by a high degree of complexity and responsibility for the implementation of specific functionalities. As a result, the consequences of malfunctioning and damage to these systems are becoming increasingly serious. It is therefore necessary to continuously check selected performance indicators of all components of complex systems in order to detect the risk early on. This control though takes place through the operation of electronic and automation equipment, which also has limited reliability. The widespread problem of ensuring the required safety level has forced the International Electrotechnical Commission (IEC) to set certain standards for the safety of electronics and automation equipment (EN 61508). These standards address so-called Safety Integrity Levels (SILs) and are now leading normative principles that are respected by dominant safety system manufacturers worldwide.

5.4.3 Obfuscation as IDS evasion technique

Obfuscation techniques can be used to avoid detection of some attacks since they are hiding some attacks by making the message hard to understand. The term obfuscation means modification of the code of the program in such a way that its functionality remains the same, while the detectability is reduced by means such as static analysis or reverse engineering. This results in making it unclear and more unreadable. In this way the obfuscation of malware allows to avoid current IDS systems. For example, Signature-based Intrusion Detection Systems (SIDS) use signature matching in order to identify malware; these signatures are created by experts that translate a malware from machine code into a symbolic language, but the code obfuscation is very common technique among cybercriminals for evading IDSs.

Challenge:

An effective IDS should support the hexadecimal encoding format or store such hexadecimal words on its list of attack signatures. Unicode/UTF-8 standard allows one character to be represented in several various formats. Cybercriminals may also utilise double-encoded data, exponentially increasing the number of signatures needed attack detection.

Mitigation:

In Anomaly-based intrusion detection system (AIDS), a model of normal computer system behaviour may be created with the use of machine learning (Buczak & Guven, 2015; Meshram & Haas, 2017), statistical-based (Lin, Ke, & Tsai, 2015) or knowledge-based (Can & Sahingoz, 2015; Elhag, Fernández, Bawakid, Alshomrani, & Herrera, 2015) methods. Any significant deviation between the observed behaviour and the model can then be treated as an anomaly, which can be regarded as an intrusion. In particular, the statistics-based approach leads to creation of a statistical model of normal user behaviour which is built by collecting and analysing every data record. On the other hand, knowledge-based methods try to identify the requested actions by examining existing system data (e.g., protocol specifications or instances of network traffic), while machine-learning

techniques discover various schemes based on training data and then perform complex pattern matching operations in order to classify the given actions.

Opportunities:

Machine learning methods are broadly used as a part of modern intrusion detection systems, such as AIDS. Some known algorithms: artificial neural networks, clustering, genetic algorithms, nearest neighbour methods, association rules and decision trees are applying in order to gain specific knowledge based on the intrusion datasets (Kshetri & Voas, 2017; Xiao, Wan, Lu, Zhang, & Wu, 2018). The recent advances in Artificial Intelligence and Deep Learning open up new opportunities for further advancing such system.

5.4.4 Encryption as IDS evasion technique

Generally, encryption supports a number of security services, such as data confidentiality and integrity, privacy protection, and others. However, authors of malware employ these security solutions to escape detection and conceal attacks that may target a computer system. For example, attacks on encrypted protocols such as HyperText Transfer Protocol Secure (HTTPS) are hard to detect by intrusion detection systems (IDS). The IDS cannot match the encrypted traffic to the existing database signatures if it does not interpret the encrypted traffic. For example, applied content-based packets detection features to identify malware in traffic network, usually cannot be readily applied if the packet is encrypted. Examining encrypted traffic is difficult for network devices and such hidden attacks can be successfully launched. Detection of such attack is a serious challenge and influences network security (Camacho, Pérez-Villegas, García-Teodoro, & Maciá-Fernández, 2016).

Challenge:

Encrypted traffic cannot be easily analysed using content-based techniques in order to distinguish malware from analysed traffic. Therefore, IDS solutions (and other similar security network devices/platforms) have a serious problem to detect malware or network attacks in encrypted packets. Ordinary signatures of malware/attack cannot be used, because after the encryption, the string of bits characteristic for a malware/attack is changed. The encrypted data also changes if different cryptographic keys are used. Thus, IDS cannot have signature for encrypted malware or characteristic sequence of attack.

Mitigation:

This challenge motivates researchers to use some statistical network flow features, which do not rely on packet content. Instead of signature-based detection methods, IDS can use anomaly-based approaches to detect malware/attack. As a result of this, malware can potentially be identified from normal traffic. Additionally, in some scenarios, it is possible to capture data from users (i.e. computers in corporate network). The user can use public key from the certificate generated by IDS to encrypt data between user and the network device. Then IDS can decrypt data, scan data and then send it to recipient using his/her own certificate. However, such approach requires full trust to network device which is able to read all data. Therefore, critics of this solution called this approach as men-in-the-middle attack.

Opportunities:

There are opportunities for new anomaly-based detection methods to be developed in order to find malware content in encrypted data. Also, it is possible to design new heuristic algorithms, which will be able to detect malware. Probably, heuristic solutions can determine if encrypted traffic contains malware content using various decision rules or weighing methods. If we are able to find some characteristic behaviours or statistical factors, IDS can also use specific AI/ML solutions to detect unwanted content in encrypted packets.

5.4.5 Man-in-the-middle attacks

A Man-in-the-Middle (MITM) is a cyberattack in which an attacker manages to relay the traffic between two endpoints of communication, usually an end user (person) and a web application. This allows the attacker to monitor the data (messages, transactions, etc.) flowing between the endpoints and modify it to his advantage. For a MITM attack to be successful, the attacker must successfully (satisfactorily enough) be able to present himself to each endpoint as the other. The principle of operation of the MITM attack is presented in Figure 12.

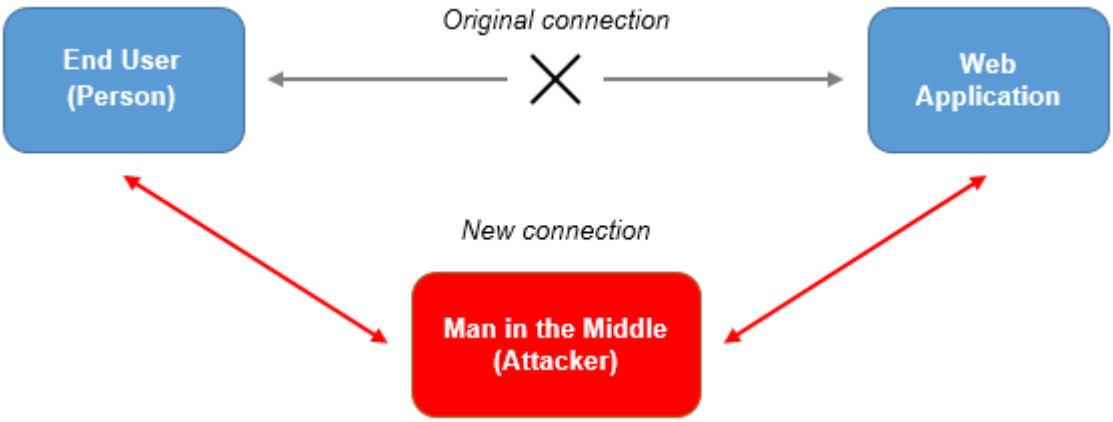

Figure 12. Man-in-the-Middle attack

Challenge:

The MITM attack is aimed primarily against the confidentiality of information, and in some cases also against its integrity. This means that along with information theft, its primary task is to remain undetected. It follows that the main challenge in counteracting the MITM attack is to detect it. There are numerous methods and techniques for executing the MITM attack. The most effective and popular ones include:

- **IP spoofing:** By spoofing the IP address of a network device under his control, the attacker can trick the end users that the web application they want to access is located on that device and can access the victim's traffic.
- **DNS spoofing:** The DNS (Domain Name Server) spoofing, also known as DNS cache poisoning, is a technique where the attacker replaces the address record of the web application in the DNS table. As a result, the end users will receive an incorrect information from the DNS and instead of the original web application will access the attacker's one.
- **HTTPS spoofing:** During HTTPS spoofing, the attackers register a domain name that is similar to the target website, and also register its SSL certificate to make it look legitimate and secure.
- **SSL hijacking:** SSL hijacking is when the attacker passes forged authentication keys to both the end user and web application during a TCP handshake. As a result, the end user and the web application consider that they communicate directly, while in fact the attacker has complete control over the communication between them.
- **Wi-Fi eavesdropping:** The attacker can set up Wi-Fi connection with very legitimate sounding name. When the end user connects to this Wi-Fi, the attacker will be able to monitor the user's online activity capture login credentials and other sensitive information.
- **SSL stripping;** SSL stripping downgrades a HTTPS connection to HTTP by intercepting the TLS authentication sent from the web application to the end user. The attacker sends an unsecured version of the web application to the end user while in the same time keep the secured session with the web application. Meanwhile, the end user's session is visible to the attacker.

Mitigation:

Mitigation measures of the MITM attack can be grouped into two main groups: end-user actions and web application admin actions.

End-users are typically advised to:

- avoid password-unprotected Wi-Fi networks;
- pay attention whether the browser determines the connection as a secure (HTTPS, not HTTP);
- log out of a secure application when it is not in use;
- not use public networks (hotels, coffee shops, etc.) when conducting sensitive transactions;
- install a comprehensive internet security solution and always keep the security software up-to-date; and
- update all default usernames and passwords on all connected devices to strong, unique passwords.

Web application administrators are typically advised to:

- use secure communication protocols, including TLS and HTTPS, to help mitigate spoofing attacks by strong encrypting and authenticating transmitted data;
- use SSL / TLS to secure every page of the website / web application and not just the pages that require users to log in (doing so helps decreases the chance of an attacker stealing session cookies from the end user browsing on an unsecured section of the website / web application); and
- regularly update the systems with the latest patches and check that any of the security protocols used have been compromised.

Opportunities:

There are several innovation opportunities related to the MITM attacks, mainly related to the cybersecurity learning and training for both IT professionals and end users. Different types of MITM attacks could be simulated in virtual environments (such as cyber ranges) in order to look for different direct and indirect signs of an attack being detected, develop methods to prevent such attacks from occurring, and support the training of IT professionals. In addition, early warning system regarding such MITM attacks could provide up-to-date information through referent libraries.

5.4.6 Denial of Service attacks

Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks refer to a complete or partial disabling of an IT service, deviating from its proper operation, by overloading the network or the server's CPU. By attacking special vulnerabilities in an application, operating system, or attribution (weaknesses) of a special protocol, the goal is to deny users authorised to access the application or system from accessing information that is important to them, the computer system, or even the computer network. As a result of the attack, the system will become very slow, inaccessible, or even crash. A simple DoS attack is a one-on-one attack where a very strong “attacking” computer and the destination computer are interlinked, i.e., there are no intervening machines, while DDoS attacks are a more complex type of attack that utilises the “power” inherent in the attacker and non-attacked computers, as well as the large number of external computers, to attack.

Challenge:

A server can become overloaded and unavailable if the operators do not properly assess the expected load before they started (i.e., they are built with few resources), or do not perform load configurations. In addition, before the live launch, the necessary load tests need to be performed on the server and / or the protection line built in front of it, so that the clients/users themselves and the malicious attackers do not become testers in a live environment. Although there are well-known server modules (such as Apache) that can reduce the impact of a DoS attack, they require expertise and practical experience to configure, and also they are not effective

against a DDoS attack. In addition to the proper load settings and the banned of unwanted (attacker) IP addresses, it should be noted that a DDoS attack can be a deceptive operation. In many cases, there is another attack behind DDoS, so the attackers try to covering up the ‘real' attack.

The most common targets of DDoS attacks are against financial service providers (e.g., banks), government agencies, large companies, non-profit (civil and political) organisations, and Internet Service Providers.

Regarding the nature and volume of the attacks, the following trends have been observed:

- the number and rate of economically motivated attacks is increasing;
- the number of targeted attacks is increasing;
- botnets and DDoS attacks launched on them have become an easily accessible, low-cost “service” that can be “purchased” by everyone;
- attacks that generate seemingly legitimate traffic make real-time detection and defence difficult;
- the rate of volumetric attacks is increasing (flood attacks);
- the traffic generated per attack is increasing on a large scale;
- the average time of attacks decreased, 86% of which were for less than an hour; and
- the "strength" of attacks has increased significantly.

Mitigation:

Such incoming threats can be mitigated through appropriate settings in the network devices, the installation of protection systems, and cloud-based protection services. Network protection is an IP-level filtering option that can be used to block network traffic with fake source addresses. Additional mitigation techniques include:

- Network bandwidth: Higher bandwidth increases the amount of bandwidth that attackers must cross before launching a successful DDoS attack. This is a security measure, but not a DDoS attack solution.
- Protection of servers: Redundant operation of DNS servers would result in attackers needing more time to install servers in different data centres connected to different networks. By geographically distributing the servers, the work of attackers can be further complicated, allowing the other (geo-redundant) server to serve the extra traffic.
- Anti-DDoS hardware and software modules: In addition to protecting the servers with network firewalls and other special web application firewalls, load balancers must be used, as well as hardware modules that provide software protection against DDoS protocol attacks, such as the SYN flood attack.
- Transparent website view: A mirror application front-end is an intelligent hardware placed on the network before traffic reaches the webservers which analyses data packets as they enter the system, and then identifies them as priority, regular, or dangerous, so the server can be protected against corruptible application content.

Opportunities:

Although DDoS attacks cannot be prevented, steps can be taken to make it harder for attackers’ operations. When designing systems, it is necessary to create a system environment that shares the traffic of the service between the multiple servers. Security features, such as the implementation of an Intrusion Prevention System (IPS), that can detect traffic from an attacking computer and discard transactions from attackers, should also be provided. It is also recommended that action plans be developed in the event of a DoS/DDoS attack to provide guidance to operators on what to do during the attack and thereafter. Overall, both hardware and software solution options are required in order to prevent such attack, along with sufficiently flexible architecture, as well as network traffic monitoring solutions and effective measures.

5.4.7 Encrypted malicious web traffic

The expanding volume of encrypted web traffic—both legitimate and malicious—creates even more challenges and confusion for defenders trying to identify and monitor potential threats. Encryption is meant to enhance security, but it also provides malicious actors with a powerful tool to conceal command and control (C2) activity, thus allowing them more time to operate and inflict damage.

Challenge:

The CISCO 2018 Annual Cybersecurity Report (2018) indicated that within one year, from November 2016 to October 2017, global (both legitimate and malicious) encrypted web traffic went up from 38% to 50%, and the expectation is that this volume will continue to increase. There are many factors driving this trend, such as the availability of low-cost or free SSL certificates, and also the web browsers' practice to display warnings when visiting websites that contains unencrypted content and flag them as non-secure. As such, many businesses are now motivated to comply with Google's https encryption requirements in order to avoid significant drops in their rankings in the Google's search page results. The same report also indicates that, along with an increase in legitimate encrypted web traffic, malicious encrypted web traffic is also growing, since adversaries would use encryption as a tool to conceal their C2 activity; during the aforementioned 12-month period, 70% of the inspected malware samples in October 2017, were using encrypted network communication, with more than a three-fold increase from what was observed in November 2016.

A further analysis of web attack methods over an 18-month period (April 2016-October 2017) presented in the aforementioned report allows us to glimpse at adversaries' intent and strategies, showing an intense focus on browser compromise. A significant and consistent detection of malicious Javascript content, hints at the effectiveness of this strategy to facilitate other malicious activity, such as browser redirection or Trojan downloads. Moreover, a similar analysis over the three-year period (October 2014 - October 2017) presented in the CISCO 2017 Midyear Cybersecurity Report (2017) indicates that suspicious binary files (executable malicious programs) were used to deliver adware and spyware; these are types of potentially unwanted applications that can present security risks, such as malware infection and theft of information. In the same report it can be observed how the volume of malicious web content fluctuates over time as attackers launch and end their campaigns and change their tactics to evade detection.

Mitigation:

In order to mitigate encrypted malicious web traffic, many enterprises are now incorporating solutions based on Machine Learning (ML) and Artificial Intelligence (AI). In fact, these tools can learn over time to distinguish normal web traffic from anomalous traffic by detecting unusual patterns that might hint at malicious activity and automatically alert security teams for further investigations. While there are many ML/AI techniques useful for detecting both known and unknown threats, those that excel in monitoring encrypted web content are those that do not rely on static or dynamic signatures, or on any other characteristic of the traffic dependent from the encryption used. Such techniques include for example (see Figure 13) "behavioural signatures", which use supervised machine learning to learn a signature behavioural pattern from the analysed traffic, "high-level patterns", which classify through semi-supervised learning high-level generic behaviour and anomalous traffic, and "unsupervised anomalies", which is an unsupervised machine learning technique that automatically extracts from the analysed web traffic "normal" behaviours and flags anomalous content when cases happen that are significantly distant from any normal behaviour.

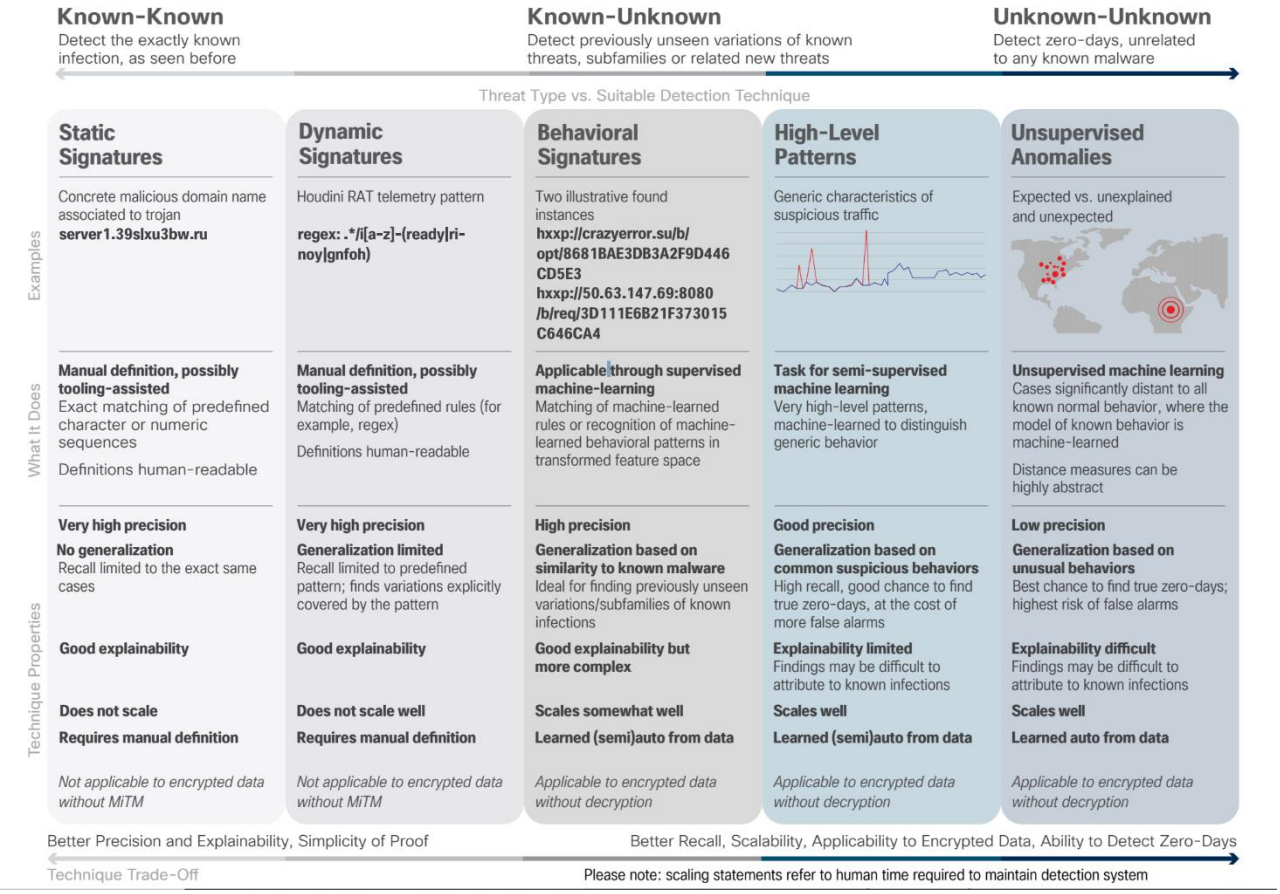

Figure 13: Threat type vs Suitable detection technique (source: CISCO 2018 Annual Cybersecurity Report, (2018))

Lack of trained cybersecurity personnel in companies can also be an obstacle to an efficient mitigation of the malicious activities, but automatic tools based on AI/ML can help defenders to identify and respond quickly to threats. However, AI/ML techniques that are applicable to encrypted data and have the highest chance to detect zero-days attacks, usually have also a lower precision and a higher risk of raising false alarms, than more standard techniques.

Opportunities:

The results of the CISCO 2018 Security Capabilities Benchmark Study (reported in the CISCO 2018 Annual Cybersecurity Report (2018)) indicated that defenders are increasingly relying on automation and AI/ML techniques, as highlighted by the chief information security officers (CISOs) interviewed by CISCO, who were eager to add such AI/ML-based tools and believed that their security infrastructure is growing in sophistication and intelligence. However, they are also frustrated by the number of false positives such systems generate, since such false positives increase the security team's workload. These concerns should ease over time as AI/ML technologies mature and learn what is "normal" activity in the network environments they are monitoring. Moreover, when asked to what extent their organisations are completely reliant on such automated technologies, 39% said they are completely reliant on automation and 32-34% on AI/ML, while behaviour analytics tools are also considered useful when locating malicious actors in networks.

5.4.8 Decentralised DNS

Lately, blockchain is being used to decentralise DNS services (referred to as "blockchain DNS"), as pioneered by the likes of Namecoin and Emercoin (among others). A decentralised and unregulated DNS will create though new attack vectors and introduce new emerging threats, such as domain hijacking and efficient Domain Generation Algorithms (DGAs) for bots etc.

Challenge:

Decentralised DNS (DDNS) introduces a number of security-related challenges, namely:

- TLD registration and potentially uncontrolled domain registration marketplaces: This can have direct consequences to intellectual property, such as trademark infringement opportunities, where an important complication of the DDNS is that due to its immutability, there is no mechanism to remove or alter a DDNS record. As a matter of fact, currently there are trademarked names registered on DLTs implementing DDNS, where the registrant is not the trademark owner, see for example the case for apple.eth[3].
- IP address resolution of the registrant as new attack vectors: An example attack would be to initially direct a *.eth (or .coin, .bazaar, .emc, etc.) domain resolution to the real business (say from a hypothetical amazon.eth to the https://www.amazon.com), but at a later stage change the IP to hijack the visitors.
- New malware attack vectors: Botnets that traditionally use Domain Generation Algorithms (DGAs) may move to registration and use of DDNS registered domains. This will have an impact on existing malware detection techniques based on DGA analysis and detection, e.g., detection of the main Non-Existent Domain messages that are generated in a short period of time when the underlying bot attempts to discover the C2 node location.
- Phishing: As the DDNS allows registration of any domain, it will be virtually impossible for a user to distinguish whether a URL refers to a genuine business owned site or not.

Mitigation:

Against the above challenges, mitigation measures could consider processes and policies to prohibit arbitrary domain registration, which should be more stringent since the DDNS is more robust than the traditional DNS, the policies should be more stringent, as well as research into development of appropriate policies (e.g., similar to DMARC and DKIM used to secure email services) and generation of new types of IOCs. These are non trivial tasks and they cannot be expected to be fully effective from the start.

Opportunities:

Innovation opportunities include the development of novel detection techniques, including techniques based on AI/ML for the detection of the (ab)use of DDNS infrastructure and protocols, as well as the development and improvement of digital forensic processes and techniques to support the investigation in DLT environments.

[3] https://www.coindesk.com/ethereum-name-service-auction-exploited-to-grab-apple-domain-and-it-cant-be-undone

5.4.9 False positives in the detection of anomalies, attacks, and intrusion attempts

The anomaly-based intrusion detection paradigm aims to decrease the amount of necessary human intervention, by implementing statistical models for the recognition and processing of standard behavioural patterns in order to detect deviation. This, however, introduces the risk of an increase of false positives or false negatives, as the ability of the system to recognise harmless environment-based and contextually-required user interactions with a specific system may decrease. In particular, IPS / IDS systems tend to generate a large amount of data and a large body of alerts, many of which can be false positives. Most of these false positives are a result of the inability of the system to apply the available and generated knowledge on behavioural and environmental patterns, which represent partial attack patterns or a standard behaviour, mistakenly flagged as a malicious activity.

Several technologies employed for the development of IPS / IDS systems have been identified by the ECHO consortium in the context of the activities of T2.4. Among these technologies are widely adopted solutions or upcoming trends, such as AI/ML, big data, (post) quantum, cloud and virtualisation, IoT, and others, all of which can have an impact and relate to multiple sectors of critical societal importance, such as healthcare, energy, transportation and defence. However, these technologies are prone to generate large amounts of false positives, when it comes to their application in intrusion prevention and detection, regardless of the installation configurations and, more often than not, due to environmental misinterpretations.

Challenge:

To completely eradicate false positives is an impossible task. For the study of anomaly detection, researchers have been using standard behavioural patterns for decades, however few solutions, even commercially available, are tailored to particular clients. The IDS / IPS development takes into account a general public or the needs of a specific sector or the standard behaviour of a representative group of systems. This makes the system prone to false positives and increases the need for additional configuration at a user-level, which, although still incredibly important, is not a bulletproof solution. Such configurations are often implemented either by a company's system administrator, or by product representatives who are more likely to not be too familiar with the context and standard behaviour of a particular system and its users. If configurations are implemented by a system administrator, more often than not, they will not be able to implement a fully customised configuration, as IDS / IPS are configured with standard parameters, as are most software product. Systems are predisposed to false positives, as their implementation is not research-informed to align to a specific environment. Thus, decreasing the overall amount of false positives is of utmost importance, as the human capacity to review incidents is very limited in anomaly-based IPS / IDS.

Mitigation:

There is really no way to absolutely mitigate false positives. However, taking actions to review the system configurations, along with the behaviour signatures are of paramount importance in order to lower the number of false positives in most IPS/IDS that follow the anomaly-based paradigm. In order to avoid the necessity of overwhelming human investment in the incident review process, it is important that by-design system allowance for customisations and custom creations of filters, configurations, and alerting models are implemented.

Another important aspect of mitigating the issue of false positives, is to regularly install all security patches, updated with the latest lists of vulnerabilities, risks, and threats. As proposed by (Grill, Pevný, & Rehak, 2017) the implementation of Local Adaptive Multivariate Smoothing could reduce a large portion of false positives introduced by the anomaly detection by replacing the anomaly detector's output on a network event with an aggregate of its output on all similar network events observed previously.

Last but not least, literature suggests the implementation of multiple IPS/IDS technologies to enable a triangulation of false positives. This approach has several benefits, stemming out of the fundamentally different capabilities, offered by the various types of such technologies. The anomaly-based detection paradigm is exceptionally good at discovering attacks from previously unknown malware, or zero-day type attacks. Other types of IPS/IDS technologies, such as the signature-based detection model, might offer the benefit of detecting some attacks more accurately, without causing significant performance impact on the protected system (but as a rule, generating more false negatives). Therefore, it might be highly beneficial for some systems to implement an intrusion prevention and detection strategy by combining multiple IPS/IDS technologies. This approach is also appreciated by data analysts, who would have more information in order to confirm or deny the validity of a given incident and ultimately reduce the human factor investment in the intrusion detection process.

Opportunities:

Multiple opportunities for further research and innovation are available in terms of the anomaly-detection paradigm. Customisable mechanisms for redundancy detection, noise reduction, correlation in features and parameters are needed, especially when integrating multiple IPS/IDS products from different vendors. Cost and power efficiency are also a significant factor for the identification and adoption of such technologies, however, not surprisingly, poor customisations and filtering often result in significant expenses, so mechanisms to refine the data obtained are a research opportunity, which is much needed in many contexts. Moreover, the problem with false positives in the anomaly-based detection paradigm often stems out not from incomplete training data, but from noisy training data. Various statistical methods are commonly applied to combat those issues, however further opportunities exist when it comes to sourcing unique approaches for different contexts, which is what a robust IPS/IDS strategies often aim at.

5.5 Cloud, edge, and virtualisation

Edge computing is a recent and promising trend that can be considered to be the next step in cloud computing technologies, while component virtualisation is a key feature of edge computing architectures. As traditional centralised infrastructures are becoming suboptimal in terms of efficiency and data processing throughput, the increase in demand for data processing power requires a new data centre architecture that can provide the necessary computational capabilities, thus resulting in a reduction of response time and bandwidth load. Edge computing aims to distribute the data processing load across an ecosystem of devices, also known as Content Delivery Networks (CDNs). As the number of connected devices will increase dramatically in the following years, processing the generated data will become virtually impossible, unless traditional cloud infrastructure shifts to a new paradigm.

5.5.1 Abuse of cloud services

Cloud computing presents threat actors with an entirely new attack surface that can potentially provide them with business-critical information or even complete control of the functional capabilities of a cloud service and its users. The sheer amount of data that cloud service providers consume and transfer makes them a common target for attacks.

Challenge:

There is a large variety of attack vectors that can be employed against cloud services, and may result in loss of data, denial of service, data breaches, financial losses, etc. The following critical issues are ranked in order of severity.

Data Breaches: A data breach is a security incident which relates to the process of viewing, stealing, or using sensitive, classified, or otherwise protected data, performed by an individual or group of individuals who do not possess the required authorisation to do so. This data may be stored on a variety of media types, such as computer tapes, internal and external hard drives, data bases, and other hardware and software systems that are used for data storage. Data breaches are a common objective of targeted attacks, and they are made possible by occurrences of active vulnerabilities, improper security measures and practices, and human error. The information affected by data breaches includes, but is not limited to, classified information, personally identifiable information, personal health information, financial information, sensitive information, intellectual property, and other applicable types of protected information. Cloud service providers are significantly affected by the threats posed by data breaches due to the access requirements and shared resources that are closely associated with such services.

Weak Identity, Credential and Access Management: The lack of properly configured and sufficiently scaled identity access management systems, multifactor authentication, strong password use, and automated rotation of secure cryptographic keys and certificates, is a leading reason for the common occurrences of data breaches and can facilitate the execution of other attacks. Due to the extensive use of identity access management systems, they have become increasingly interconnected, hence the existence of cloud-based identity federation mechanisms, such as SAML. Such solutions ease user management, but they demand complete understanding of cloud processes, infrastructure, and topology, as well as cloud tenant segmentation in multi-tenant implementations. In addition, technologies such as multifactor authentication systems provide a much needed additional level of security when interfacing with cloud services by introducing a second authentication prompt, that is often fulfilled by the use of smartcards, one-time tokens and authenticators.

Insecure APIs: Application Programming Interfaces (APIs) are an extremely common way cloud computing services provide an interface that customers can use in order to manage and work with features that are specifically made accessible by the cloud service provider, such as such provisioning, management, orchestration and monitoring. These procedures are business critical and need to be properly protected by employing strict authentication and access control, secure communication channels, and activity monitoring. Due to their wide accessibility, exposed nature, and the potential unrestricted data access they can provide, APIs are a common target of attacks against cloud service providers.

System and Application Vulnerabilities: System and application vulnerabilities represent weak points in the system that can be exploited by threat actors in order to obtain unauthorised access, exfiltrate data, steal finances, perform advanced attacks, or negatively affect availability to devices, networks, or entire services. Cloud based services are often comprised of multitenant environments that store systems from various users, clients, and organisations. Successful exploitation of a single device in such a system can provide access to shared resources and data that affect and are relevant to the entirety of the multitenant environment. The time required to apply vendor-provided patches, fixes, updates, and workarounds, is critical in handling the potential exploitation of system and application vulnerabilities.

Account Hijacking: This threat represents the process of a threat actor stealing or hijacking the cloud service account of a specific individual or organisation. To this end, threat actors perform credential harvesting attacks, such as phishing campaigns and fraud, or exploit system and application vulnerabilities in order to circumvent the implemented layers of authentication. Since it is common practice among users to reuse passwords, if an account hijacking attack is successfully performed, the hijacked individual's account can be used to inform the stealing of additional accounts that share the same credentials. In the case of the successful account hijacking of an organisational account that has the authorisation to view sensitive data or make holistic changes to the affected service, threat actors can gain access to stored user data such as credentials, personally identifiable information, personal health information, and others, thus resulting in an organisation-wide data breach. If this hijacking is not detected, threat actors can proceed to monitor user activity, shape data, continuously harvest user information, or execute additional advanced attacks, such as Cross Site Scripting (XSS).

Malicious Insiders: This term represents a group of individuals that are in some way affiliated with, or have been affiliated with, an organisation and its assets, and have intentionally breached the confidentiality, integrity, or availability, of the aforementioned assets, by ways of data exfiltration, data deletion, data corruption, business operation disruption, damaging organisational brand, internal and external distribution of malware, etc.

Advanced Persistent Threats (APTs): APTs are threat actors that are typically sponsored by national states or large organisations with the sole purpose of obtaining unauthorised access to a computer network and further establishing a foothold for an extended period of time. Their goals are usually motivated by political or economic reasons. Towards obtaining initial access to the target network, APTs use attacks such as spearfishing, social engineering, and vulnerability exploitation. Once they have secured access, APTs can proceed to infiltrate partner or connected third-party networks, move laterally and pivot to other systems depending on their objective. Lack of user awareness is a critical setback against the initial vectors APTs commonly use such as spearfishing and social engineering.

Data Loss: Data Loss is a prospect that is stifled by the prominence of cloud storage but is not made extraneous. Data stored in the cloud can still be mismanaged and permanently deleted due to human error, natural catastrophes such as earthquakes and fired, or even malicious actions. The creation of business continuity and disaster recovery plans is critical for the protection of organisational and user data in the case of a worst-case scenario. This process is further aided by the continuous and scheduled creation of backups for data at rest. Users can implement additional layers of protection for their data by applying redundancy with both cloud and on-premise storage solutions. Data loss can also be incurred by user-made errors such as the loss of an encryption key or improper versioning.

Insufficient Due Diligence: When an initial business strategy is being drafted, due diligence is required during the critical process of choosing the correct cloud technology or cloud service provider. Proper evaluation of risks for organisational and user data must be performed in order to insure the implementation of a sufficiently secure solution. The lack of a due diligence can result in a drop of customer satisfaction due to cloud service provider limitations, operational setbacks caused by limitations imposed by the cloud infrastructure, or even adverse effects in compliance and legal requirements for data in use, motion or at rest.

Abuse and Nefarious Use of Cloud Services: Improperly secured cloud services, cloud service trials, and malicious accounts can allow threat actors to target IaaS, PaaS, and SaaS models with attacks. The misuse of such cloud services may result in the launching of DDoS attacks, spam e-mail and phishing campaigns, malicious cryptomining activities, user data and credential exfiltration, Cross-Site Scripting attacks, etc.

Shared Technology Issues: An integral part of cloud service providers and their infrastructure is the shared nature of their applications. Cloud technology is commonly presented in “as a Service” type models that only have slight variances from model to model. This practice can adversely affect multiple solutions simultaneously if they have been improperly secured, or if off-the-shelf hardware and software is used in order to supplement the required ease of sharing. If a singular cloud service provider model is affected by a vulnerability, all models such as IaaS, PaaS or SaaS can suffer from the shared vulnerability due to software and hardware reuse. Mitigations to prevent a breach in shared resources should be implemented, such as multi-factor authentication on all hosts, Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS) on internal networks, applying concepts of networking least privilege and segmentation, and keeping shared resources patched.

Mitigation:

Data Breaches: In order to prevent data breaches, advanced security solutions in an overall defence-in-depth plan should be integrated, such as:

- perimeter and internal firewalls;
- file and device encryption;
- IDS and IPS solutions;
- regular internal and external vulnerability scanning;
- log management and auditing procedures;
- multi-factor authentication; and
- principle of least privilege.

In order to mitigate data breaches after their occurrence, monitoring services need to be activated in order to track misuse of exfiltrated user data and information.

Weak Identity, Credential and Access Management: Proper identity and credential management are key for protecting user and organisational data. Data encryption, hashing, and salting can protect data from being misused or exfiltrated. Strict password policies and GDPR compliance supplement the process of identity and credential management. Implementation of proper access management is critical for the prevention of potential misuse of data. Principles such as least privilege and dual control are vital parts of a secure data access and management structure. Implementing access controls such as Mandatory Access Control (MAC), Role-based Access Control (RBAC) or any other applicable access control can streamline and ease the burden of access management.

Insecure APIs: Implementing procedures such as regular code review and requiring secure code writing practices can mitigate the commonality of insecure APIs. Performing threat modelling should be implemented in the software development lifecycle in order to avoid potential vulnerabilities. Scheduling penetration tests and vulnerability scans can also be used in order to identify vulnerabilities before they have been published to the general public. The usage of secure communication channels such as TLS is pivotal in the current cybersecurity landscape, while the implementation of properly configured authorisation mechanisms and input validation can prevent the potential misuse of APIs. Versioning, patch and change management, can spearhead mitigation in the case of the existence of a vulnerability in a live product.

System and Application Vulnerabilities: The implementation of regular vulnerability scanning, delta reporting and patch management procedures can significantly reduce the potential chance of vulnerability exploitation. Keeping up-to-date inventory lists or Configuration Management Databases (CMDBs) can inform decisions and assist in the detection of outdated software and hardware.

Account Hijacking: User awareness and education is a critical countermeasure for account hijacking due to the prevalence of phishing campaigns that aim at credential harvesting. The use of unique strong passwords and their secure storage and use can provide an additional layer of protection to accounts. In addition to passwords, other authentication mechanisms should be required, such as smart cards, one-time tokens, or authenticators. Products such as e-mail security solutions can be configured to filter out the vast majority of phishing and malicious e-mails.

Malicious Insiders: In order to avoid actions by malicious insiders, proper access control management must be implemented by means of the principles of least privilege and dual control. The revocation of user access post termination should be added as part of the deprovisioning process. Log analysis and management mechanisms should be implemented for purposes of holistic view facilitation.

Advanced Persistent Threats (APTs): APTs commonly make use of phishing campaigns as an initial attack vector and therefore user awareness and education can serve to reduce instances of user interaction with malicious e-mails. E-mail security solutions can be used to filter out unwanted spam, phishing, or malicious e-mails. Implementing strong egress and ingress traffic monitoring and filtering mechanisms can completely mitigate an attack, or inform relevant parties of its occurrence. This can be achieved by the usage of firewalls,

IPS and IDS, and other security devices. Internal network segmentation is also crucial in preventing the potential spread and pivoting capabilities of APTs in the case of successful exploitation.

Data Loss: Data loss can be mitigated by facilitating the geodiversity of storage. If data is stored in multiple diverse locations, both in the cloud and on premises, the chance of potential loss of data is greatly diminished. Proper mechanisms for the protection of data at rest, data in motion and data in use need to be configured. This can be achieved with the usage of access controls, encryption, data retention, IDS/IPS, Antivirus software, and Data Loss Prevention (DLP) solutions.

Insufficient Due Diligence: Due diligence requires thorough examination of a cost-benefit analysis or another similar analysis in order to reach an informed decision. Performing checks for potential risks inherent to specific cloud service providers or issues with required compliance, cloud availability, capacity and elasticity, is necessary for the purposes of due diligence. Extensive strategies are necessary for the successful implementation of the cloud service. These strategies should include, but should not be limited to, examination of data storage practices, data breach or data loss recovery plans, targeted attack mitigation, governance practices, etc.

Abuse and Nefarious Use of Cloud Services: Mitigation of cloud service abuse is facilitated by the usage of advanced security software and hardware, as well as best practices, such as:

- IDS/IPS solutions;
- perimeter and internal firewalls on a tenant-by-tenant basis;
- asset identification and inventorisation;
- regular risk assessment; and
- scheduled threat and vulnerability scans.

Shared Technology Issues: Multiple security requirements and protocols should be integrated in the shared infrastructure in order to mitigate potential technology issues. Different layers of abstraction should be protected separately (operating systems, hypervisors, virtual machines, hardware, network, and storage). Consistent patch management procedures should be implemented in order to avoid the potential exploitation of vulnerabilities. Perimeter, host-based and per-tenant firewalls need to be implemented in order to segment and protect singular tenants and the cloud environment as a whole. Other solutions such as Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS) should be implemented in order to further segment and protect the cloud. Data should be accessed based on the least privilege principle, as well as encrypted while it is at rest, in motion, or in use.

Opportunities:

As discussed above, data confidentiality and integrity in the cloud environment is directly linked with identity management and access control. The use of conventional authentication and authorisation systems is not very effective in cloud environments, mainly because the user base comes from different organisations using different authentication and authorisation frameworks. Many schemes have been proposed in order to address identity management issues on the cloud, however since all of them remain on a theoretical level, thought-provoking opportunities arise that motivate further exploration of the subject. Recently attention has moved to using Identity Access Management-as-a-Service (IDaaS) to control access to applications. It is estimated that IDaaS will grow at around 14% compound annual growth rate (Cser et al., 2018) as more businesses are looking to move from on premises Identity and Access Management (IAM) infrastructures to solutions hosted on the cloud. In addition, the use of passwords and tokens will continue to drop over the next years due to the introduction of new recognition technologies, such as biometrics, that offer higher accuracy at a decreased cost, something that allows the transition from in-house IAM to IDaaS even easier.

5.5.2 Vulnerabilities in cloud infrastructure

The discovery of multiple side-channel vulnerabilities in modern CPUs over the last two years could pose a high risk to organisations running their compute infrastructure in the public cloud.

Challenge:

Many enterprises are moving workload to cloud architecture. Security researchers and adversaries have been focusing on the analysis of vulnerabilities in the cloud infrastructure and thus, several side-channels CPU vulnerabilities have been found in the last years, that could be used by adversaries to read sensitive data hosted on the cloud. The discovery of such vulnerabilities (broadly classified as Spectre and Meltdown) in microprocessors have brought back to the foreground hardware security and CPUs security research. Other vulnerabilities in the Intel microprocessors have been discovered in 2019, such as Zombieload, RIDL, Fallout, and many variants of already known Spectre and Meltdown. This trend is likely to continue in the next years, given the amount of interest it has sparkled, and the effort currently spent in the investigations.

These side channels vulnerabilities of modern microprocessors stem directly from the strategies used to improve CPUs performance, executing instructions in parallel. One of the methods used consists in transiently executing some operations, prior to the instructions being requested, based on a prediction of possible future values. In such a way, if the prediction was correct, when the speculated group of instruction arrive, the processor already has computed the result, while if the prediction was incorrect, the results are discarded. It has been found that there are ways (side channels) to gain information on the transient results, and this information disclosure has led to vulnerabilities such as Spectre, Meltdown and Foreshadow.

While these side-channel vulnerabilities affect most modern microprocessors, servers and workstations, the largest risk occurs in cloud computing. In fact, public cloud computing services have multiple tenants sharing compute instances on the same physical hardware. In such a multi-tenant architecture, each tenant's data is supposed to be completely isolated and secured from the other tenants, but if processors in use have side channels vulnerabilities, then a malicious co-tenant can exploit them in order to launch an attack and extract information from another tenant's instance.

Mitigation:

Most of the affected hypervisors, operating systems, and hardware vendors have released patches, mitigations, and defences to tackle the multitude of speculative execution issues that have been brought to light in the past years.

Software updates: Security updates issued can mitigate the above-mentioned vulnerabilities, but usually at a performance cost; in some cases, even a 30% staggering was reported. For example, for the Portsmash vulnerability, the solution is to disable simultaneous multi-threading, thus degrading performance; the most popular software patch is Google's Retpoline, which prevents the processor from speculating on the target of an indirect jump ("CVE-2018-5407 - Multiple Vendor Microprocessors Design Error Information Disclosure Vulnerability"[4]).New compiler flags adding protection against some vulnerabilities (such as Spectre) have been included as default on new compilers. However, to take advantage of these compiler updates, applications must be recompiled with the updated compilers, and since components of larger applications may still use old libraries, this is not always easy, and the overall security could be somewhat degraded.

[4] https://www.cvedetails.com/cve/CVE-2018-5407/

New hardware: Replacing the hardware with newer models with built-in protections is the simplest mitigation strategy. Even if the cost of replacing hardware prematurely can be expensive, it may be worth the investment to replace server hardware out of cycle. However, updating to new hardware does not guarantee future security as new classes of CPU vulnerabilities are found every year. To counter this, processor vendors provide firmware updates where possible, also providing microcode updates to operating system vendors, shipped as security updates. Microcode updates are applied at boot-time by the operating system, helping in patching some of the security vulnerabilities on-the-fly. The ideal way to deal with this risk is to apply mitigations at all possible levels of the compute stack, hardware and software.

Opportunities:

Cloud deployments: Using a single tenant dedicated host cloud environment that provides a more isolated hardware environment is an opportunity for organisations that want to minimize the risk associated with cloud infrastructure, but use its flexibility. It is important for organisations to read carefully the option regarding dedicated physical hardware resources in the cloud offer, as the implementation may vary from host to host. For example, Amazon Web Service (AWS) has the option to run dedicated instances in a virtual private cloud on hardware dedicated to a single customer or account. While the physical isolation is guaranteed, dedicated instances may share the same underlying physical hardware with non-dedicated instances from the same account, and this can be exploited when a single account is running a multi-tier application with several components, running both on dedicated and non-dedicated instances. Another option for organisations that want to drastically reduce risk is to deploy an on-premises cloud; this option will require more management effort from the organisation, but will allow to maintain the same performance.

Private infrastructure: Organisations can try to mitigate the risk on privately maintained infrastructure, and many vendors are offering mitigations at various levels of the computing stack: processors, hypervisors, operating systems, and software.

Risk acceptance: The use of cloud computer architecture changed how organisations assumed risk. The most used solution is multi-tenant cloud, and best practices are devised to minimise risk for cost savings. Such an approach can work well, especially for smaller organisations, when the computed data is less sensitive. However, for organisations that prefer to have complete control over the compute resources, the higher costs of an on-premises cloud solution can be viable. In such way, an organisation with an on-premises cloud solution can choose to not apply the mitigations which may heavily degrade application performance. A hybrid approach which uses on-premises cloud for sensitive data and the public cloud for non-sensitive data can also be a solution.

5.5.3 Content Delivery Network (CDN) manipulation

Content Delivery Networks (CDNs) are frequently being used as a target due to the ease at which an attacker can use the trust relationship of the user to the provider to manipulate the user's machine. For example, there have already been a plethora of attacks which leveraged Office365 to gain entry into victims' machine, while Azure and AWS are also prime targets.

Challenge:

Attacks based on social engineering and manipulation of CDNs are not new, but they will still represent a threat in the future. In the second quarter of 2019, according to the Positive Technologies report (2019), there have been attacks on Steam, Azure App Service, and AWS. On Steam for example, users were lured to enter log credentials on a website where they had been lured with the promise of a free new game. Within Azure, criminals launched several types of frauds deploying phishing pages with fake login forms or creating fake

Microsoft technical support pages with popups alerting of an ongoing infection by a non-existent virus. Also, emails have been sent prompting to download a file, after logging in via a fake form hosted on Azure Blob Storage.

Mitigation:

A solution to the specific Azure Blob Storage attack is described in the above article, consisting of setting a custom rule, to stop emails containing windows.net domains (since official login forms hosted by Microsoft would use Microsoft.com, live.com or outlook.com). In general, users can protect themselves against these attacks using complex passwords, setting different passwords and email addresses for each site or account used, and keep changing passwords every two or three months. Moreover other security practices can help avoid being victims of social engineering, such as scanning all email attachments with antivirus software, checking certificates when visiting a website, paying close attention every time a password is a requested, or a security warning appear, do not click on popup windows, even if the advertised product is known, and avoiding downloads from suspicious or unknown sources.

Opportunities:

The cybersecurity challenges described above, are closely related to the identity management issues of cloud services in general, thus the opportunities described in Section 5.5.1 apply also in this case.

5.5.4 Data confidentiality and privacy in cloud environment

Secure data storing and processing in public and hybrid clouds are another technical challenge. An example is the privacy of security policies in Security-as-a-Service (SecaaS) services, where it is necessary to expose to the cloud service provider the customer's security policy which may contain confidential information regarding the organisation's infrastructure, vulnerabilities, and threats. As the concept of a hybrid cloud is to allow an organisation with an existing private cloud to partner with a public cloud provider, it allows companies to keep some of their operation in-house, while benefiting from the scalability and on-demand nature of the public cloud. However, there are some issues that arise when users take advantage of using hybrid clouds; in particular, since the first part of hybrid cloud is owned or operated by a third party, this can lead to security concerns, while with a true private cloud (hosted entirely on your own premises) the security concerns for an IT manager are no different to those associated with any other complex distributed system.

Challenge:

Issues that are related through to cloud services are connected with compliance, privacy, trust, and legal matters. Data security becomes particularly important in the cloud computing environment, since data are scattered in different machines and storage devices, including servers, PCs, and various mobile devices, such as wireless sensor networks and smart phones. Data security in the cloud computing is more complicated than data security in the traditional information systems. Therefore, to make the cloud computing be adopted by users and enterprises, their security concerns should be addressed in order to make cloud environment trustworthy. The trustworthy environment is the basic prerequisite to win confidence of users to adopt such a technology.

Mitigation:

Data confidentiality: Encryption is typically applied in order to ensure the confidentiality of data and to this end, homomorphic (and partially homomorphic) encryption methods for secure cloud computing have been studied (e.g., Farokhi, Shames, & Batterham (2017) and Alexandru, Morari, & Pappas(2018)). The most secure cloud encryption environment (considering it runs in the cloud) is to separate the three components

involved in the encryption process: key, algorithm, and data. In this way, even if one of them is compromised, the attacker still needs to compromise the other two. This allows to gain time in order to secure the data, provided that the first attack is observed. In addition, a message authentication code is generated which it transmits along with the encrypted data to cloud. This is a small fixed size block of data that is generated based on message/file F of variable length using any secret key. It is called cryptographic checksum and is used to check whether data has been tampered throughout the transmission and this check can be made by the user or owner of data on retrieving the file.

Data integrity and retrievability: In the case of Storage-as-a-Service (e.g., storing encrypted data in a public cloud), it is also important, aside from confidentiality, to implement an integrity mechanism that confirms that no one tampered with the data. This can be achieved through digital signatures. There are some data retrievability mechanisms that allow users to confirm whether their data is still intact in the cloud.

Data lineage and provenance: In addition to protecting data, security also ensures that audit procedures can be operated. These procedures serve not only for forensic evidence in case of an attack, but can also help the customer better understand how their data is being manipulated in the cloud, so that appropriate security measures are employed. In such a dynamic environment as the cloud, it is desirable to keep track of the data lineage, i.e., where each particular piece of data was at any given moment of time. As the cloud infrastructure operates with virtual devices, this lineage tracking should be extended to virtual instances as well. Because of the high dynamism in the cloud, it is very difficult to collect extensive information on data lineage, such as the state of the systems dealing with each data piece. In fact, it is likely that the only information collected is limited to e.g., IP addresses, country where a specific host resides, host name, host domain and time stamp. Nonetheless, this information alone is relevant and important in many cases. In some applications it might also be relevant to consider data provenance which describes where and when data originated.

Opportunities:

Homomorphic and semi-homomorphic encryption approaches have been employed for ensuring confidentiality in cloud computing services, by mainly focusing though on static control laws without any form of memory. The need though for incorporating dynamic control laws (even at the cipher stage) is apparent and several opportunities arise for cases where an encrypted memory/state should be maintained remotely.

5.6 AI and Big Data analytics

5.6.1 Adversarial Machine Learning

Attacks based on Adversarial Machine Learning aim at identifying and exploiting vulnerabilities within AI systems in order to cause changes in the behaviour of such systems. Adversarial attacks include the poisoning of training data and/or the altering of learning algorithms, such that adversarial perturbations of the input data performed during the training stage and/or at inference time can subvert the performance of AI/ML algorithms.

Challenge:

The significant effectiveness of AI/ML techniques in detection and prevention solutions, such as in malware detection and intrusion detection and prevention (IDS/IPS) systems, has resulted in their increasing adoption as cybersecurity defence solutions. This has though created an additional attack vector, namely the actual data-driven models underlying these AI/ML approaches, which may also be themselves subject to cyberattacks through Adversarial Machine Learning. Here, the ultimate goal is to alter the behaviour of the underlying system by automatically introducing slight perturbations in the training data (referred to as “adversarial samples”) that would result in potential misses by the detection systems, thus allowing adversaries

to bypass them. For instance, the introduction of slight perturbations while training the classifiers employed by such detection systems could cause the decision boundary to change and thus misclassify any adversaries at inference time (Thomas, Vijayaraghavan, & Emmanuel, 2020). Similarly, an adversary may perturb some features of a malicious attack or intrusion at inference time in order to circumvent the available detection systems; for example, malicious network traffic can be hidden by injecting and/or mimicking features of legitimate network traffic in order cause a misclassification by the detection system.

Mitigation:

Training AI/ML systems with adversarial examples is typically used as a security mechanism to test the robustness of such models, and to help protect such systems from attacks. This practice is gaining popularity, and several AI researchers have created open-source libraries of adversarial examples for this purpose such as IBM's Adversarial Robustness Toolbox (albeit not necessarily focused on the cybersecurity domain). Other research has made progress toward universal protection against well-defined classes of adversaries.

Opportunities:

In the quest to develop adversarial-resistant and/or adversarial-aware AI/ML approaches, several opportunities arise. Adversarial Machine Learning could for instance also be leveraged to develop AI/ML security systems (such as malware detection systems and IDS/IPS), though this will probably always be one step behind attacks. Nevertheless, the resources that could be used for the development of such cybersecurity systems will likely be greater than those used for the attacks. Moreover, ensemble learning approaches that leverage multiple classifiers based on a variety of AI/ML approaches have the potential to make it more difficult for attackers to evade such detection solutions.

5.6.2 Malicious use of AI

As discussed, AI is an attractive target for attackers since they can attempt to manipulate algorithms or the data that these algorithms rely on in order to influence the results. However, apart from influencing the behaviour of any AI-based systems, malicious actors could also launch AI-based cyberattacks.

Challenge:

As evidenced in many of the challenges analysed in this deliverable, AI is being widely used on the defensive side of cybersecurity. AI can also though be used to launch cyberattacks, e.g., attackers could develop algorithms to discover what types of malware will be the most effective in certain environments, or what type of users are the most susceptible to spear phishing. To the best of our knowledge, and based on publicly disclosed information, AI for the offensive side of cybersecurity has been used up to now only by "white hat" researchers (Brundage et al., 2018), who aim to increase cybersecurity through finding existing and potential vulnerabilities and suggesting solutions. This does not preclude that AI has already been used by malicious actors in a manner that has remained undetected, and, if not, it is highly likely that AI-based cyberattacks will soon take place in the wild.

In particular, AI-based malware and AI-based password brute-force attacks are considered among the most prominent case studies of AI-based cyberattacks (Kaloudi & Li, 2020). For example, DeepLocker (Kirat et al., 2018) is a highly targeted and evasive malware, which conceals its malicious intent and is only activated when it reaches specific targets, while smart malware (Chung et al., 2019) is a self-learning malware, which performs malicious attacks that are masked as accidental failures on critical infrastructures. On the other hand, AI-based password brute-force attacks have focused on either constructing the attacking dictionary based on prior passwords (Trieu & Yang, 2018) or by learning the distribution from actual password leaks (Hitaj et al., 2019).

Mitigation:

Defensive solutions to such types of AI-based attacks have not been implemented yet, but the researchers introducing the aforementioned case studies have suggested some countermeasures. For example, Kirat et al. (2018) proposed the use of cyber deception to misdirect and deactivate malware, while Chung et al. (2019) suggested as potential mitigation approaches the of IDS/IPS in the control network, stricter security policies multi-factor authentication, and system-level security monitoring to validate the physical aspects of measurements.

Opportunities:

The possible malicious uses of AI are as boundless, as are its beneficial ones, but attackers will probably always have the advantage of surprise as well, able to test their creations against existing protection, and also use adversarial machine learning to hone their attacks. Nevertheless, there appear to exist several opportunities to research and develop AI-based defensive solutions against AI-based cyberattacks, while the use of Explainable AI (particularly in critical cases) could help to prevent malicious (or accidental) changes or insertions into the code.

5.6.3 Disinformation, fake news, and deepfakes

Dissemination of deliberate disinformation - colloquially referred to as ‘fake news’ or ‘pseudo-news’ - is a relatively recent phenomenon in modern society (Lazer et al., 2018). Such practice is predominantly facilitated by social media networks, which escalates the scalability of propagation (Allcott and Gentzkow, 2017). The widespread distribution of misleading information tends to be a harmful and malicious endeavour, wherein it can negatively impact individuals’ perceptions, behaviours, and attitudes (Ştefăniţă, Corbu, and Buturoui, 2018). Such disinformation campaigns are supported by AI, enabling them to become more targeted and effective and greater in scale. Moreover, AI technologies also make it easier to manipulate video/audio files, which has intensified concerns about trust in communications. These variants of synthetic media are colloquially referred to as a ‘deepfakes’ (a portmanteau of “deep learning” and “fake”), whereby an individual in an existing video/audio is virtually replaced with someone else's likeness in appearance and/or voice (Floridi, 2018). Both disinformation campaigns and deepfakes could be employed by cybercriminals and hackers, e.g., in phishing emails or social media posts, or even chatbots embedded in websites, to socially engineer victims into clicking links, downloading malicious files, or sharing private information.

Challenge:

AI technologies support disinformation campaigns, enabling them to become more targeted and effective and greater in scale (Woolley, 2020). These campaigns are capable of inciting fear, instability, and hatred, which can be used to undermine democratic systems and processes or to target minority populations. Moreover, the spread of disinformation can lead to many harmful outcomes, including widespread loss of trust in media communications. A recent example of the interplay between of spreading of fake news and AI surrounded the 2016 presidential election in the United States, whereby it was discovered that social media bots (i.e., spam accounts that post autonomously using pre-programmed scripts) accounted for a surprisingly high percentage of posts (Allcott and Gentzkow, 2017). Between the first two presidential debates, for example, the Atlantic reported that a third of pro-Trump tweets and nearly a fifth of pro-Clinton tweets were generated by fake, automated accounts, also known as ‘bots’ (Guilbeault, and Woolley, 2016). Bots of this kind are not only used to build political support, but also for other purposes closely associated to cybersecurity threats and challenges, including the social engineering of victims to downloading, for instance, malware and other malicious files.

AI capabilities have also made it easier to manipulate video/audio, which has intensified concerns about trust in communications. The creation of ‘deepfake’ videos relies on an artificial neural networks, called

autoencoders, wherein large databases of images are needed to instruct and shape the software to synthesise human images (Maras and Alexandrou, 2019). Given the sheer quantity of images and video footage that is needed to reproduce videos, individuals in the public eye are more at risk of being 'deepfaked' (Floridi, 2018). Worryingly, audio can also be deepfaked, to create "voice skins" or "voice clones", which have been used in the creation of fake news, misrepresentation of well-known politicians, hoaxes, and financial fraud through phishing attacks (Westerlund, 2019).

Mitigation:

While these are relatively recent phenomena, given the rate by which 'fake-news' and 'deepfakes' are disseminated, there is a growing need to mitigate the harmful influence that these synthetic variants of media present to the general public. One innovative way of mitigating 'fake news' pivots on the adoption of AI/ML techniques as a means of detecting, and indeed eliminating at least some of the fake news before it reaches the user. Several applied examples of this process have been shown by multiple research efforts (Wu et al., 2019), while industry also has a vested interest in this, and thus a number of start-ups have also integrated AI/ML technology into similar products to combat the spread of disinformation (Lomas, 2019 via Techcrunch).

With respect to 'deepfake' videos and audio and the potential cybersecurity risks, it is apparent that education is the strongest long-term solution that exists to combat the proliferation of this problem (Chivers, 2019 via The Guardian). While this mitigating solution is trickier to implement and possibly a slower means of garnering results, it is achievable. This means of mitigation would involve informing the general populace about the existence of 'deepfakes', combining critical thinking and digital literacy, in which our best defence is to produce informed digital citizens (Naffi, 2020 via The Conversation). Individuals in society need to learn to treat even the most realistic videos with some degree of skepticism. The rollout of this form of education could be operationalised through a number of channels, whether it by traditional means (i.e. delivered as part of information technology and computer science qualifications) or included as part of a IT threat awareness programme in academic curricula. Moreover, the media should ensure that only factual footage is reported upon and should lobby for the general public to only rely on factual sources.

Although it is may be considered a difficult task, there is a growing need to develop technology that can better detect 'deepfakes'. While AI/ML is a central piece in the creation of these fake contents, it is necessary to create a counter-technology that is capable of detecting these, so as not to depend on human intuition solely. Moreover, social platforms should recognise and address this potential threat as soon as possible, as it is through these platforms that fabricated videos are most likely to spread and have a detrimental impact on society. A possible mitigation venture could be the development and inclusion of a filtering system (that is AI driven) that systemically screens tweets, posts, uploads, links, videos, etc. Industry has shown some promise in this area, particularly with respect to combating technologies such as 'deepfakes' with initiatives such as the launch of the "Deepfake Detection Challenge" (DFDC; Dolhansky, et al., 2019), which seeks to promote the development of technology capable of combating the impact of 'deepfake'.

Opportunities:

With regards to mitigating the damaging influence of 'deepfake' videos/audios and 'fake news' and the cybersecurity threats these entail, it appears that focused and sustained investment towards educating the general population is crucial. Indeed, governments must educate and equip their citizens to be in a position to recognise fabricated content and discourage its sharing. Moreover, while these are relatively recent phenomena, they are rapidly developing, mostly attributed to the innovative nature of AI/ML techniques. While recent research has detected that biases currently exist in fake news datasets (Gordon, 2019), the means of adopting AI/ML for detecting misinformation and deep fakes is a growing field which is constantly improving. Such AI/ML algorithms will become more fine-tuned and accuracy benchmarks will improve across time by virtue of conducting more research and investing more towards developing such databases and developing

such technologies. Consequently, more investment in technology, but also education, appear to be most fruitful ventures towards reducing and potentially eradicating the proliferation of such AI/ML-based fake artefacts.

5.6.4 Big data security

"Big Data" security covers many different fields. From the devices (or people) which produce the data, to the machines on which the data is stored, to the algorithms used to process the data, and also touches upon the entities which the data is about. "Big Data" refers to the collection, storage, and processing of large amounts of data; this can clearly have benefits for those who wish to extract useful information from the data, but makes the data and/or its processing a valuable target to attack as well. Beyond considering how one may attack "Big Data" in general, we can also consider using Big Data to formulate attacks or its use in detecting and mitigating attacks. Many of the areas discussed here are also discussed in other sections of this document, but it bears repeating how they are related to Big Data, and that attacks on these areas present a problem for obtaining the useful information which might come from such data processing.

Challenge:

Big data starts with inputs; these could be obtained by a literal sensor of a physical variable (like temperature), which may be an IoT device, or they might be the inputs of a large number of users and/or associated network traffic. While many physical sensors have a great deal of noise, one generally assumes that their measurements are centred around the actual value. However, if IoT devices are not properly secured (both physically and electronically) they may be tampered with to produce a systematic bias, or, if their inputs are sufficiently important, have their inputs simply stolen. With regards to data coming from human or network activities, the data processing one wishes to do, or the outputs one wishes to produce, depend on having real data. As such, it is important to filter out all bot activity before beginning the processing (both in terms of time and cost of processing and because of the possible skewing or pollution of the results). As bots become better (mainly due to AI technologies), this filtering becomes more difficult.

After the collection comes the storage of such big data. As such data may obviously be confidential or private, and thus may be very valuable both to the entity owning the data and to thieves, it is clear that all data security best practices should be considered. But the application of such practices may be challenging given that it may be impossible to anonymise the data, and also the data may exist as a distributed database over many servers. Controlling access to these servers and the data they contain, physically and electronically, may be vitally important, meaning that there is need to apply defence in depth for both physical and cyber-security, and also consider the encryption of the data whenever possible.

The next step concerns the processing of such data. Efficient processing of huge databases/logs for detecting malicious activities (e.g., for intrusion detection) is an ongoing challenge. Such processing is important because of the need for the detection of anomalies and malware to prevent attacks which are not easy or even possible based on selected logs from one network device/system (sometimes only correlation between logs allows us to predict/detect network attacks or malware campaigns). In case such data has been corrupted, the processing may give incorrect results, and therefore there is a need to spend more resources on pre-processing (or filtering corrupt data), or the results we can obtain (after proper filtering) may be much more limited than expected. In addition, leaving aside the effects of faulty/corrupted data, methods of data processing themselves may be open to various forms of attack or manipulation (as discussed in the previous sections). Beyond "gaming" the processing of data, either through implicit or explicit knowledge of the processes, if the processing machines are not properly secured, the processing algorithms themselves may be tampered with by a malicious actor.

Finally, we discuss about the results of big data processing. Clearly these may be influenced by tampering or corruption at any of the previous steps, but even if everything has gone according to plan, we should be careful about how results are presented, if, for example, we must maintain the privacy or anonymity of the origin of the data. This may require aggregation of the data at a coarser level than what might be expected, as sometimes uniquely identifying information can be obtained from just a few fields of information, even if obviously identifying information such as name or identification number is excluded; this question should generally also be addressed at the very beginning of data collection.

Mitigation:

There are no particular mitigation strategies which apply only to Big Data, except perhaps diligent filtering and pre-processing of data to determine if it is clean and free from tampering. Accidental breach of privacy is one of the greatest concerns related directly to Big Data. This should be handled at all stages: when the data is sourced, how the data is stored and accessed, and how the data is aggregated, processed, and presented at the end.

Opportunities:

Big Data analysis provides a great opportunity for cybersecurity as well as potential applications are almost limitless, bounded only by the capital we are willing to invest and our creativity. Analysis of network traffic to spot intruders or malware infection is a great example of an application of Big Data, but many others abound.

5.7 Data security and privacy

Data security and data privacy are strongly interconnected, but they are not the same. Data privacy, on the one hand, is a part of data security and is related to the proper handling of data, e.g., how you collect it, how you use it, and how you maintain compliance. Data security is about access and protecting data from unauthorised users through different forms of encryption, key management, and authentication.

5.7.1 Breaches and data leaks

With data's expanding importance, information security is evolving into a critical aspect for organisations, as the risk of sensitive data being breached (due to intended or unintended incidents) increases at an alarming pace, and the challenge is to be one step ahead of the cybercriminals. The digital transformation implies that changes in the organisations are necessary since newly adopted technologies open up new risk profiles that companies cannot lose sight of.

Challenge:

The digital transformation initiated by most organisations has required the change of their processes, including the development and deployment of new business models with highly technological components, requiring either new technical profiles or the adaptation of existing ones to support the speed of these changes. This transformation process has had a direct impact on cybersecurity, forcing companies to perform vulnerability analyses in order to reduce the possibilities of being a victim of a cyberattack or a data breach. Management teams have been immersed in new paradigms that require their capabilities to continue to maintain the existing business 'in flight', while adapting to the new digital context. According to a study carried out by the Ponemon Institute in 2018 in different countries (Ponemon Institute Research Report, 2018), 72% of IT security professionals believe that the urgency to achieve digital transformation has increased the risk of suffering a data breach, particularly since 45% of the reported organisations did not have a strategy to face the digital transformation.

Therefore, for the teams in charge of security management, it becomes a primary requirement to have a constant flow of information about all the changes that occur within the organisation. For this reason, threat monitoring and intelligence technologies are important to them since they provide the foundation on which other processes can be executed safely and maintain compliance throughout the organisation. Security management teams require a constant flow of information both externally and internally about changes within the organisation. For this reason, threat monitoring and intelligence technologies are critical to ensure that the rest of the organisation's processes can be executed safely and in compliance with internal and external regulations.

Mitigation:

Organisations should thus consider information security as an integral part of their digitisation. Given that such digitisation is developing along with a set of technologies being developed in parallel, such as cloud computing, 5G, IoT, and Big Data/AI/ML, an analysis of the security of the data delegated to these technologies is required to allow business continuity, since these new contexts create great opportunities to extend the attack surface undoubtedly taken advantage by cyberattackers.

This digitisation, which has been gradually introduced into organisations, has not taken in most cases cybersecurity into account. Given the importance of protecting the company's assets, which today more than ever are distributed across different servers around the world, the choice of appropriate protection services is not trivial and must take into account critical aspects, such as the damage to the business that could be caused by the possible leakage of data from different points of view, such as reputation, loss of secrets, or aspects of legal non-compliance. Therefore, the mitigation aspects must consider a complete strategy where on one hand all legal aspects are complied with, but also all necessary steps are taken in order to guarantee the continuity of the business and the protection against any attack. Security teams must focus on taking advantage of monitoring technologies and not only on detection technologies. It is important that companies include in their processes the mechanisms to respond to an incident that will allow them to return to operation as soon as possible, by solving the incidents and applying the appropriate corrective measures.

The new data protection regulation (GDPR) affects the privacy of users and customers, providing the latter with new, stricter frameworks for the protection of personal data. This situation generates new contexts where people are beginning to know their rights in greater depth and are more interested in knowing how organisations can manage their data. Organisations that, on their own initiative, define strategies to generate confidence in their clients will have an advantage when it comes to fostering long-term commercial relations

Opportunities:

There are several opportunities in the process of the digital transformation of organisations that concern the protection against breaches and data leaks. Among them, the following can be highlighted:

- Cybersecurity should be considered from the design up to the deployment of new technologies. Security is an enabler of business or rather it should be an attribute that is present in all activities and processes, since not considering cybersecurity in the deployment of new technologies will cause more problems than solutions.
- While the focus should be placed on incident prevention, incident detection and response should also be considered. This requires an analysis of the technologies to be incorporated into an organisation.
- The approach to security cannot rely solely on the security of individual devices and thus an integral vision of security is required to address security as a whole. It is at the edges of technologies, devices, different roles, etc. where a system is most vulnerable, since cyber threats are most likely to find a niche to attack and violate the security of an organisation.
- In today’s data world, decisions are often based on data generated from the implemented technologies. In these contexts, the 'appropriation' of data by specific people is not permissible, while

though this new context also requires greater collaboration and alignment among people and processes.

- The digital transformation is nothing more than the transformation of the people that make up a company using new technologies and this situation requires putting people at the centre of the strategy. People who behave differently in their social contexts to those at work may assume greater risks. While this did not pose many problems in the past, it can pose serious problems for organisations in today's world with everything interconnected, since their information can be vulnerable to social engineering attacks.

5.7.2 Brute-force attacks

A brute force attack is a technique of breaking a cryptographic system where the attacker checks all possible keys. It is possible to launch such an attack both on symmetric and asymmetric cryptographic systems, and its effectiveness depends on the number of keys to check, and the time required to check a single key (key length). Defenders can protect themselves with a secure key management, which in real-life cryptographic system is one of the most important aspects of its security.

Challenge:

A cryptographic algorithm (cypher) is applied to encrypt a non-encrypted message (called plain text) or vice-versa to decrypt an encrypted message. Mathematically it can be described as a function depending on a parameter, called the key, which is used for encrypting and decrypting. Formally we can write: Encryption $E_K(M)=C$, Decryption $D_K(C)=M$; $D_K(E_K(M))=M$, where E is the encrypting function, D the decrypting function, M the plain-text, C the encrypted message, and K the key.

We can distinguish symmetric (or secret-key) cyphers and asymmetric (or public-key) cyphers. In the former, the encryption key can be calculated from the decryption key (the two could also be the same), and the security of the algorithm is based on the secrecy of the key. Symmetric ciphers require that the receiver and sender of the message have in advance the respective keys, and are thus responsible for keeping them secret.

In asymmetric or public key ciphers, encryption and decryption use two different keys, a private key is used to decrypt, and a public key is used to encrypt; in addition, it is not possible to calculate the decryption key from the encryption key. The encryption key is called the public key because it is not necessary to keep it secret, and everyone can use it encrypt a message. However only the receiver with the respective private (and secret) key is able to decrypt the message. Thus, asymmetric cyphers do not require any prior exchange of keys between sender and receiver. However, it is necessary to add a signature protocol to ensure the authentication of the sender, based on the sender private key.

Different cryptographic systems have different levels of security, depending on how difficult it is to break them down and how long the encryption key is. Thus, the security of one symmetric cryptographic system depends from the strength of the algorithm and the length of the key.

Mitigation:

Most attacks to cryptographic systems are directed to some weakness in the key management, so secure key management practices can mitigate or prevent brute force attacks. Key Management should thus cover: (i) key generation, (ii) key distribution, (iii) use of the keys, (iv) storage of the keys, (v) time (period) of use of the keys, (vi) key change, and (vii) destruction of keys.

Key generation: Since the strength of a cryptographic algorithm is based on the key used, generating keys is the first problem to solve. Bad practices to be avoided include reduction (limitation) of the key length and selection of a bad (weak) key; the ANSI X9.17 standard defines one method for generation of good keys and includes the use of cryptographic algorithms.

Key distribution: The key distribution's security is covered via the use of master key or key encryption key, and crypto algorithms with public keys (especially important for big computer networks).

Use of the keys: Software tools for encryption carries some risks; in particular, the availability of multi-user and multi-task operation systems is a precondition for compromising the key, while the use of hardware solutions is preferred, but it is much more expensive.

Key storage: The possible solutions for key storage are: (i) remembering the key, which is impossible for real complex systems, (ii) storage of the key on separate technical media (electronic or magnetic), sometimes consisting of two or more parts, (iii) storage of the key in an encrypted format, and (iv) a combination of the above methods.

Time (period) of use of the keys: Keys cannot be in use for unlimited time periods; there must always be a policy that defines the time of use of the different keys. The criteria to define this period depend on the purpose, the frequency of use and the type of cryptographic algorithm used.

Destruction of keys: Once keys have changed, it is necessary to destroy old keys; key destruction methods however have to prohibit the second use of the old keys. In computer networks, this could be problematic due to the possibility that the keys are easily copied and stored in many different places, the existence of memory controlling processes, the existence of swapping processes and the existence of buffering. Therefore, it is necessary to create a model of distribution of keys, addressing the following requirements: (i) users' characteristics change often, (ii) users do not have access to the distribution, control or translation centres, and users communicate via open (non-secure) channels.

Opportunities:

As discussed in Section 5.6.2, next-generation brute-force attacks will leverage AI technologies and therefore there is a need to develop defensive strategies against such attacks. To this end, there are opportunities towards developing advanced techniques for the early detection of such attacks, while defensive strategies will need to re-evaluate password policies and can include the combination of several multi-factor authentication mechanisms for efficient and secure authentication.

5.7.3 Credential theft

Login-password credentials are the most widely used for authenticating users in both their physical and digital lives, but there exist many other systems for such purposes, e.g., digital private keys, digital certificates, session cookies, cryptocurrency wallets or those more related with hardware devices like physical keys to tokens and cards. All of them are types of credentials, and any credential is vulnerable to be attacked.

Challenge:

Credential theft is a type of cybercrime that involves the unlawful attainment of an organisations' or individual's credentials with the intent to access and abuse/exfiltrate critical data and information. Often an early stage of a cyberattack starts with credential theft, enabling attackers to operate undetected throughout a network (e.g., reset passwords, lock the victims out of accounts, download private data, gain access to cloud service, etc.)

with the same account privileges as the victim to wreak havoc within an organisation. Credential theft should be a high priority for all the organisations independently of their size, but with the advent of IoT more and more industrial control systems and other critical infrastructure are also vulnerable to credential-based attacks.

There is an extremely broad market on the Dark Web where criminals can purchase stolen credentials. It is in such markets where illegal activities allow criminal to open doors to organisations and their customers. According to Blueliv[5], 81% of hacking-related breaches leverage either stolen or weak passwords. Motivations range from data breach to leverage corporate accounts, to impersonate corporate VIPs on social media, or email communications to damage reputation, or instruct fraudulent financial transactions. The lifecycle of credential theft could be divided in four phases (i) gathering data, (ii) filtering and extracting, (iii) validating manually or by using botnets or account checkers, and (iv) profiting by selling credentials or using directly.

Credentials can be obtained using multiple mechanisms and tools, all of them cheaply acquired in the underground. Malware infection, phishing, vulnerabilities, social engineering, man in the middle, brute force attacks, DNS hijacking, and leaked databases are the techniques used to extract credentials. Some of them, like phishing is based on human interaction, unlike malware and exploits, which depend on vulnerabilities in security defences. Phishing is actually one of the most widely used techniques for credential theft and is constantly evolving especially in the corporate environment, where attackers make the emails and websites look the same as current corporate applications and communications.

It is quite common to consider that a good password construction, in complexity and length, is sufficient to keep the credentials secure. In reality most of the methods used in credential theft are based on stealing the exact password rather than guessing it. Based on stealing the exact password is how keystroke logging acts, in which malware virtually watches a user type in their password, is another method of credential theft that works regardless of password complexity.

Mitigation:

Identifying credential theft attacks early and mitigating them in seconds is critical when working to protect sensitive data. In order to mitigate credential theft, there is no unique approach, but what is proven is that the more techniques are deployed, the more difficult it becomes to get access for a criminal to credentials. One possible option is to monitor activity and identify use of credentials that violate heuristics, for example, when a user is accessing from a location that is anomalous or multiple logins in a short duration of time across the network that clearly appear to be programmatic, rather than human initiated. Advanced network traffic analysis tools that use machine learning engines and deep learning techniques are now available to autonomously detect for credential theft.

A single sign-on (SSO) solution means users only have to keep in mind one credential that grant them total access to the authorised corporate services, like email and business applications (if SSO is not totally integrated along the organisation, the services accessed could be partial and it would be a weaker solution). If SSO is combined with education/training about the dangers of password sharing, SSO will help to reduce the likelihood that end users compromise password security for the sake of convenience.

In many cases, further analysis reveals that the attack could have been avoided if the organisation had followed standard security hygiene practices like patching operating systems, apps, etc. or protecting identities by adding multi-factor authentication (MFA). MFA helps to render stolen credentials useless because it requires a user to enter a second form of identification for access (e.g., a temporary code sent securely to a separate

[5] https://www.blueliv.com/the-credential-theft-ecosystem/

device like the user's smartphone). So, with MFA activated, a stolen password is not sufficient to breach an account, thus creating, jointly with the traditional password, one of the most effective solutions to combat credential theft.

Network controls should also be checked. On-premises wi-fi access should be secured with an up-to-date Radius server and individual credentials to internet access (there are organisations with communally shared password). The same password best practices apply for on-site file storage and other LAN resources.

Moreover, organisations should follow some best practices to mitigate credential theft, such as privileged access management (PAM) best practices, accessing only approved applications via corporate credentials, blocking usage from unlikely or unknown applications and websites, keeping updated the software with security patches (OS, devices, etc), using encryption and endpoint security to secure identity storage, and assessing vulnerabilities frequently. For consumers, the best protection solution would be regularly change passwords and use MFA wherever possible.

Opportunities:

There are multiple techniques for mitigating the effect of credential theft on users, but perhaps the most interesting is the work on educating users on proper use of credentials and compliance with best practices. All the security products in the world cannot protect an organisation if the criminals have the right key to open the door, given that the organisation's resources can be compromised by credential theft if a user shares a password, or slightly different versions of the same password, across a variety of accounts. Their credentials might be well-protected at work, but they could be stolen from a less-secure personal account and used by a criminal later. Education and awareness of the importance of security thus becomes a fundamental pillar in combating this type of attack that causes serious damage to both organisations and individuals.

5.7.4 Unauthorised access

Unauthorised access presents a real and pervasive risk to cybersecurity. It occurs when a threat actor gains access to computer systems by elicit means to harvest confidential information.

Challenge:

This challenge can be operationalised in many ways, including accessing information via plug-in devices (e.g., USB flash drives), data leakage, credential theft, malware, and ransomware

USB Thief Trojans: Data theft can occur when a threat actor inserts a USB flash drive into a computer containing malicious software, such as the "USB Thief", that is capable of attacking systems isolated from the internet. This type of malware does not install on the victim's computer, but rather works stealthily in the background typically hidden in a DLL of some other application, such as a web browser. Thus, USB Thief Trojans do not show any hallmarks of being present and are usually only discovered once data has been harvested, or in the worst-case scenario, are not detected at all.

Data Leakage: The trading of large databases containing hacked, sensitive data on the internet, usually via the Dark Web, has become a widespread global practice (Missaoui et al., 2018). Sensitive data in this context represents passwords, banking details, classified information, and information linked to individual's identity (such as their name, credential access to computer systems, mail addresses, etc.) which were illegally garnered. Leakage of this information can allow threat actors access to individuals' personal accounts (financial, employment, health, etc.). Additionally, this risk could represent a potential larger-scale vulnerability

in organisations mainframes and servers, wherein credentials are stolen with the objective of accessing and exfiltrating critical data.

Malware: The utilisation of malware to infiltrate systems and gather sensitive data is a highly prevalent practice Malware is a software which, once executed on a computer system, can damage the user files and also cause harm to the system itself, by deleting, damaging or modifying stored information or stealing credentials of users. As malware has become increasingly sophisticated over time, it has become harder to detect and destroy.

Ransomware: Ransomware, also known as cryptolocker, presents a significant threat to users and mainframes. The primary objective of this malicious type of malware is to prevent the victim access and use of documents and devices. The attacker then blackmails the victim by asking for a ransom for the release of inaccessible resources, a phenomenon termed as “digital extortion” (Bhardwaj, 2017). While simplistic in execution, ransomware can have devastating effects on end-users, not only in the digital sense (i.e. loss of personal or company data; possibly a complete shutdown of an organisations’ operations), but also in a societal context, wherein blackmailed victims fear damage to reputation, financial loss as a result of revenue generating operations being shut down or loss associated with remediation efforts (Al-rimy et al., 2018).

Mitigation:

At a systematic level, to mitigate the likelihood that a system could get hacked, it is necessary that all wireless networks are configured with Wi-Fi Protected Access 2 (WPA2) security algorithm and access passwords are replaced periodically. Unauthorised access is considered a major concern in industry, thus in an effort to reduce breaches to corporate systems through the internet, networks are now protected with prevention tools such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

Mitigation Techniques for USB Thief Trojans: With respect to mitigating illicit entry via USB devices, it is essential that users are educated on the secure management of the removable media and any risks related to the use of unauthorised devices. Thus, the regular delivery of security awareness training programmes can be very beneficial towards raising the awareness on the potential risks that plug-in devices present. Businesses could also be proactive with regards to device/systems management by maintain an inventory of systems, devices, software, and services which are under the remit of the organisation. Moreover, it is crucial that such an inventory, irrespective of how extensive it is, should be kept up to date, in that older devices are correctly disposed of and newer updates are recorded. Crucially, critical information and data also need to be identified in the first instance, and protection protocols for these are enforced.

Data Leakage: With regards to mitigating data leakage, the poor management and the lack of monitoring of personal data within the organisation can cause or facilitate the leak of personal data, belonging to employees and users. Thus, it is necessary for organisations to have at least one manager who is trained exclusively on the management of data and personal information. Further to this measure, it is also vital to instil the following measures to employees: (i) maintaining strong access credentials, (ii) encouraged to regularly update credentials, and (iii) instructed not to share passwords or sensitive data. With regards to password creation measures, it should be relayed that strong passwords need to be at least twelve characters in length, containing letters, numbers and symbols; likewise, users should be prevented from using the same password twice. While employees have a vital part to play in the prevention of credential theft, so does industry, wherein organisations should ensure that security controls are strong at a technological level, with the implementation of privilege control and multi-factor authentication.

Malware: While spyware and malware are constantly innovating, periodic updating of systems and mainframes allows the means of detecting and blocking new iterations. Although the use of anti-malware software is necessary, these cannot offer a full protection. Therefore, it is essential that all staff are trained to

maintain a proper level of security. Synchronously, in industry, the use of protection systems can reduce the probability of infection or at least, through network traffic analysis tools, provide indications on a possible malicious event.

Ransomware: Ransomware can have detrimental effects on users; however, frequent and systematic security awareness training would be a key area for improvement in protecting organisations against ransomware. With regards to mitigation measures in industry, the rollout and consistent updating of anti-malware software would be the best defence towards combating the newest cryptolocker threats.

Opportunities:

While unauthorised access is highly prevalent, it does not have to be inevitable. It is apparent that the implementation of a few key mitigation measures, could reduce or prevent the likelihood of a breach. Opportunities would present in key areas of education and training, irrespective of profession; the general public should be aware of the dangers that malware, ransomware, data leakage and credential theft present. There is also an onus on organisations and indeed governments to invest in key, critical infrastructures (adequate security algorithm, IDS, IPS,) and software (firewalls, multi-factor authentication, etc.) which can reduce or prevent breaches.

5.7.5 Smishing (SMS Phishing)

Smishing is a social engineering technique that is a subvariant of phishing. It is used as a means of gathering sensitive information via a text or SMS message. Its usage is a growing threat in the current cybersecurity landscape due to the trusting nature of potential victims.

Challenge:

Threat actors that perform smishing attacks use psychological techniques and malicious URL links in order to trick targets into wilfully sharing information that includes, but is not limited to, passwords, personal information, financial information, corporate information, classified information, etc. An overview of typical smishing attack is shown in Figure 14.

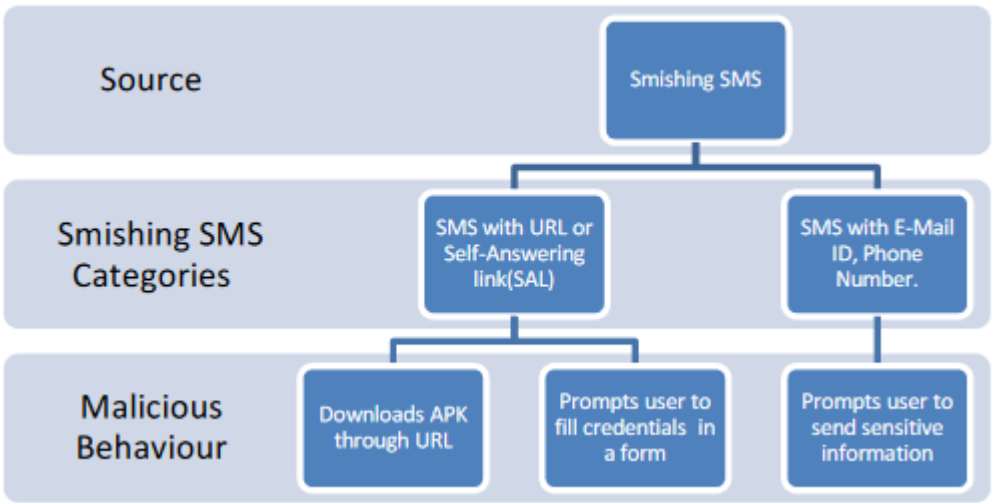

Figure 14: Malicious smishing activity (source: Mishra & Soni, 2019)

Mitigation:

Due to the deceptive nature of this threat, common phishing detection techniques and systems can be implemented in order to mitigate the threat of smishing attacks. Techniques such as content-based filtering, blacklisting, and whitelisting, can serve to protect potential victims from accessing malicious URL links or from disclosing sensitive data to threat actors.

Content-based filtering: Content is examined for malicious URL links and specific keywords such as e-mail addresses, phone numbers, and phrases or constructs commonly used by threat actors. If the invocation of the URL results in malicious activity or if the analysed content fits the criteria for a malicious classification, the message can be blocked before delivery to the intended recipient. Techniques such as machine learning can be used to inform the content-based process of detecting smishing messages.

Blacklisting: This technique requires the implementation of a process that continuously manages a list of explicitly malicious URL links. This list can be populated by hand or with the use of publicly available OSINT resources. After the list has been populated, it can be used in order to match received URL links to the links present in the list. If such a match is discovered, the link can be safely blocked. While this approach cannot mitigate newly created smishing URL links, it has a very low false positive rate.

Whitelisting: This technique also requires the implementation of a process that continuously manages a list. In this case, the aforementioned list is populated with URL links that are allowed and are considered trusted. This process should be performed by hand in order to prevent the occurrence of any false positives. After implementation, the whitelist is used for URL matching. If any given URL is a match, it can be considered trusted and access is allowed. If the URL is not a match, depending on configuration, the URL can either be blocked, or it can be considered as potentially malicious and separately analysed.

Opportunities:

Smishing attacks are a particularly hard threat to mitigate due to the high variance of potential URL links and deception techniques that threat actors employ. The capital reason for smishing attack effectiveness is lack of user awareness. User education about the dangers and common practices of smishing is pivotal for its successful mitigation. Furthermore, the usage of security solutions such as antivirus software for mobile devices can prove vital in limiting the effectiveness of threats like smishing.

5.7.6 Vishing (Voice Phishing or VoIP Phishing)

Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorised entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency.

Challenge:

Phishing is a social engineering technique used to trick people in a large-scale campaign of repeated and often automated messages. When targets respond to the trick, they respond by giving money, resources, or access to the phisher. These messages might be an SMS, email, instant message, paper mail, voicemail, human callers, or even voice chatbots that will speak back to the victim. Voice phishing or vishing specifically refers to phishing carried out verbally.

Voice phishing is relatively a costly and laborious crime and requires some sophistication and carrier knowledge to automate. For this reason, it is typically reserved for gaining access to high-value resources. Vishing is used to gain access to credit card numbers, but more commonly it is used to gain access to the victim's phone account or bank account. It may also be combined with identity theft for even more invasive and damaging attacks.

Surrounding techniques such as caller ID spoofing (also called CLID spoofing) allow the calling attacker to look as if the call is coming from the victim's bank, a government office, a reputable private company, or a local number. By posing as one of the aforementioned, the suspicious "international" component of the fraud is hidden, until the fraud manifests as one.

Black flag voicemail spam and secondary blacklisting is also a concern. This refers to the breach of a carrier's voicemail that allows the sending of large-scale vishing or fraud, knowing the activity will get the carrier's number range blacklisted. If the criminal's intent is to get the numbers of a specific victim blocked, using fraud to manipulate carrier call-blocking procedures would achieve this.

Mitigation:

The key to mitigating such attacks are user education and awareness by following some best-practice advice and recommendations, such as:

- Never call the number given to you or displayed on your caller ID (unless it is a number from a friend, relative, etc.); take the time to look it up to check if it the legitimate number and then call it.
- Never give out any personal information to anyone; legitimate companies do not ask for such information, e.g., social security number, national ID numbers, credit card numbers or PINs via phone

Opportunities:

Since Vishing is a subset of a larger group of social engineering attacks, the most effective type of defence against it is an educated and well-trained end user. While technology plays an important role in reducing the impact in case of a successful social engineering attack, the ultimate vulnerability is the human factor with its psychological predispositions (Conteh & Schmick, 2016). Evidently, education campaigns are the most effective way of avoiding Vishing attacks and this is the main area that organisations should invest on.

5.7.7 Data loss

It is important to ensure the integrity of an organisation's data which usually exist in the following three basic states (McCallister, Grance, & Scarfone, 2010): (i) distributed data at rest, i.e., stored in file systems, (ii) data located at the endpoints of the network, such as laptops, USB devices, external drives, CD / DVDs, archive tapes, MP3 players, or other mobile devices, and (iii) data in motion, as it travels across the network to the outside world via email, instant messaging, peer-to-peer (P2P), FTP, or other communication mechanisms.

Challenges:

Data loss incidents, whether ransomware attacks, hardware failures, accidental or intentional data destruction, can be disastrous for Managed Service Providers (MSPs) and their customers. Backup systems implemented and not tested or planned, increase the operational risk for MSPs. The consequences of data loss events may include one or more of the following: loss of performance, customer revenue loss, and negative reputation. Depending on the type of data loss, an organisation may face various consequences, but in almost all cases this involves both financial and reputational costs.

Mitigation:

Data Loss Prevention (DLP) tools should be able to identify, track, and protect data at rest, data on the move, and data that are used (Liu & Kuhn, 2010). Such tools should use in-depth content analysis and must be customisable to meet the organisation's unique business goals and information security requirements. DLP tools allow organisations to control user interaction with data and may include policies prohibiting users from copying content to removable media or sending it by e-mail. The DLP solution must also be able to generate audit logs to support incident investigation. Testing (both manual and automatic) of processes, procedures, and response and recovery technologies makes it possible to verify the integrity of backup files,and ensure the efficiency and effectiveness of recovery processes and procedures.

Opportunities:

Existing DLP solutions monitor filenames and keywords that are contained in a file, without however being able to detect when the original file is modified or rewritten using similar characters and words. An example that such DLP scheme will fail is the case where an insider malicious actor transcribes a document using different terminologies. Contrary to the approach of these DLP solutions, the scheme proposed by (Alhindi, Traore, & Woungang, 2018) uses domain-specific ontologies for different kinds of documents to create document semantic signatures (DSS). The DSS allows the constant monitoring of sensitive documents on a semantic level and as such, protects the actual knowledge of the data. To the best of our knowledge, such a solution still remains on an experimental level.

5.7.8 Data tampering

Attacks which tamper with, rather than steal or deny access to data, have always been a feature of cybersecurity. An attack on the integrity of data is particularly dangerous when the victim is not aware that changes have been made. For example, Juniper Networks announced[6] in December 2015 that it had discovered "unauthorised" code embedded in an operating system running on some of its firewall products since August 2012. This would have allowed an attacker to gain control of affected firewalls and possibly even decrypt VPN connections. Using an integrity attack against software to create VPN backdoors has considerable downstream effects, weakening security in their customers' networks, which may well have been the attacker's intentions. Moreover, at the end of 2016, cybersecurity researchers at the Security Research Labs (SR Labs) demonstrated[7] how it was possible for relatively unsophisticated actors to change online flight bookings; such access to booking data could enable an attacker to cancel or rebook a flight, or to steal passengers' reward miles.

Challenge:

Data tampering is the act of deliberately modifying (destroying, manipulating, or editing) data through unauthorised channels. Data tampering can take place on the file system, i.e., the modification of bits on disk to so as to perform specific actions and activities other than what the authorised user intends, or it can be on web files, whereby data tampering in web applications is simply a way in which a malicious user gets into a web site and changes, deletes, or gains access to unauthorised files.

IoT devices are also particularly susceptible to cyberattacks since they produce large amounts of sensitive data and they often use the public Internet for data transfer. Among these attacks, data tampering or

[6] https://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554
[7] https://srlabs.de/bites/travel-hacking/

modification attacks that aim to disrupt or bias the states of applications using these data may result in widespread damage and outages. Moreover, only a part of providers is encrypting data in transit. This means that the providers that are not encrypting data are sending protected information and other data in the clear, thus leaving data susceptible to being breached by eavesdropping, packet sniffing, or other means. Additionally, the lack of encryption means that data may be tampered in transit, thus, there is little assurance that the sender's data has fidelity with the receiver's data. Examples of such cases include the following.

Embedded systems: Research (Maggi et al., 2017) has identified five classes of robot-specific attacks that violate the basic operational requirements (accuracy, safety, integrity) of industrial robots: (i) control-loop parameters alteration, (ii) user-perceived robot state alteration, (iii) actual robot state alteration, (iv) calibration parameters tampering, and (v) production logic tampering. Potential impact of these attacks includes defective or modified products, robot damages, operator injuries, sensitive data exfiltration (e.g., industrial secrets) and/or ransomware attacks on altered products.

Advanced Metering Infrastructure (AMI): In this case, potential impact originates from connecting vulnerable smart meters to a home network and is affected by the insecure features of hardware, embedded software, and networks of the AMI. For example, in 2010, an FBI report analysed the Puerto Rico's case where a fraud against an electric utility was disclosed[8]. Adversaries (former company's employees) were tampering smart meters and modifying measurement and billing data, using an infrared communication port, resulting in an estimated financial loss of up to $400million.

Flight information spoofing: Other attack scenarios include flight information spoofing (altitude or speed), introduction of fake route messages on the interactive map, or tampering the crew management application that controls the public address system, lighting, and actuators. In a worst case scenario, in which the vulnerable in-flight entertainment system is indirectly connected to airplane's mission critical control systems, it could be possible hijack the aircraft from a passenger's seat with devastating consequences.

Mitigation:

The spread of smart devices and their use in primary sectors, such as health, transport and others, requires that these devices improve their cybersecurity systems and that at the same time the applied security layers can be managed by devices with reduced capacity. To prevent unauthorised access and thus tampering, sensitive data should be stored in nodes located within trusted parts of the network. In addition, access to physical media should be regulated by appropriate safety procedures, while the storage file system should be based on carefully designed access policies. Finally, all data fetched must be captured and safely transmitted and stored in a secure server to avoid losing vital information and/or tampering.

To detect tampering attempts, watermarking could be applied to multimedia data stored in a system. Digital watermarking is the process of embedding additional information into multimedia files. Ordinarily, when additional description of the multimedia is needed, the metadata fields of certain file formats are used for that purpose. However, this information can be easily removed or simply lost during format changes. Digital watermarking embeds the data by modifying the digital signal (e.g., the sound of an audio file or the appearance of an image) and depending on the application, the introduced changes might be visible (e.g., an overlaid logo or the signature of the owner) or imperceptible. Regardless of this, this additional information should withstand any intentional (e.g., tampering, forgery) or accidental (e.g., JPEG compression, brightness changes) modifications.

To mitigate data tampering threats, VPNs secure the transmitted data by encapsulating the data and then encrypting the data. Encapsulating is often referred to as tunnelling because data are transmitted from one

[8] https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/comment-page-1/

network to another, transparently across a public network infrastructure. Therefore, a good VPN solution should address protecting packets from tampering by using packet integrity hashing functions. Also, onion routing can be used as a mitigation act in this context.

Data tampering in an IoT context can also take place at the edge layer where there is a certain number of lightweight nodes exchanging messages by using the MQTT protocol through a broker which is placed on a fog node. To mitigate data tampering and eavesdropping, it is possible to apply Elliptic Curve Cryptography (ECC) on the MQTT payloads. Nowadays, TLS is widely used, but its use in an IoT context can consume a lot of device energy. Research (e.g., De Rango et al., 2020) has thus proposed the use of ECC in an IoT context, since it is an ideal candidate for implementation on lightweight devices, such as in an IoT fog network.

Finally, IoT devices should implement, also, mechanisms to detect and prevent physical tampering because that can also allow for data tampering to take place. For example, mechanisms that physically destroy a critical component or that securely delete an embedded crypto key, if physical tampering is detected.

Opportunities:

Blockchain-based applications are arising because they ensure integrity, anti-tampering, and traceability. The data tampering risk is one of the main security concerns of data-centric applications. By the nature of the blockchain technology, it is befitting a revolutionary solution to mitigate the tampering risk.

5.8 Quantum technologies

Quantum technologies rely on the principles of quantum physics, a special branch of physics which describes the behaviour of matter and energy at the atomic and subatomic levels. Nowadays, some features of quantum physics are used to design new methods of improving the cybersecurity and performance. The new solutions, such as quantum computers or quantum cryptography, could potentially replace existing solutions. Thus, quantum technology has the potential to change our society significantly.

Quantum computation is one of quantum technology dimensions. It can solve problems beyond the reach of classical processors by using programmable quantum gates/device s. Quantum computer is the device where a quantum algorithm is implemented, such as Grover's (Grover, 1996) or Shor's (Shor, 1994) algorithm. Based on quantum bits, the quantum computer acts as a massive parallel device with large number of computations taking place at the same time. It allows to solve difficult mathematical/computational problems and break currently used encryption methods. The problem is serious because many researchers and engineers expect that quantum computers will achieve such level of power in about twenty-thirty years.

5.8.1 Conditional security of asymmetric cryptography and fast development of quantum computers (Shor's algorithm)

Nowadays, we observe the fast development of quantum-based techniques towards building effective quantum computers. This raises a serious security challenge for public-key cryptography schemes: broken encrypted communication based on asymmetric ciphers (i.e., the widely used RSA). In particular, Shor's algorithm is able to fast factorise big numbers and therefore it is a great threat to global cybersecurity, since with its implementation on a powerful quantum computer, an attacker could break the fundamental security of commonly used asymmetric cryptography (e.g., broken https connections, PKI services, SSL VPNs, etc.).

Challenge:

Shor's algorithm is a polynomial-time quantum algorithm for integer factorisation and thus solves the problem of finding prime factors of large numbers in an effective way. It influences cybersecurity because the security

of asymmetric ciphers is conditional. For example, RSA cipher defines integer N as a part of the public key, but if someone is able to compute the prime factors of N, then they will be able to find the private key and break the security of RSA. Using Shor's algorithm, fast factorisation of large number is possible and therefore, a quantum computer with the implemented quantum algorithm would raise a serious security challenge, namely broken encrypted communication based on widely used asymmetric ciphers (Shor, 1994).

Mitigation:

Nowadays, administrators of information systems usually accept this threat. However, sometimes users try to mitigate this problem by changing used cryptographic solutions to other solutions, resistant to Shor's algorithm. The example is quantum cryptography, where cryptographic key distribution problem is solved by quantum key distribution protocols (i.e., BB84). Also, solutions such as neural cryptography seem to be resistant, since the key distribution problem is solved by using synchronised artificial neural networks.

Opportunities:

One opportunity is the development of other quantum solutions to establish secure communications between entities. Therefore, new quantum cryptography protocols are being developed and technical barriers connected with practical implementations of quantum cryptography are overcome. However, communication based on quantum cryptography is not the only possible way. Nowadays, the development of post-quantum cryptography algorithms creates new opportunities, such as the new algorithms (e.g., lattice-based ciphers or even new symmetric key quantum resistance methods) currently being developed and tested (Mavroeidis, Vishi, Zych, & Jøsang, 2018).

5.8.2 Encryption based on symmetric ciphers with currently using keys can be broken by quantum computer (Grover's algorithm)

Nowadays we observe the fast development of quantum-based techniques towards building effective quantum computers, which will be able to run quantum algorithms. This raises a serious security challenge: broken encrypted communication based on symmetric ciphers using Grover's algorithm. This algorithm allows for effective searching in the unstructured databases which support cryptanalysis of symmetric ciphers (i.e., AES).

Challenge:

Grover's algorithm is a quantum algorithm which finds the input to a black box function that produces a particular output value. Using this solution, it is possible to search much faster the unstructured databases than using classical algorithms since it provides a quadratic speedup over its classical counterparts. Therefore, this algorithm can be used for the cryptanalysis of ciphertexts; for example, a brute-force attack for 128-bit symmetric cryptographic key (i.e., the most popular key length of AES cipher) would need approximately only 264 iterations (Grover, 1996).

Mitigation:

Nowadays, administrators of information systems usually accept this threat, especially, since it is possible just to double the key length of using symmetric ciphers. Sometimes users try to mitigate the problem by changing used cryptographic solutions to other solutions, resistant to quantum algorithms. An example is quantum cryptography, where the cryptographic key distribution problem is solved by quantum key distribution protocols (i.e., BB84). Such cryptography systems are able to establish encryption keys in continuous ways when the key is not needed yet (in advance) and as a result long keys (that increase the level of security) stored at end-

users can be used later. In some scenarios, even secure algorithms such as one-time-pad can be used in practice.

Opportunities:

Development of post-quantum cryptography algorithms creates new opportunities. The new algorithms (e.g., lattice-based cryptography) are currently being developed and tested, while development of new quantum solutions to secure communications between entities is also desirable.

5.9 Incident handling and digital Forensics

Computer security incident response has become an important component of information technology programs as it is necessary for rapidly detecting incidents, minimising loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

5.9.1 Attribution of cyberattacks

Identifying the source of a malicious cyber-activity is a challenging and complicated task, which is further being complicated by the rapid technological developments, bearing increasing complexity in communication and devices. Furthermore, especially with more recent technological innovations, such as the introduction of IoT and massive machine type communications, among others, which more often than not lack maturity in the cybersecurity domain, attackers can remain unidentified. By the same token, digital tools, used to protect the identity of an attacker tend to evolve with the same speed, as other technologies do.

As in the “analogue” world, technical and physical intelligence capabilities and initiatives, as well as insufficient data and evidence can undermine current and future operations. Consequently, even upon forensic evidence, when intelligence agencies can determine with a high degree of confidence the attacker, they face a second attribution problem in the court of public opinion and prosecuting a cybercriminal internationally. At the level of state, attribution or the inability to attribute a cyberattack is a great challenge for decision-makers and a matter of national security, international conflict, and, potentially, worldwide importance.

Experts often say that everything within the cyberspace leaves a trail that could lead to the identification and attribution of a cyberattack. Unfortunately, attackers often exploit vulnerabilities in existing technology and specialise in preserving their anonymity while doing so. Especially with newer technological developments, where a lot of vulnerabilities are stull unpatched, it is becoming increasingly difficult to gather sufficient forensic evidence to pinpoint a person and attribute, with a degree of certainty, a cyberattack to a person, organisation, or state.

Challenge:

Gathering the evidence necessary for prosecuting a potential criminal, or group of criminals, is becoming ever-more technologically challenging. Attributing a cyberattack usually relies on the ability to obtain, through technical means, sufficient forensic evidence. However, when dealing with an experienced attacker, or group of attackers, this is easier said than done. Even more difficult is obtaining forensic evidence from newer technological paradigms, such as IoT, where the field of digital forensics is still at an early stage of development, while at the same time, the level of cybersecurity maturity of the technology is still relatively low, thus allowing for attackers to exploit vulnerabilities in a way that grants them anonymity or does not leave a substantial trail. Furthermore, geo-location spoofing, obfuscation of identifiable information, along with the robust set of tools to achieve anonymity, while performing an attack, leaves forensic experts with little to no

evidence to work with. There is always a trail, however it may not always be sufficient in order to attribute a cyberattack, especially when it comes to national security.

Mitigation:

Technological hinderances become less important against the backdrop of unified efforts and multi-national cooperation in the field of cybersecurity; a nation's lack in cybersecurity capabilities is a much greater challenge than the technological difficulties, related to digital forensics. Building a network of competence, cooperation, and capabilities internationally, is helpful in respect to the prevention of cyberattacks, the faster reaction to them, when they occur, which might be a determining factor in the attribution of cyberattacks, and the prosecution of identified attackers internationally, when there is sufficient proof for their actions.

Engaging the European community with the development of cybersecurity culture is at the root of any further mitigation techniques. Raising the cybersecurity consciousness Europe-wide will motivate national and international actors to build a better cybersecurity posture and improve the technical capabilities for digital forensics and attribution of cyberattacks. A framework for cooperation, on the other hand, will make it easier to obtain missing expertise quickly and to prosecute internationally.

Establishing strategies, unifying cybersecurity efforts, norms and legislations, will serve as a starting point for the mitigation of such difficulties and will attract more people to the field of digital forensics, which will lead to new improvements in the cyber-investigation technologies and individual cybersecurity capabilities in general. Unifying the efforts in cybersecurity will lead to international cooperation in the technical field as well.

Opportunities:

The challenge of attribution of cyberattacks, reveals not only an opportunity for international cooperation in the field of cybersecurity, but also the great need for it. Building a robust cybersecurity environment will greatly contribute to building an environment, which is not as forgiving of malicious activities and cyberattacks. Such cooperation will help identify rapid reaction mechanisms, stronger technological capacity and abilities, as well as help speed the identification of vulnerabilities in newer technologies, technological innovation and experimental software or hardware, identifying common gaps between countries, technologies and mechanisms for accountability.

5.9.2 Lack of proper raw data collection

Cyber Threat Intelligence is the information an organisation uses to understand the threats that have, will, or are currently targeting the organisation and is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources. Gathering raw data about emerging or existing threat actors and threats from a number of sources is thus essential.

Challenge:

As security events generate a huge amount of data, usually in the format of logs, organisations generally delete, filter, or rotate security data from the log sources and do not forward such data to a central log management system. As modern cyberattacks, especially targeted attacks take months in preparation, while in most cases such attacks remain undetected for other months or even years, organisations and responsible agencies are not able to investigate all details of them.

Mitigation:

Raw security data should be reviewed periodically in order to identify previously undetected cyberattacks. Advanced SIEM systems can be used to notify organisations about potential incidents and let them find the

relevant information before raw data is deleted. Managed Security Services (MSS) or outsourced Security Operation Centres (SOCs) can also be hired for threat hunting.

Opportunities:

Since AI/ML techniques typically need data for learning, they leverage such security data which can serve as a basis for security-oriented AI, as it can be seen in some advanced SIEM system. Therefore, a security data lake can be created from raw data by using all the advancements around Big Data.

5.9.3 Lack of dedicated tools to manage cyber threats

Over the past decade, hackers have been increasing their technical capabilities by exploiting vulnerabilities against equipment that is not attacked often. For example, the StuxNet worm has demonstrated that it is possible to disrupt the behaviour of centrifuge in a nuclear power plant disconnected from the Internet, while exploits leaked by the Shadow Broker group show that vulnerabilities have been exploited to execute code remotely and take control of certain CISCO and Fortigate Firewalls. These relatively recent incidents show that any type of device can be targeted.

Challenge:

The diversity of equipment (e.g., SCADA, PLC, Firewall, Router, IoT, etc.) and operating systems (Windows, Unix, OSX) making up the network of an organisation makes detection and analysis difficult, since they can generate a large number of logs, each in a different format depending on the manufacturer. Given the quantity of logs generated and the lack of simple and adapted tools to facilitate interpretation, unskilled operators are not able to perform first-level checks in order to detect cyber threats.

Mitigation:

Addressing this issue would require collecting, standardising, and centralising all these logs in a dedicated tool, such as an SIEM, while the use of advanced technologies, such as AI and ML, could help to analyse and correlate such large quantities of logs. The various network devices are able to create and log each event, but need to be supplemented by IDS. Indeed, a compromised equipment can be manipulated to send logs suggesting that the activity is normal. A learning phase in an environment considered healthy would then be necessary to detect any deviation from the learned model. These deviations could be reported in a readable and graphical way to the unskilled operators, who can then carry out some basic checks using simple and documented tools (integrity check, collecting some artifacts or volatile memory, etc). Another response could be to delegate this task to a specialised company (cybersecurity-as-a-service); by sending logs to a service provider specialised in the management of cyber threats, would allow to benefit from its experience, its knowledge about attacks against actors in the same sector, as well as its technical support for data collection and analysis.

Opportunities:

There are many OSINT tools available utilising different techniques. However, there are gaps and limitations in the currently available tools which make apparent the need for more sophisticated solutions in order to cover unpredictable real-world scenarios. To this end, there are opportunities towards:

- **Information gathering automation:** the greater the amount of the gathered information, the greater the possibility to create correlations and relations between data. Considering the huge amount of data that is publicly available, the task of manually collecting all available information is a very tedious one

and heavily relies on the end user's expertise. Big data techniques, such as crawling and scraping, are solutions that could potentially improve the OSINT exploration of high volumes of data.

- **Filtering of the gathered information**: Due to the huge amount of data which is available, it is almost impossible to go manually through all the available information in order to extract intelligence about a target. Additionally, it is important to detect misinformation that can divert our search. For that reason, filtering and discarding data that do not add any value to our knowledge base is important.

5.9.4 Malware anti-analysis techniques

In the past, IT professionals and end users had an easier time detecting malware using industry antivirus tools, and tools. Nowadays, hackers are starting to create more sophisticated forms of malware that can go undetected, making it hard for security professionals. Some of these malwares have been developed with the sophistication of heuristic capacity to detect any analytic environments (sandboxes) or antivirus software and change their behaviour to bypass detection. An example of such techniques includes checking DLL libraries and analysing any DLLs associated with sandbox environments, virtual machines, and debugging programs. Sophisticated malware can also inspect the environment to see if it is a sandbox, by looking for disk spaces, active windows, user inputs or scanning applications with antivirus capabilities. If the malware finds any indicator of a sandbox environment, it can decide to terminate itself or alter its behaviour characteristics to foil antivirus analysis. Malware can even utilise trusted network utilities like PowerShell and live in obscurity away from antivirus defences.

Challenge:

Malware tools are outfitted with features to disable security tools and to help avoid common antivirus and other threat detection analysis mechanisms. Adversaries are constantly using and modifying these complex anti-analysis techniques to stay ahead of defenders, which poses a dilemma for enterprise organisations and their security. Because these malwares have the sophistication to deploy techniques that avoid sandbox environments and modify their characteristics to avoid detection, they can present a problem for IT professionals and antivirus vendors. These new complex malwares with no way to easily way to detect them can compromise networks and render a lot of antivirus utilities obsolete.

Mitigation:

The growing use of anti-analysis and broader evasion tactics poses a challenge to enterprise organisations and underscores the need for multi-layered defences that go beyond traditional signature and behaviour-based threat detection. Utilising dynamic analysis techniques over traditional static analysis methods, like code debugging platforms, can prove to be an effective tool depending on how it is executed. A hybrid method involves using a malware analysis environment excluding the usage of virtualisation applications in order to avoid triggering the malware's evasive mechanics for virtual machines (VMs) and executing the code into a bare-metal physical environment consisting of hardware systems neutralising the malware's evasive techniques on virtual machines. Investing in threat intelligence systems in conjunction with analysis environment can optimise detecting and safeguarding against malware evasive threats. Incorporating threat intelligence platforms can help assess what kind of new and current threats that may compromise businesses and develop an actionable strategy in mitigating the threat. As mentioned, investing in a dynamic analysis environment with a specific focus on malware evasive threats, in addition to other threats like zero-day exploits and other APTs can be beneficial in thwarting these malwares.

Another tactic that can be used as a countermeasure against anti-analysis malwares is to counteract the evasion techniques of the malware itself, rather than solely focusing on the malicious code itself. By integrating evasion security measures into the baseline antivirus platform, not only will you be able to prevent the malware

from using signature evasive techniques to avoid detection, but also will be able to effectively neutralise the threat.

Finally, patching codes association with DLLs and debugging programs without altering its functionality makes the malware believe the patched code isn't associated with a debug program or sandbox, which will allow the malware to continue its behaviour making its presence more detectable.

Opportunities:

Opportunities involve researchers trying to find solutions to reverse engineer these anti-analysis attacks, because malware authors are becoming more resilient creating improved, and multi-layered malwares that can jeopardise enterprises and other businesses. More security companies are beginning to develop more dynamic-based platforms dedicated to analysing and defeating these sophisticated evasive malwares.

5.9.5 Sandbox evasion techniques

Adversaries are becoming adept at developing threats that can evade increasingly sophisticated sandboxing environments. Sandbox-evading malware is a new type of malware that can recognise if it is inside a sandbox or virtual machine environment. These malware infections do not execute their malicious code until they are outside of the controlled environment. Sandbox-evading malware can be programmed to find some features of a real system that are not available in a sandbox or virtual environment.

Challenge:

Over the years, sandbox systems have become part of the ecosystem of cybersecurity infrastructures adopted by organisations and are widely used for file validation and malware analysis. For these reasons, malware authors start writing code that can detect specific behaviour during their execution in order to understand if they are running in a sandbox environment and avoid their malicious behaviour.

There are several techniques used for sandbox evasion, the most common are:

- **Delaying execution:** To circumvent the timeout configuration applied in most of the modern sandboxes, malware delay the execution of the malicious payload.
- **Hardware detection:** With the aim of understanding if the running environment is a sandbox, malware analyses the fingerprint of hardware components in order to find well known indicators.
- **CPU detection:** Most sandboxes use a low amount of resources and therefore in order to estimate this information, malware detects the number of CPU cores.
- **User interaction:** This technique is used to detect user interaction since such sandboxes are not a real machine used every day.
- **Environment detection:** In order to detect well known sandboxes environments, malware analyse the environment where they are running.

Mitigation:

To circumvent the sandbox evading techniques, several recommendations have been introduced:

- **Dynamically change sleep duration:** Increase the duration of execution and analysis of the malware in order to avoid the delaying execution of malicious payload. Also, the dynamic changing of execution time may trigger the malware.

- **Simulate human interactions:** Real user simulation can trigger malicious behaviour of the malware. Since modern malware can detect random user interactions, this type of simulation has to be the closest possible to real user interaction. The use of AI/ML techniques can help in this way.
- **Add real environmental and hardware artifacts:** In order to avoid hardware and CPU detection, adding real resources will help to get better results, albeit with an increase of the cost.
- **Use fingerprint analysis:** Fingerprinting technology allows to analyse a malware file and find indicators of compromising and thus can also be used for detecting evasion characteristics of malware.
- **Use behaviour-based analysis:** In order to detect and counterattack an evasion technique, monitoring the behaviour of the analysed file may help.
- **Customise the sandboxing:** Adding no default language, resource, installed programs, and others may help to avoid this kind of techniques.

Opportunities:

The development of AI/ML techniques can really help to avoid sandbox-escaping malware and simultaneously help us to understand better the techniques used by malware developers. Customisation of the sandbox is another important aspect that can be translated in new technological and market products.

5.9.6 Lack of adequate cyber risk mitigation frameworks

Cyber risk mitigation frameworks aim to propose appropriate mitigation strategies following a real or potential cyberattack with the goal to minimise the expected resulting loss to business.

Challenge:

The identification of the most appropriate cyber risk framework needs to be addressed in order to perform an exhaustive risk mitigation, given that not all frameworks are applicable to all scenarios and sectors. For example, The Open Group Architecture Framework (TOGAF) can be used to also address cyber risk, but it is not applicable to the case of a ship cyber risk assessment inasmuch it is based on a strict definition of architecture that is not applicable in a ship.

Mitigation:

In order to identify the best cyber risk mitigation framework that is applicable to a certain scenario, the team that performs the assessment and estimates the risk must have a complete knowledge of the domain.

Opportunities:

Defining cyber risk mitigation framework that are applicable cross-sector may help organisations in the process of framework selection. Moreover, organisations ned to invest in professionals that have substantial knowledge of the examined domain and deep knowledge of cyber risk mitigation frameworks.

5.10 Summary

Overall, this section provided a detailed review of the identified transversal technical cybersecurity challenges, while the discussion on the potential opportunities that arise touched upon multiple facets of required solutions that would need to leverage a combination of advanced technology (including the latest advances in AI/ML technologies), clear processes, and qualified and informed people. Moreover, solutions that are customisable and adaptive to particular environments are often needed, including dynamic solutions that can learn both

based on past experience and also on-the-fly. Finally, such a systematic review has the potential to address the fragmentation often observed in the cybersecurity domain, and also form the basis for additional meta-analyses that will provide further insights into the current landscape and potential opportunities.

6. Conclusions and next steps

This deliverable is the first version of the deliverables reporting on transversal technical cybersecurity challenges and will be validated, updated, and revised in D4.8. This initial study was based on an extensive report collection and analysis, as well as on the knowledge and expertise of the members of the consortium participating in T4.1. Given the evolving nature of cybersecurity, and the progress of the ECHO project there are many challenges that the need to be discussed as we progress through the next stage of the task.

Part of the deliverable was to organise the challenges in categories that are better tailored to the needs of the task. We settled on a classification with 10 categories which are aligned with the JRC taxonomy and also encapsulate all of the identified challenges, despite the fact that the multifaceted nature of the cybersecurity discipline makes this quite challenging. The aforementioned categories are prone to changes and open to validation, as new challenges emerge and the ongoing process of identification continues.

The next steps include conducting dedicated workshops to receive feedback from cybersecurity experts, as well as collect input through questionnaires. For this purpose, a list of recipients has already been collected and the plan is to use it in the next version of the deliverable. Also, the report collection process is ongoing in order to keep up to date with all emerging cybersecurity challenges. Finally, the ECHO Multi-sector Assessment Framework will be used in order to prioritise the challenges in a quantitative manner.

Annexes

Annex 1 – List of analysed reports

Report title	Published by	Publication date	Country	Type of organisation
Trust Services Security Incidents 2018 - Annual Report	ENISA	2019	EU	EU agency
Industry 4.0 Cybersecurity: Challenges & Recommendations	ENISA	2019	EU	EU agency
Good Practices For Security Of Internet Of Things: In The Context Of Smart Manufacturing	ENISA	2018	EU	EU agency
X-Force Threat Intelligence Index	IBM	2019	Global	Industry
APT Trends Report Q3 2019	Kaspersky	2019	Russia	Industry
Mcafee Labs Threats Report	McAfee	2019	USA	Industry
CISCO 2018 Annual Cybersecurity Report	CISCO	2019	USA	Industry
Internet Security Threat Report	Symantec	2019	USA	Industry
M-Trends 2019: Fireeye Mandiant Reports	FireEye	2019	USA	Industry
Microsoft Security Intelligence Report	Microsoft	2019	USA	Industry
Annual Review 2019	National Cyber Security Centre	2019	UK	National organisation
Where Cybersecurity Stands 2018	Black Hat	2018	USA	Industry
2018 Data Breach Investigations Report	Verizon	2018	USA	Industry
Web Attacks And Gaming Abuse	Akamai	2019	USA	Industry
Retail Attacks And API Traffic	Akamai	2019	USA	Industry
DDoS And Application Attacks	Akamai	2019	USA	Industry
Annual Cyber Security Assessment 2019	Republic of Estonia - Information System Authority	2019	Estonia	National organisation
Security In Polish Cyberspace 2019 ['Polski Barometr Cyberbezpieczeństwa Społecznego 2019']	Polish Institute of Cybersecurity	2019	Poland	Non-governmental organisation (NGO)

Report title	Published by	Publication date	Country	Type of organisation
Specification Of Requirements For Security And Confidentiality Of The System (D8.1)	INDECT project (EU FP7 project)	2012 (revised version)	EU	Law enforcment agency
A Survey On Cybersecurity, Data Privacy, And Policy Issues In Cyber-Physical System Deployments In Smart Cities	Elsevier	2019	Global	Other
Muddling Through Cybersecurity: Insights From The U.S. Healthcare Industry	Elsevier	2019	USA	Academic
Global Threat Intelligence Report	NTTSecurity	2019	Germany	Industry
2019 Data Breach Investigations Report	Verizon	2019	USA	Industry
Cyber Attack Trends Analysis	Check Point Research	2019	Israel	Industry
2019 Cyber Security Risk Report - What's Now And What's Next	Aon	2019	UK	Industry
Cyber Security Report 2019	Swisscom	2019	Switzerland	Industry
The Cost Of Cybercrime	Accenture Security	2019	UK	Industry
A First Look At Browser-Based Cryptojacking	IEEE	10/7/2018	EU	Academic
Cyber Threatscape Report 2018	Accenture Security	2018	UK	Industry
Cyber Assessment Framework V3.0	National Cyber Security Centre	2019	UK	National organisation
Comprehending The IoT Cyber Threat Landscape: A Data Dimensionality Reduction Technique To Infer And Characterize Internet-Scale IoT Probing Campaigns	Elsevier	2019	USA	Academic
Navigating The Insider Threat Tool Landscape: Low Cost Technical Solutions To Jump Start An Insider Threat Program	IEEE	2018	USA	Other
A Study On Cyber-Crimes, Threats, Security And Its Emerging Trends On Latest Technologies: Influence On The Kingdom Of Saudi Arabia	Researchgate	2018	Saudi Arabia	Other
Survey Of Intrusion Detection Systems: Techniques, Datasets And Challenges	Springer	2019	Australia	Other
The Growth Of Fileless Malware	Florida International University	2019	USA	Other
Internet Security Report	WatchGuard	2019	USA	Industry

Report title	Published by	Publication date	Country	Type of organisation
The Secret Life Of Websites	SiteLock	2018	USA	Industry
Website Security Insider	SiteLock	2017	USA	Industry
2019 Cybersecurity Report	The National Defense Industrial Association NDIA	2019	USA	Other
Threat Landscapereport	fortinet	2019	USA	Other
Threat Report	Proofpoint	2019	USA	Industry
2015 Italian Cyber Security Report	National Cyber Security Centre	2015	Italy	EU Agency
Cybersecurity In China	KPMG	2019	China	Industry
National Cyber Security Organisation:Israel	NATO CCDCOE	2017	Israel	National organisation
2019 Healthcare Threat Report	Proofpoint	2019	USA	Other
Phishing As An Attack Vector	INFOSEC Institute	2019	USA	Academic
A Survey Of IoT-Enabled Cyberattacks: Assessing Attack Paths To Critical Infrastructures And Services	IEEE	2018	USA	Academic
Cyber Threat Intelligence Sharing Survey And Research Directions	Elsevier	2019	Global	Academic
SECURING DIGITAL HEALTH - Initial Reflection S For Steering Global Cyber Security Efforts In Health	The Global Digital Health Partnership (GDHP)	2019	Global	Other
ETSI TR 103 305-1 V3.1.1 - TECHNICAL REPORT Critical Security Controls For Effective Cyber Defence; Part 1: The Critical Security Controls	ETSI	2018. sept	Global	Industry
ETSI TR 103 305-2 V2.1.1 - TECHNICAL REPORT Critical Security Controls For Effective Cyber Defence; Part 2: Measurement And Auditing	ETSI	2018. sept	Global	Industry
ETSI TR 103 305-3 V2.1.1 - TECHNICAL REPORT Critical Security Controls For Effective Cyber Defence; Part 3: Service Sector Implementations	ETSI	2018. sept	Global	Industry
Etsi Tr 103 306 V1.3.1 - Technical Report	ETSI	2018. aug	Global	Industry

Report title	Published by	Publication date	Country	Type of organisation
Cyber; Global Cyber Security Ecosystem				
ETSI TS 103 645 V1.1.1 - TECHNICAL SPECIFICATION CYBER; Cyber Security For Consumer Internet Of Things	ETSI	2019. febr.	Global	Industry
When Machine Learning Meets Security Issues: A Survey	IEEE	2018	Global	Academic
Quantum's Promise And Peril:2019 Digicert Post Quantum Crypto Survey	DigiCert	2019	USA	Industry
Cyberthreat Report: Reconnaissance 2.0	PaloAlto	2018	USA	Industry
The 6 Biggest Cybersecurity Risks Facing The Utilities Industry	ABI Research	2019	USA	Other
Cyber Threatscape Report	Accenture Security	2019	UK	Industry
Internet Security Threat Report 2019	Symantec	2019	Global	Industry
State Of Malware 2019	Malwarebytes	2019	Global	Industry
2020 Global IoT/ICS Risk Report	CyberX	2019	Global	Industry
Responding To Cyberattacks: Prospects For The EU Cyber Diplomacy Toolbox	Paul Ivan - EPC	2019	EU	EU Agency
Living Off The Land And Fileless Attack Techniques	Symantec	2017	Global	Industry
2019 Global Cyber Risk Perception Survey	Marsh & McLennan with Microsoft	2019	USA	Industry
Cyber Security Assessment Netherlands Csan 2019	CSBN (National Coordinator for Security and Counterterrorism)	2019	Netherlands	National organisation
Defiéndase Contra Amenazas Críticas De La Actualidad	CISCO	2019	Spain	Industry
Correo Electrónico: Pulse Con Precaución	CISCO	2019	Spain	Industry
Informe CIBERSEGURIDAD En Entornos Digitales	VU LABS	2019	Spain	Industry
La Ciberseguridad En España	The cocktail Analisis y GOOGLE	2019	Spain	Industry
La Tecnología Se Está Volviendo Cada Vez Más Inteligente. ¿Y Nosotros?	ESET	2019	Spain	Industry

Report title	Published by	Publication date	Country	Type of organisation
Tendencias En El Mercado De La Ciberseguridad	INCIBE	2016	Spain	National organisation
Informe De Tendencias En Ciberseguridad 2019	Eleven Paths	2019	Spain	Industry
Estrategia Nacional De Ciberseguridad 2019	Presidencia de Gobierno	2019	Spain	National Government
A Survey Of IoT-Enabled Cyberattacks: Assessing Attack Paths To Critical Infrastructures And Services	IEEE	2018	Global	Academic
A Study On Security And Privacy Guidelines,Countermeasures, Threats: IoT Data At Rest Perspective	MDPI	2019	Global	Academic
Advanced Deception With BEC Fraud Attacks	Researchgate	2018	Global	Academic
Email Fraud And Identity Deception Trends	Agari Data	2019	Global	Industry
How Ransomware Attacks	Sophos	2019	Global	Industry
Himss Cybersecurity Survey	HIMSS	2019	USA	Industry
5 Best Practices For Data Breach Prevention In 2019	Endpoint Protector	2019	Global	Industry
An Activity Guideline For Technology Roadmapping Implementation	Researchgate	2010	Global	Academic
Measuring The Maturity Of Business Intelligence In Healthcare: Supporting The Development Of A Roadmap Toward Precision Medicine Within ISMETT Hospital	Elsevier	2018	Global	Academic
Cybersecurity And Cyber Defence: National Level Strategic Approach	Taylor & Francis Group	2017	Global	Academic
Cybersecurity Threatscape	Positive Technologies	2019	Russia	Industry
Energy Technology Roadmaps A Guide To Development And Implementation	International Energy Agency	2014	Global	Industry
Evaluation Of Cybersecurity Data Set Characteristics For Their Applicability To Neural Networks Algorithms Detecting Cybersecurity Anomalies	Researchgate	2020	Global	Academic
Fundamentals Of Technology Roadmapping	Sandia National Labs	1997	Global	Industry
Protecting Patients, Providers And Payers	Proof Point	2019	Global	Industry
Handling A Trillion (Unfixable) Flaws On A Billion Devices: Rethinking Network Security For The Internet-Of-Things	ACM	2015	Global	Academic

Report title	Published by	Publication date	Country	Type of organisation
Towards A Technology Roadmap For Big Data Applications In The Healthcare Domain	IEEE	2014	Global	Academic
Internet Of Things & Cybersecurity Readiness In Smart-Government And Organizations	Researchgate	2019	Global	Academic
Internet Of Things: Realising The Potential Of A Trusted Smart World	Royal Academy of Engineering	2018	Global	Academic
Malware Threats And Mitigation Strategies: A Survey	Researchgate	2011	Global	Academic
Ransomware: Best Practices For Prevention And Response	Carnegie Mellon University	2017	Global	Academic
Ransomware Deployment Methods And Analysis: Views From A Predictive Model And Human Responses.	Crime Science	2019	Global	Academic
State Of Cybersecurity & Cyber Threats In Healthcare Organizations	ESSEC Business School	2016	Global	Academic
The Road Ahead: Cybersecurity In 2020 And Beyond	Fireeye	2020	USA	Industry
Securing Medical Research: A Cybersecurity Point Of View.	Science	2012	Global	Academic
Technology Roadmapping And Smes: A Literature Review.	DRUID Society	2012	Global	Academic
Threat Landscape Report	Fortinet	2019	USA	Industry
Towards Big Data Governance In Cybersecurity	Researchgate	2019	Global	Academic
What Is Cryptojacking? How To Prevent, Detect, And Recover From It	CSO	2020	USA	Industry
Towards A Framework For Policy Development In Cybersecurity	ENISA	2018	EU	EU agency
Panorama Actualde La Ciberseguridaden España	Google	2018	Spain	Industry
The Biggest Threat From Ransomware: Malicious Encryption Of Sharednetwork Files	Vectra	2019	USA	Industry
2019 Global Cyber Risk Perception Survey	Microsoft	2019	USA	Industry
Toward Ai Security	Center for Long-Term Cybersecurity (CLTC)	2019	USA	Other
Cyber-Telecom Crime Report 2019	Europol	2019	EU	Law enforcment agency
Piano Nazionaleper La Protezione Cibernetica E La Sicurezza Informatica	Presidenza del Consiglio dei Ministri	2013	Italy	National organisation

Report title	Published by	Publication date	Country	Type of organisation
2016 Italian Cybersecurity Report	University of Rome	2017	Italy	National organisation
Piano Nazionaleper La Protezione Cibernetica E La Sicurezza Informatica	Presidenza del Consiglio dei Ministri	2017	Italy	National organisation
Himss Cybersecurity Survey	HIMSS	2017	USA	National organisation
Himss Cybersecurity Survey	HIMSS	2018	USA	National organisation
Healthcare And Cross-Sector Cybersecurity Report	HIMSS	2019	USA	National organisation
A Case Study Analysis Of The U.S. Office Of Personnel Management Data Breech	Researchgate	2019	USA	Academic
The Cyber Threat To UK Business	National Cyber Security Centre	2017	UK	National organisation
Cyberspace Dilemmas. Containment Of Cybersecurity Threats	Relaciones Exteriores	2019	Spain	Other
Cybersecurity And Privacy Dialogue Between Europe And Japan	EUNITY	2018	EU	Other
Preliminary Version Of The Cybersecurityresearch Analysis Report For The Two Regions	EUNITY	2018	EU	Other
Revised Version Of The Cybersecurity Researchanalysis Report For The Two Regions	EUNITY	2018	EU	Other
Miscreant Motivations For The Office Of Personnel Management Data Breech	Researchgate	2019	USA	Academic
The Future Of Cybersecurity	SecurityIntelligence	2017	Global	Industry
Next Generation Cyber Security Solution For An Ehealth Organization	IEEE	2017	Global	Academic
Global Information Assurance Certification Paper	SANS	2019	Global	Industry
Project 2020 Scenarios For The Future Of Cybercrime - White Paper For Decision Makers	Europol	2010	EU	Law enforcment agency
Digital Vision For Cybersecurity	Atos	2019	EU	Industry
Berkeley Cybersecurity Futures 2025 Insights And Findings	Center for Long-Term Cybersecurity (CLTC)	2019	USA	Other
Bohemia Study: Continuous Cyberwar Targeted Scenario No4	European Commision	2018	EU	EU Agency
Towards The Cyber Security Paradigm Of Ehealth: Resilience And Design Aspects	AIP Publishing	2017	Global	Academic

Report title	Published by	Publication date	Country	Type of organisation
Energy Insight: Cybersecurity In The Energy Sector	Energy Institute	2017	Global	Other