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

D4.2 INTER-SECTOR TECHNICAL CYBERSECURITY CHALLENGES REPORT

Work package	WP4 INTER-SECTOR TECHNOLOGY ROADMAPS
Lead author	NOTIS MENGIDIS (CERTH)
Contributors	Marco Cammisa (EXP), Davide Ferrario (Z&P), Brid Davis (NUIM), Antal Bódi (SU), Mike Anastasiadis (CERTH), Marcin Niemiec (AGH), Giuseppe Chechile (FNC), Monica Constantini (LCU), Vyacheslav Kharchenko (KhAI), Veselin Dobrev (BDI), Julien Blin (NG), Theodora Tsikrika (CERTH), Notis Mengidis (CERTH), Csaba Krasznay (SU), PioTr Bogacki (AGH), Riccardo Feletto (FNC), Oleg Illiashenko (KhAI), Pencho Vasilev (BDI), Gregory Depaix (NG), Kornél Tóth (SU), Marco Dri (FNC), Herman Fesenko (KhAI), Kristina Ignatova (BDI), Maryna Kolisnyk (KhAI)
Peer reviewers	Burak Mavzer (VST), Matteo Merialdo (RHEA), Nikolai Stoianov (BDI)
Version	V1.0
Due date	30/04/2020
Submission date	18/06/2020

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)

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

Version history

Revision	Date	Editor	Comments
0.1	18/03/2020	Notis Mengidis (CERTH)	Table of Contents
0.2	21/03/2020	Notis Mengidis (CERTH)	Introduction
0.3	23/03/2020	Notis Mengidis (CERTH)	Section 3
0.4	29/04/2020	Notis Mengidis (CERTH)	Integrated inputs from all contributors in Section 3 – first version of the deliverable
0.5	03/05/2020	Notis Mengidis (CERTH)	Adjusted references
0.6	07/05/2020	Notis Mengidis (CERTH)	Internal QA Review
0.7	12/05/2020	Notis Mengidis (CERTH)	Executive summary
0.8	21/05/2020	Notis Mengidis (CERTH)	Added amended contributions to Section 3
0.8.1	27/05/2020	Notis Mengidis (CERTH)	Added Section 2 – Aligned with D4.1
0.8.2	28/05/2020	Notis Mengidis (CERTH)	Updated references and glossary of acronyms
0.9	18/06/2020	Tiago Nogueira (VisionSpace)	QA checks
0.9.1	18/06/2020	Notis Mengidis (CERTH)	Corrections based on QA checks
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, 4	Notis Mengidis (CERTH), Theodora Tsikrika (CERTH)
3.1.2.1	Marco Cammisa (EXP)
3.1.1.1, 3.3.1.2	Davide Ferrario (Z&P)
3.1.1.2	Brid Davis (NUIM)
3.2, 3.2.1, 3.2.2, 3.2.3	Antal Bódi (SU), Csaba Krasznay (SU), Kornél Tóth (SU)
3.3.1.1	Mike Anastasiadis (CERTH)
3.3.1.3, 3.4.1, 3.4.2, 3.7.3	Marcin Niemiec (AGH), PioTr Bogacki (AGH)
3.3.1.4, 3.4.3, 3.9, 3.9.1, 3.9.2, 3.9.3, 3.9.4	Giuseppe Chechile (FNC), Riccardo Feletto (FNC), Marco Dri (FNC)
3.4.4, 3.7.4, 3.7.5	Monica Constantini (LCU)
3.5, 3.5.1.1, 3.7.1, 3.7.2,	Vyacheslav Kharchenko (KhAI), Oleg Illiashenko (KhAI), Herman Fesenko (KhAI), Maryna Kolisnyk (KhAI),
3.6.1	Veselin Dobrev (BDI), Pencho Vasilev (BDI), Kristina Ignatova (BDI)
3.8, 3.8.1	Julien Blin (NG), Gregory Depaix (NG)

Keywords

CYBERSECURITY, TECHNICAL, RESEARCH DOMAINS, SECTORS, CHALLENGES, INTER-SECTOR

Disclaimer

This document contains information which is proprietary to the ECHO consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or parts, except with the prior written consent of the ECHO consortium.

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

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 to 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 *inter-sector* technical cybersecurity challenges, i.e., technical cybersecurity challenges that are sector-related, but span across more than one sectors.

These challenges were identified through a multistep process described in the accompanying deliverable D4.1 “Transversal technical cybersecurity challenges report”, while also taking 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 83 technical cybersecurity challenges: 57 transversal challenges (reviewed in D4.1) and 26 inter-sector challenges (reviewed in this deliverable). 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 D4.2 “Inter-sector 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 D4.2 concerns the latter, while the accompanying deliverable D4.1 concerns the former. 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. The applied methodology is described in detail in the accompanying deliverable D4.1 "Transversal technical cybersecurity challenges report".

Our analysis resulted in the identification of a total of 83 technical cybersecurity challenges: 57 transversal challenges (reviewed in the accompanying deliverable D4.1) and 26 inter-sector challenges (reviewed in this deliverable). 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 has four sections with the first one being introduction; the following three sections are:

- Section 2 provides an overview of the results of the analysis performed for the identification of inter-sector technical cybersecurity challenges.

- Section 3 analyses in depth the identified inter-sector technical cybersecurity challenges, i.e., technical challenges that are sector-specific, but span more than one of the ECHO priority sectors of healthcare, transportation, energy, and defence.
- Section 4 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.
- D4.1 “Transversal technical cybersecurity challenges report”. This deliverable uses the same sources as D4.1 and also applies the methodology (as described in Section 2 of D4.1).

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.

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
Amin et al., 2017	A software agent enabled biometric security algorithm for secure file access in consumer storage devices.	Amin, R., Sherratt, R. S., Giri, D., Islam, S. H., & Khan, M. K. (2017). A software agent enabled biometric security algorithm for secure file access in consumer storage devices. IEEE Transactions on Consumer Electronics, 63(1), 53-61.	2017
Bao, Zhang, & Shen, 2006	Physiological signal based entity authentication for body area sensor	Bao, S.-D., Zhang, Y.-T., & Shen, L.-F. (2006). Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. In Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference.	2006

Reference	Document Title	Document Reference	Date
	networks and mobile healthcare systems		
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
Caltagirone, S., et al., 2013	The diamond model of intrusion analysis	Caltagirone, S., et al. (2013). The diamond model of intrusion analysis, Center For Cyber Intelligence Analysis and Threat Research Hanover Md.	2013
Can & Sahingoz, 2015	A survey of intrusion detection systems in wireless sensor networks	Can, O., & Sahingoz, O. K. (2015). A survey of intrusion detection systems in wireless sensor networks. In Proceedings of the 2015 6th international conference on modeling, simulation, and applied optimization (ICMSAO).	2015
Cherukuri et al., 2003	Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body	Cherukuri, S., Venkatasubramanian, K. K., & Gupta, S. K. (2003). Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In Proceedings of the 2003 International Conference on Parallel Processing Workshops, 2003.	2003
Cytomic, 2019	Living-off-the-Land attacks: what are they and why should they worry you?	Cytomic, 2017. Living-off-the-Land attacks: what are they and why should they worry you? Cytomic News August 19 2019. Retrieved April 3rd 2020 from: https://www.cytomicmodel.com/news/living-off-the-land-attacks/	2019
Dejon et al., 2019	Automated Security Analysis of IoT Software Updates.	Dejon, N., Caputo, D., Verderame, L., Armando, A., & Merlo, A. (2019, December). Automated Security Analysis of IoT Software Updates. In IFIP International Conference on Information Security Theory and Practice (pp. 223-239). Springer, Cham.	2019
Dejon, Caputo, Verderame, Armando, & Merlo, 2019	Automated Security Analysis of IoT Software Updates	Dejon, N., Caputo, D., Verderame, L., Armando, A., & Merlo, A. (2019). Automated Security Analysis of IoT Software Updates. In Proceedings of the IFIP International Conference on Information Security Theory and Practice.	2019
Denning, Fu, & Kohno, 2008	Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security	Denning, T., Fu, K., & Kohno, T. (2008). Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security. In Proceedings of the HotSec.	2008
Diogenes, and Ozkaya, 2018	Cybersecurity Attack and Defense Strategies: Infrastructure	Diogenes, Y. and Ozkaya, E., 2018. Cybersecurity Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing Ltd.	2018

Reference	Document Title	Document Reference	Date
	security with Red Team and Blue Team tactics.		
Du & Lin, 2005	Designing efficient routing protocol for heterogeneous sensor networks	Du, X., & Lin, F. (2005). Designing efficient routing protocol for heterogeneous sensor networks. In Proceedings of the PCCC 2005. 24th IEEE International Performance, Computing, and Communications Conference, 2005.	2005
Du & Wu, 2006	Adaptive cell relay routing protocol for mobile ad hoc networks	Du, X., & Wu, D. (2006). Adaptive cell relay routing protocol for mobile ad hoc networks. IEEE Transactions on Vehicular Technology, 55(1), 278-285.	2006
Du, Guizani, Xiao, & Chen, 2008	Defending DoS attacks on broadcast authentication in wireless sensor networks	Du, X., Guizani, M., Xiao, Y., & Chen, H.-H. (2008). Defending DoS attacks on broadcast authentication in wireless sensor networks. In Proceedings of the 2008 IEEE International Conference on Communications.	2008
Du, Shayman, & Rozenblit, 2001	Implementation and Performance Analysis of SNMP on a TLS/TCP Base	Du, X., Shayman, M., & Rozenblit, M. (2001). Implementation and Performance Analysis of SNMP on a TLS/TCP Base. In Proceedings of the 2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No. 01EX470).	2001
Elhag, Fernández, Bawakid, Alshomrani, & Herrera, 2015	On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems	Elhag, S., Fernández, A., Bawakid, A., Alshomrani, S., & Herrera, F. (2015). On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems. Expert Systems with Applications, 42(1), 193-202.	2015
Gonda, O., 2014	Understanding the threat to SCADA networks.	Gonda, O. (2014). "Understanding the threat to SCADA networks." Network Security 2014(9): 17-18.	2014
Green, 2020 via Varnois Inside Out Security Blog	What is Fileless Malware? PowerShell Exploited.	Green, A., 2020. What is Fileless Malware? PowerShell Exploited. Varnois Inside Out Security Blog – Threat Detection, April 1st 2020. Retrieved April 7th 2020 from: https://www.varonis.com/blog/fileless-malware/	2020
Gorog, 2018	Solving Global Cybersecurity Problems by Connecting Trust Using Blockchain.	Gorog, C. and T. E. Boult (2018). Solving Global Cybersecurity Problems by Connecting Trust Using Blockchain. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE.	2018

Reference	Document Title	Document Reference	Date
Groza & Minea, 2011	Formal modelling and automatic detection of resource exhaustion attacks.	Groza, B. and Minea, M., 2011, March. Formal modelling and automatic detection of resource exhaustion attacks. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (pp. 326-333).	2011
Halperin et al., 2008	Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defences	Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., . . . Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defences. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP 2008).	2008
Hei, Du, & Lin, 2014	Poster: Near field communication based access control for wireless medical device	Hei, X., Du, X., & Lin, S. (2014). Poster: Near field communication based access control for wireless medical devices. In Proceedings of the Proceedings of the 15th ACM international symposium on Mobile ad hoc networking and computing.	2014
Hei, Du, Wu, & Hu, 2010	Defending resource depletion attacks on implantable medical devices	Hei, X., Du, X., Wu, J., & Hu, F. (2010). Defending resource depletion attacks on implantable medical devices. In Proceedings of the 2010 IEEE Global Telecommunications Conference GLOBECOM 2010.	2010
Henry, Paul, & McFarlane, 2013	Using bowel sounds to create a forensically-aware insulin pump system	Henry, N., Paul, N., & McFarlane, N. (2013). Using bowel sounds to create a forensically-aware insulin pump system. In Proceedings of the Presented as part of the 2013 {USENIX} Workshop on Health Information Technologies.	2013
Hu et al., 2013	OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks	Hu, C., Cheng, X., Zhang, F., Wu, D., Liao, X., & Chen, D. (2013). OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. In Proceedings of the 2013 Proceedings IEEE INFOCOM.	2013
Jack, 2013	Implantable medical devices: Hacking humans	Jack, B. (2013). Implantable medical devices: Hacking humans. Black Hat USA.	2013
Jan et al., 2019	A payload-based mutual authentication scheme for Internet of Things	Jan, M. A., Khan, F., Alam, M., & Usman, M. (2019). A payload-based mutual authentication scheme for Internet of Things. Future Generation Computer Systems, 92, 1028-1039.	2019
Kim, Lee, Raghunathan, Jha, & Raghunathan, 2015	Vibration-based secure side channel for medical devices	Kim, Y., Lee, W. S., Raghunathan, V., Jha, N. K., & Raghunathan, A. (2015). Vibration-based secure side channel for medical devices. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC).	2015

Reference	Document Title	Document Reference	Date
Kim, S. H., & Lee, K. H., 2018	VPN-Filter Malware Techniques and Countermeasures in IoT Environment.	Kim, S.-H. and K.-H. Lee (2018). "VPN-Filter Malware Techniques and Countermeasures in IoT Environment." Journal of Convergence for Information Technology 8(6): 231-236.	2018
Korolov, 2019	What is a supply chain attack? Why you should be wary of third-party providers.	Korolov, M., 2019. What is a supply chain attack? Why you should be wary of third-party providers. CSOnline, Jan 25th, 2019. Retrieved April 1st 2020 from: https://www.csoonline.com/article/3191947/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html	2019
Kshetri & Voas, 2017	Hacking power grids: A current problem.	Kshetri, N., & Voas, J. (2017). Hacking power grids: A current problem. Computer, 50(12), 91-95.	2017
Langer, 2011	Stuxnet: Dissecting a cyberwarfare weapon	Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51.	2011
Leszczyna et al., 2011	Protecting industrial control systems-recommendations for europe and member states.	Leszczyna, R., et al. (2011). "Protecting industrial control systems-recommendations for europe and member states." tech. rep., Technical report, European Union Agency for Network and Information Security (ENISA).	2011
Li, Raghunathan, & Jha, 2011	Hijacking an insulin pump: Security attacks and defences for a diabetes therapy system	Li, C., Raghunathan, A., & Jha, N. K. (2011). Hijacking an insulin pump: Security attacks and defences for a diabetes therapy system. In Proceedings of the 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services.	2011
Liang & Du, 2014	Permission-combination-based scheme for android mobile malware detection	Liang, S., & Du, X. (2014). Permission-combination-based scheme for android mobile malware detection. In Proceedings of the 2014 IEEE international conference on communications (ICC).	2014
Lin, Ke, & Tsai, 2015	CANN: An intrusion detection system based on combining cluster centers and nearest neighbors	Lin, W.-C., Ke, S.-W., & Tsai, C.-F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-based systems, 78, 13-21.	2015
Liu, Al Ameen, & Kwak, 2010	Secure wake-up scheme for wbans	Liu, J.-W., Al Ameen, M., & Kwak, K.-S. (2010). Secure wake-up scheme for wbans. IEICE transactions on communications, 93(4), 854-857.	2010
M. Li, Yu, Guttman, Lou, & Ren, 2013	Secure ad hoc trust initialization and key management in wireless body area networks	Li, M., Yu, S., Guttman, J. D., Lou, W., & Ren, K. (2013). Secure ad hoc trust initialization and key management in wireless body area networks. ACM Transactions on sensor Networks (TOSN), 9(2), 1-35.	2013

Reference	Document Title	Document Reference	Date
Marin, Singelée, & Preneel, 2014	Secure remote reprogramming of implantable medical devices	Marin, E., Singelée, D., & Preneel, B. (2014). Secure remote reprogramming of implantable medical devices. COSIC, Kent, WA, USA, Internal Tech. Rep, 2485.	2014
Marin, Singelée, Yang, Verbauwhede, & Preneel, 2016	On the feasibility of cryptography for a wireless insulin pump system	Marin, E., Singelée, D., Yang, B., Verbauwhede, I., & Preneel, B. (2016). On the feasibility of cryptography for a wireless insulin pump system. In Proceedings of the Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy.	2016
Meshram & Haas, 2017	Anomaly detection in industrial networks using machine learning: A roadmap Machine Learning for Cyber Physical Systems	Meshram, A., & Haas, C. (2017). Anomaly detection in industrial networks using machine learning: A roadmap Machine Learning for Cyber Physical Systems (pp. 65-72): Springer.	2017
Microsoft Defender ATP Research Team, 2020	Latest Astaroth living-off-the-land attacks are even more invisible but not less observable.	Microsoft Defender ATP Research Team, 2020. Latest Astaroth living-off-the-land attacks are even more invisible but not less observable. Microsoft Security Blog, March 23rd 2020. Retrieved April 7th 2020 from: https://www.microsoft.com/security/blog/2020/03/23/latest-astaroth-living-off-the-land-attacks-are-even-more-invisible-but-not-less-observable/	2020
Moein et al., 2017	Hardware attack mitigation techniques analysis.	Moein, S., Gulliver, T. A., Gebali, F., & Alkandari, A. (2017). Hardware attack mitigation techniques analysis. International Journal on Cryptography and Information Security (IJCIS), 7(7), 9-28.	2017
National Cyber Security Centre, 2018	Supply chain security guidance.	National Cyber Security Centre. Supply chain security guidance, reviewed 16th Nov 2018. Retrieved April 2nd 2020 from: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples	2018
Nazir et al., 2017	Assessing and augmenting SCADA cyber security: A survey of techniques.	Nazir, S., et al. (2017). "Assessing and augmenting SCADA cyber security: A survey of techniques." Computers & Security 70: 436-454.	2017
Neupane, K., et al., 2018	Next generation firewall for network security: A survey.	Neupane, K., et al. (2018). Next generation firewall for network security: A survey. SoutheastCon 2018, IEEE.	2018
O'Dowd, 2017	Considerations for Connected Medical Device Networks	O'Dowd, E. (2017). Considerations for Connected Medical Device Networks. HITInfrastructure.	2017
Park, 2014	Security mechanism based on hospital authentication server for secure	Park, C.-S. (2014). Security mechanism based on hospital authentication server for secure application of implantable medical devices. BioMed research international, 2014.	2014

Reference	Document Title	Document Reference	Date
	application of implantable medical devices		
Radcliffe, 2011	Hacking medical devices for fun and insulin: Breaking the human SCADA system	Radcliffe, J. (2011). Hacking medical devices for fun and insulin: Breaking the human SCADA system. In Proceedings of the Black Hat Conference presentation slides.	2011
Rubin et al, 2019	Detecting Malicious PowerShell Scripts Using Contextual Embeddings	Rubin, A., Kels, S., & Hendler, D. (2019). Detecting Malicious PowerShell Scripts Using Contextual Embeddings. arXiv preprint arXiv:1905.09538.	2019
Samtani et al., 2016	Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques.	Samtani, S., et al. (2016). Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. 2016 IEEE Conference on Intelligence and Security Informatics (ISI), IEEE.	2016
Scarfone, K., & Mell, P. , 2012	Guide to intrusion detection and prevention systems (idps)	Scarfone, K. and P. Mell (2012). Guide to intrusion detection and prevention systems (idps), National Institute of Standards and Technology.	2012
Schwartz 2019, via CIODive	Why 'living off the land' has become a preferred method of cybercrime.	Schwartz S.A. 2019. Why 'living off the land' has become a preferred method of cybercrime. CIODive, Feb 20th, 2019. Retrieved April 2nd 2020 from: https://www.ciodive.com/news/why-living-off-the-land-has-become-a-preferred-method-of-cybercrime/548767/	2019
Snell, 2017	78% of Providers Report Healthcare Ransomware, Malware Attacks	Snell, E. (2017). 78% of Providers Report Healthcare Ransomware, Malware Attacks. HealthITSecurity.	2017
Sun, Zhu, Zhang, & Fang, 2011	Cryptography based secure EHR system for patient privacy and emergency healthcare	Sun, J., Zhu, X., Zhang, C., & Fang, Y. (2011). HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. In Proceedings of the 2011 31st International Conference on Distributed Computing Systems.	2011
Symantec Security Response, via Medium, 2018	What is Living off the Land?	Symantec Security Response 2018). What is Living off the Land? Medium, 3rd October 2018. Retrieved April 3rd 2020 from: https://medium.com/threat-intel/what-is-living-off-the-land-ca0c2e932931	2018
Thomas et al., 2019	Protecting accounts from credential stuffing with password breach alerting.	Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Kelley, P.G., Invernizzi, L., Benko, B., Pietraszek, T., Patel, S., Boneh, D. and Bursztein, E., 2019. Protecting accounts from credential stuffing with password breach alerting. In 28th USENIX Security Symposium (USENIX Security 2019) (pp. 1556-1571).	2019

Reference	Document Title	Document Reference	Date
Tom et al., 2008	Recommended practice for patch management of control systems	Tom, S., et al. (2008). Recommended practice for patch management of control systems, Idaho National Laboratory (INL).	2008
Wu, Du, Guizani, & Mohamed, 2017	Access control schemes for implantable medical devices: A survey	Wu, L., Du, X., Guizani, M., & Mohamed, A. (2017). Access control schemes for implantable medical devices: A survey. IEEE Internet of Things Journal, 4(5), 1272-1283.	2017
Xiao, Wan, Lu, Zhang, & Wu, 2018	IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?	Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? IEEE Signal Processing Magazine, 35(5), 41-49.	2018
Xu, Revadigar, Luo, Bergmann, & Hu, 2016	Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication	Xu, W., Revadigar, G., Luo, C., Bergmann, N., & Hu, W. (2016). Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication. In Proceedings of the 2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN).	2016
Xu, Wendt, & Potkonjak, 2014	Matched digital PUFs for low power security in implantable medical devices	Xu, T., Wendt, J. B., & Potkonjak, M. (2014). Matched digital PUFs for low power security in implantable medical devices. In Proceedings of the 2014 IEEE International Conference on Healthcare Informatics.	2014
Yadav, G., & Paul, K. , 2019	PatchRank: Ordering updates for SCADA systems.	Yadav, G. and K. Paul (2019). PatchRank: Ordering updates for SCADA systems. 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE.	2019
Zhang, Raghunathan, & Jha, 2013	Securing medical devices through wireless monitoring and anomaly detection	Zhang, M., Raghunathan, A., & Jha, N. K. (2013). MedMon: Securing medical devices through wireless monitoring and anomaly detection. IEEE Transactions on Biomedical circuits and Systems, 7(6), 871-881.	2013
Zheng, Fang, Orgun, & Shankaran, 2014	A non-key based security scheme supporting emergency treatment of wireless implants	Zheng, G., Fang, G., Orgun, M. A., & Shankaran, R. (2014). A non-key based security scheme supporting emergency treatment of wireless implants. In Proceedings of the 2014 IEEE International Conference on Communications (ICC).	2014

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
AI	Artificial Intelligence
AIDS	Anomaly-based Intrusion Detection System
AMSI	Antimalware Scan Interface
APT	Advanced Persistent Threats
ASIC	Application Specific Integrated Circuit
BDD	Behaviour-Driven Development
BFSM	Boosted Finite State Machine
BIST	Built-in Self Test
CCW	Certain Conventional Weapons
CMS	Content Management System
CNI	Critical National Infrastructure
COA	Course of Action
CoAP	Constrained Application Protocol
COTS	Commercial off-the-shelf
CSP	Content Security-Policy
CVSS	Common Vulnerability Scoring System
DDos	Distributed Denial of Service
DDos	Denial of Service
DES	Data Encryption Standard
DMZ	Demilitarised Zone
DoD	Department of Defense
DRP	Dual-Rail Pre-charged
DTLS	Datagram Transport Layer Security
EEPROM	Electrically Erasable Programmable Read-Only Memory
EM	Electromagnetic
EMR	Electronic Medical Records
FPR	False-Positive Rate
FSM	Finite State Machine
GA	Grant Agreement
GGE	Group of Governmental Experts
GT	Game Theory
HMI	Human Machine Interface
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IMD	Implanted Medical Device

Acronym	Description
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
LAWS	Lethal Autonomous Weapon Systems
MITM	Man-In-The-Middle
MTU	Master Terminal Unit
NGFW	Next Generation Firewall
NVD	National Vulnerability Database
OS	Operating System
PLC	Program Logic Controller
RAT	Remote Administration Tool
RNG	Random Number Generator
RTU	Remote Terminal Unit
SaaS	Software as a Service
SAM	Scanning Acoustic Microscopy
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SNR	Signal-to-Noise Ratio
SOA	Service Oriented Architectures
SRI	Subresource Integrity
TCP	Transmission Control Protocol
TDD	Test-Driven Development
TTP	Tactics, Techniques and Procedures
UDP	User Datagram Protocols
UEBA	User and Entity Behavioural Analysis
VSM	Viable System Model
WAF	Web Application Firewall
WP	Work Package
XRF	X-Ray Fluoroscopy

Table 3: Glossary of acronyms, initialisms and abbreviations

2. Overview of the analysis of the inter-sector challenges

The analysis based on the methodology described in Section 2 of the accompanying deliverable (D4.1) resulted in the identification of a total of 83 technical cybersecurity challenges: 57 transversal and 26 inter-sector; this deliverable focuses on the latter, while the transversal challenges are analysed in the D4.1.

The 26 inter-sector technical cybersecurity challenges that were identified are listed below and are also depicted in Figure 1. 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 (see D4.1). 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 1 and Figure 2 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 “Incident Handling and Digital Forensics” 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 inter-sector technical challenges were identified and are listed with respect to their primary category. As a result, the category “Quantum Technologies” is not listed below, as none of the identified inter-sector challenges considers this as their primary category; as a matter of fact, this category was not considered at all by the identified challenges.

- Software and Hardware Security Engineering
  - Application Security
    - PowerShell and VBScript sophisticated backdoors
    - Living off the land and supply chain attacks
  - Web Applications
    - Formjacking
- Critical Infrastructures
  - Lack of SCADA/ICS vulnerability assessment tools
  - Configuration and patch management in ICS/SCADA
  - Perimeter defence of ICS/SCADA systems
- IoT, Embedded Systems, Pervasive Systems
  - Gain access to connected medical devices
  - Gain access to implanted medical devices
  - Weak encryption protocols on medical IoT devices
  - Resource exhaustion attacks on medical IoT devices
- Network and Distributed Systems
  - Fragmentation as IDS evasion technique
  - Flooding as IDS evasion technique
  - Not minding the gap: direct internet connections
  - Theft, sabotage, and fraud in SIEMs and analytics systems
- Cloud, Edge and Virtualisation
  - Hardware vulnerabilities

- AI and Big Data Analytics
    - AI in the Military
- Data Security and Privacy
    - Credential stuffing attacks
    - Access to unencrypted data (finance, health records)
    - Unauthorised modification of multimedia content
    - Ransomware against Electronic Medical Records (EMR)
    - Bio-hacks for multi-factor authentication
- Incident Handling and Digital Forensics
    - Lack of SCADA Forensic Tools
- Vehicular Systems
    - Detection of rogue or unauthorised autonomous systems
    - Interference
    - Transparency and accountability
    - Unauthorised access to autonomous cars and unmanned vehicles

Figure 1 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; these include “theft, sabotage, and fraud in SIEMs and analytics systems” which reflect the current pressing concerns on insider threats which are more prevalent in some sectors compared to others, and the “resource exhaustion attacks on medical IoT devices” which reflects the emerging cybersecurity challenges in sectors that are rapidly adopting IoT devices.

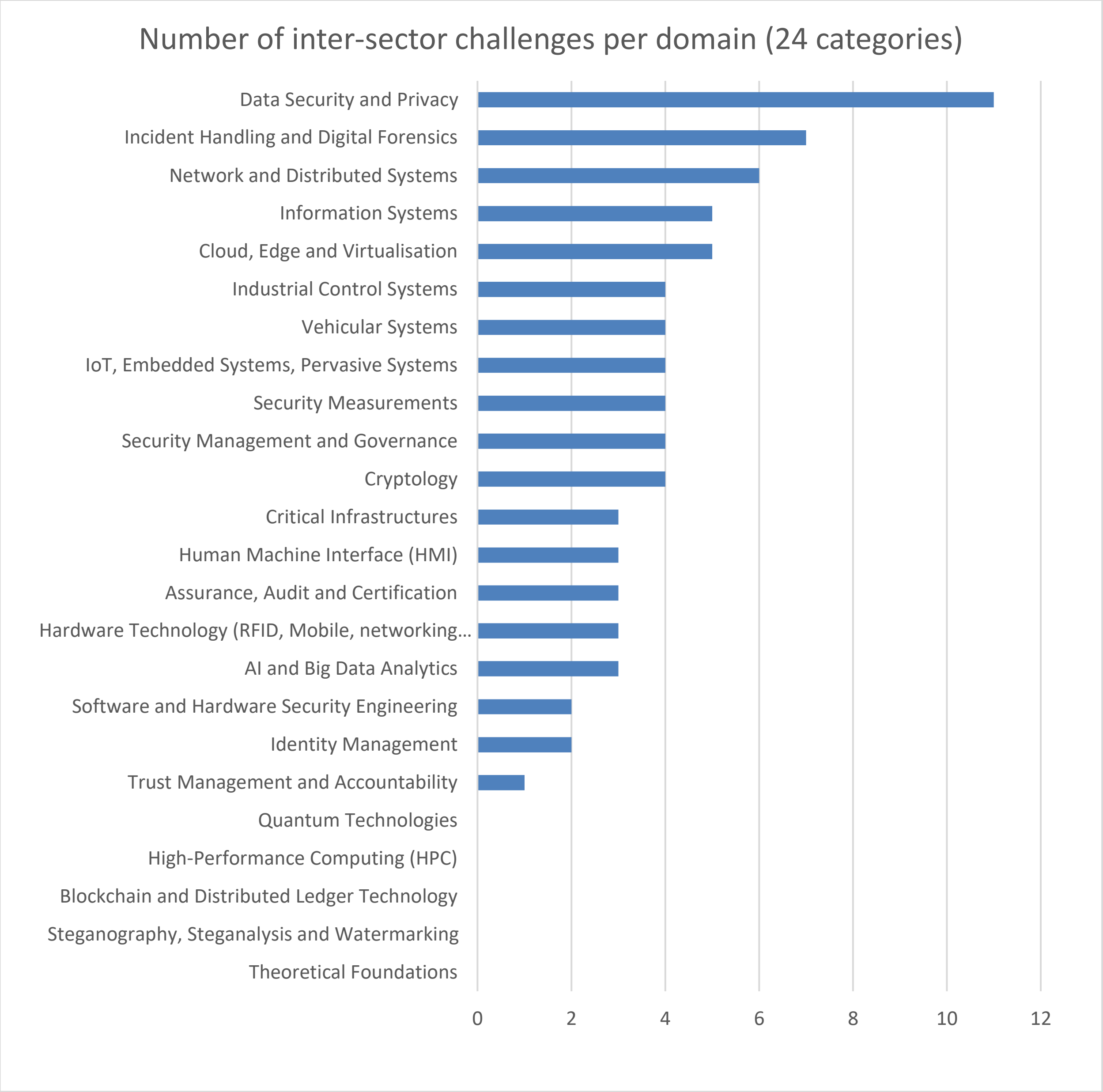

Figure 1: Number of identified challenges per domain based on the initial categorisation

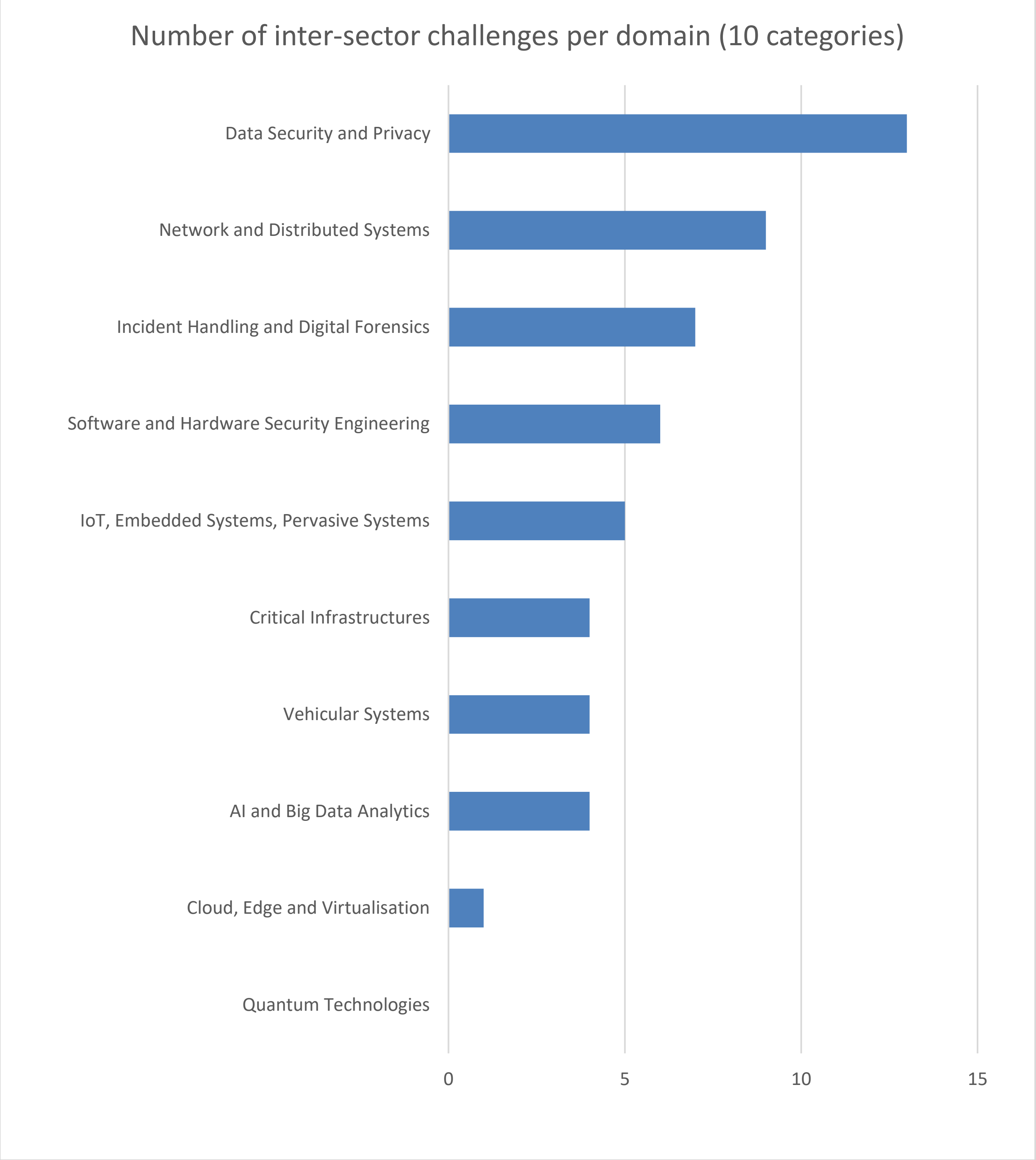

Figure 2: Number of identified challenges per domain based on the final categorisation

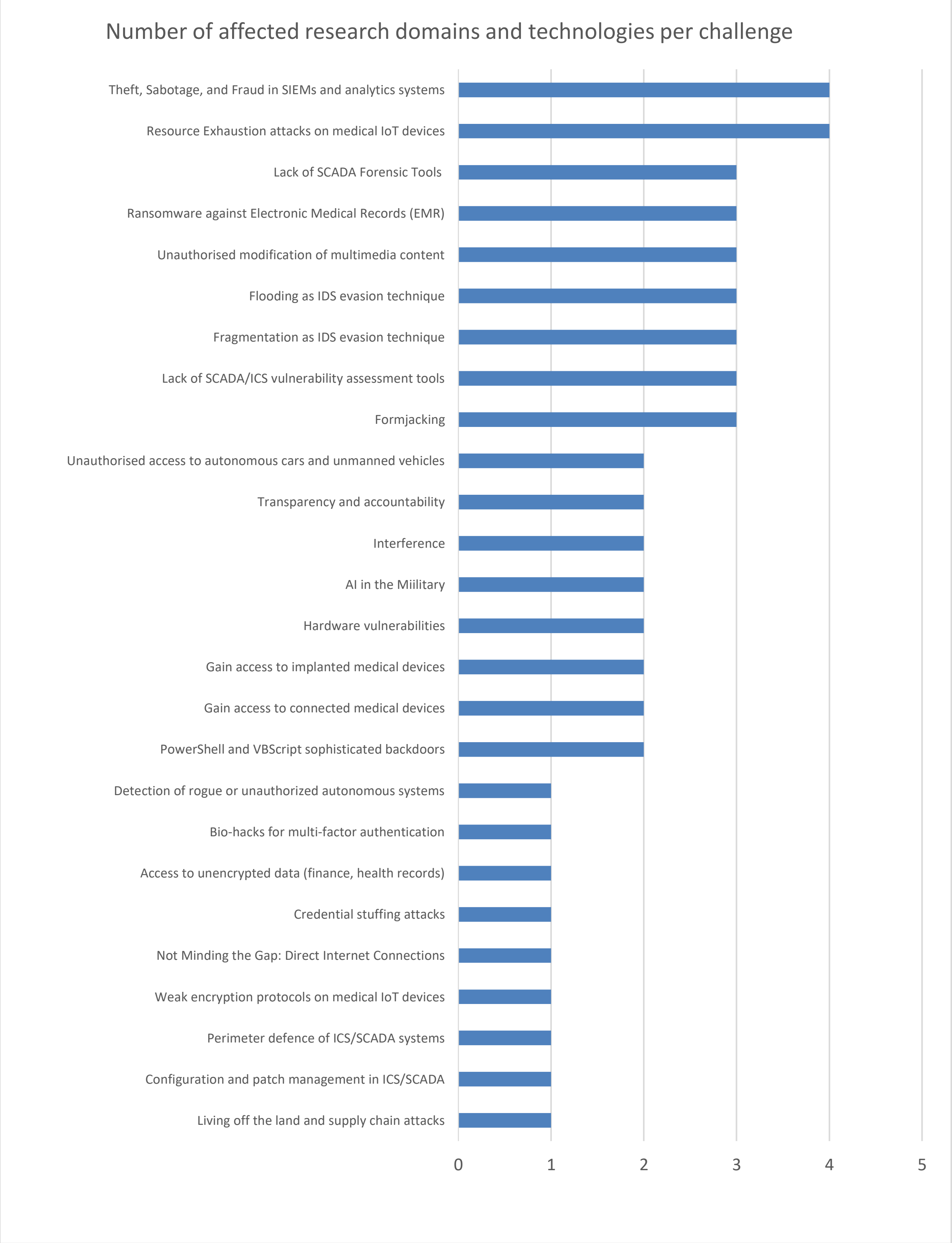

Figure 3: Number of affected research domains and technologies per challenge

Next, a discussion on the identified inter-sector technical cybersecurity challenges as these are categorised to the domain that they primarily affect is provided (Section 3).

3. Inter-sector 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 inter-sector 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 26 inter-sector technical cybersecurity challenges belonging to nine of the previously defined research and technological domains are analysed.

3.1 Software and hardware security engineering

With the increasing frequency, intensity, disruptions, hazards, and other threats to organisations, the military, businesses, and the critical infrastructures, the need for more trustworthy and secure systems has never been more important. Engineering-based solutions are essential to managing the growing complexity and interconnectedness of today’s systems, as exemplified by cyber-physical systems and systems-of-systems, including the Internet of Things (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.

3.1.1 Application security

3.1.1.1. PowerShell and VBScript sophisticated backdoors

The Powerstats malware family are PowerShell-based first-stage backdoors that use and drop scripts to contact a command-and-control (C2) server. These backdoor attacks include some sophisticated and advanced infection and evasion techniques, such as AppLocker bypass methods, malware analysis tool detection, anti-sandbox checks, extended C2 proxy lists, base64 encoding, and PowerShell obfuscation

Challenge:

iDefense threat intelligence reported in the Cyber Threatscape report 2018 (J. Rayet al., 2018) several Powershell and VBSript sophisticated backdoors attacks and attributed these activities to Iran based actors.

POWERSTATS malware family: POWERSTATS is a PowerShell-based first-stage backdoor that uses and drops scripts to contact a command and control server. The first attacks were observed and disclosed in 2017, and they were accredited to Iran-based actors known as “Muddy Water”. Attacks did continue throughout 2018 and are expected to keep evolving in the next years. The malware first performs reconnaissance on the victim system, then lowers Microsoft Office security settings in order to be able to execute any PowerShell command. The first generation used basic PowerShell and VisualBasic Script. However, higher complexity was observed in its evolution, which included more advanced infection techniques, such as methods to bypass AppLocker, methods to detect malware analysis tools and isolated environments (anti-sandbox checks), extended Command and Control proxy lists, embedded base64 encrypted code and more PowerShell obfuscated layers. Moreover, a java-based version of POWERSTATS has been observed, associated with BurpSuite-KeyGen and a malicious Microsoft Help file.

In their initial reporting from October 2017, the iDefense threat intelligence was able to attribute these attacks with moderate confidence to Iran-based actors: specific strings and metadata discovered within the malware supported malware’s Iranian origin; additionally, the continuous changes of the malware is consistent with the behaviour of the Iranian threat group that is supposed to be behind it. Furthermore, iDefense, with the help of a third party, that posed as a victim, successfully managed to detect a tradecraft error made by the operator: an exposed IP address in Iran believed to be a final endpoint. After the security community attributed the malware to Iran-based actors, attempts to cause misattribution and confusion were detected by Mo Bustami (in the Security Ownage blog), such as the embedding of Chinese false-flag strings in early 2018.

PIPEFISH espionage activities: Similarly, another group is active in the Middle East, called PIPEFISH (aka OilRig). Its main targets are entities for surveillance and infrastructures in the energy sector. Its characteristic behaviour includes reuse of metadata, IP infrastructure, lure documents, and domain registrants. Thus, analysts succeeded in producing a high-confidence profile against the group. In particular, new ISMDoor variants (including information stealer and remote administration tool - RAT) were identified in early 2018, which proved to be consistent with the previous samples created by this threat group.

However, this new ISMDoor presents an important change from its early variants: no persistence mechanism is explicitly implemented. The reasons behind the removal of the persistent component of the malware are still unclear, but it could be to avoid detection or to create tailored persistent access. In fact, the persistence of the backdoor may be achieved by a C2 human operator, which is manually downloading additional backdoor payloads or creating scheduled tasks in the compromised machine.

Also stemming from PIPEFISH group, the new .NET-based Trojan named “OopsiE trojan” uses the Internet Explorer application object to cover its communications and make them look like they are part of a legitimate browser session; the trojan also has the ability to execute remote commands and to upload and download files from the victim’s system.

PBR-Backdoor, named after the function used in the final PowerShell script payload, is another malware linked to PIPEFISH, targeting companies in Egypt. It shares some similarities with POWERSTATS, such as obfuscation and substitutions, and this may suggest code reuse by “Muddy Water” actors. Accenture Security expects this activity to continue and to evolve, despite efforts by Microsoft to securely control PowerShell, as public reporting of the group’s tactics, techniques and procedures (TTP) continues to emerge.

Mitigation:

In 2015 Microsoft announced a new built-in capability of Windows 10, called AntiMalware Scan Interface (AMSI). This newly introduced capability allows applications, but also script engines, to perform an on-demand scan by the anti-malware installed on the system. PowerShell code is by default sent to AMSI for scanning prior to its execution, greatly reducing the percentage of malicious PowerShell code execution rate. Also, both the command-line code and the content of the script are being analysed by AMSI, something that gives the anti-malware software extended information regarding the true nature of the running code.

Opportunities:

Even though AMSI is a step towards mitigating the risk of PowerShell backdoors, given the widespread usage and adoption of legitimate PowerShell scripts, it is necessary to achieve a small false-positive rate (FPR). In the study of (Rubin et al., 2019) a novel idea was presented, where a deep learning-based detector leveraged a pretrained contextual embedding in order to detect malicious PowerShell code. In this study, a detection rate of nearly 90% was achieved while at the same time and FPR of 0.1% was maintained.

3.1.1.2. Living off the land and supply chain attacks

Internal reconnaissance attacks are cyber breaches which are carried out within an organisation's network, systems, and premises, in which the attacker interacts with the actual target systems in order to find out information about its vulnerabilities (Diogenes, and Ozkaya, 2018). 'Living off the land' is an internal reconnaissance technique which has become increasingly common in recent years (Cytomic, 2019). This variant of attack consists of threat actors taking advantage of built-in trusted and legitimate applications that are installed on victim's systems – essentially using native software (e.g., Powershell, Command Prompt, Windows Management Instrumentation) which are already present on the system to accomplish adverse objectives (Schwartz 2019, via CIODive). Supply chain attacks, comparatively, seek to harm an organisation by targeting less-secure elements. These types of attacks typically involve exploitation of third-party services and software to compromise a final target (National Cyber Security Centre, 2018).

Challenge:

'Living off the land' attacks are particularly harmful since they are malware-free, therefore difficult to detect as they are not readily recognisable by anti-malware screening tools. Furthermore, the legal tools which are typically vulnerable to exploitation oftentimes have been granted overarching access privileges and recognitions as standard, known as ‘whitelisting’; thus manipulation of these is difficult to detect by security systems (Symantec Security Response 2018, via Medium).

Supply chain attacks take many forms, including hijacking software updates and injecting malicious code into legitimate software. Supply chain attacks commence with advanced persistent threats (APT), in which developers then continue to be exploited, either through attackers stealing credentials for version control tools, or by attackers compromising third-party libraries that are integrated into larger software projects. One of the largest breaches in the retail industry was a supply chain attack with besieged the American department store, Target (Korolov, 2019). While this breach was attributed to lax security at a heating, ventilation, and air conditioning vendor, Target spent approximately $61 million trying to resolve the fallout from the attack.

Mitigation:

Given that 'living off the land' techniques use legitimate tools for malicious purposes, and also considering that there are no fingerprints or trace of the source of the attack (as random access memory is volatile), it is quite difficult to mitigate against such attacks, as there are no files to analyse, making the malware practically undetectable (Microsoft Defender ATP Research Team, 2020). However, such ventures in industry and research spheres could be some promise. Most cybersecurity vendors already have begun to deploy features implementing behavioural analytics using Artificial Intelligence (AI).

These industries have essentially determined that identification and blocking of these attacks requires the use of advanced detection methods such as analytics and machine learning (Green, 2020 via Varnois Inside Out Security Blog; Symantec Security Response, via Medium, 2018). With regards to supply chain attacks while detection is also equally difficult, it is evident that there is no one-size-fits-all approach to its security. However, enterprises need to be aware that while their proprietary systems might be secure, linkages while with third-party might be the weakest link. All outside systems, even if trusted, should therefore be treated with caution (Korolov, 2019), whereby layers of separation in the virtual sense should be established.

Some sectors have recognised that the deployment of sensitive security policy could have potential in countering supply chain attacks by making potential targets less vulnerable and less attractive to attackers. Mitigation techniques which have been researched in academic circles have focused on determining effective intrusion detection methods in the first instance and using behavioural analytics to detect anomalies.

Opportunities:

'Living off the land' and supply chain attacks are highly complex and stealthily orchestrated, therefore difficult to detect. However, some ventures could potentially be explored with regards to mitigating such breaches. These include: (i) **educating enterprises** on the existence of these hacking practices and raising awareness that while their mainframes may have strong tools to counter malware attacks, built-in applications and third-party software also can be compromised without detection (thus represent the weakest link in the supply chain), and (ii) **develop Artificial Intelligence (AI) techniques** (analytics and machine learning) in an attempt to accurately detect these attacks (Green, 2020 via Varnois Inside Out Security Blog).

3.1.2 Web applications

Web application security is a branch of information security that deals specifically with the security of websites, Web applications, and Web services. At a high level, Web application security draws upon the principles of application security, but applies them specifically to Internet and Web systems.

3.1.2.1. Formjacking

Formjacking involves adjustment of websites, which allows the attacker to obtain data entered by users. Attackers can adjust websites by hacking them and putting malware code or adjusting the code of shared sections of websites. These techniques enable attackers to intercept confidential data, such as credit card numbers.

Challenge:

The majority of website owners do not keep their Content Management System (CMS) (or its plugins) up to date and unsurprisingly suffer compromises. The fear of breaking a site by upgrading it is often cited as a reason to remain on an older revision. Having said that, unless those sites are protected behind some kind of application firewall, they can easily be hacked. A common example is the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites.

Symantec’s telemetry shows that it is often small and medium sized retailers, selling goods ranging from clothing to gardening equipment to medical supplies, that have had formjacking code injected onto their websites. These smaller businesses are less likely to maintain appropriate cybersecurity measures. Formjacking may also target third-party services in order to get its code onto targeted websites. Formjacking has no immediate telltale signs. Victims may not realise they are victims of formjacking as generally, their websites continue to operate as normal.

Mitigation:

The first line of defence is deployment of effective security solutions, such as Intrusion Detection and Prevention Systems (IDPS) and firewalls, and keeping CMS software updated. Using products such as Symantec Web Application Firewall (WAF) can help protect Web applications from getting compromised in the first place, as well as using HTTP directives, such as HTTP Content Security-Policy (CSP) and SubResource Integrity (SRI), to limit where scripts can be loaded from, where they can send data to, what they can do, and to check the integrity of remotely loaded scripts. Using an automated framework, like PhantomJS, and simulating user behaviour, including test purchases, allows tracking of interactions and monitoring for suspicious activity, such as if any resources are loaded from new domains.

Symantec blocked more than 3.7 million formjacking attempts in 2018, with more than 1 million of those blocks occurring in the last two months of the year alone. Formjacking activity occurred throughout 2018, with an anomalous spike in activity in May (556,000 attempts in that month alone), followed by a general upward trend in activity in the latter half of the year. We may speculate that the spike in May could be related to Mother's Day, while the rising trend in the latter half of the year related to shopping for Christmas (Cyber Monday, etc.).

Opportunities:

Opportunities to avoid formjacking, or at least most of the major consequences for customers of a business which may have its website formjacked, that is, especially for credit card details, include the use of cryptocurrency. The use of public receive keys and private spend keys allows the user to maintain control of their finances as only the public receive key of the business needs to be on the website, while the customer maintains control of their private spend key on their own application. Of course, this does not mitigate the problem of paying the wrong entity, but it will protect assets remaining in the customer's account, and, depending on the choice of cryptocurrency, protect the personal and financial details of the victim as well.

Simply switching to more secure and private payment systems (as with cryptocurrency, but note that asymmetric encryption technology could also be applied to traditional bank or credit accounts) would greatly reduce the incentive for formjacking. It reduces the possible payoff simply to the payments obtained, thus remaining account funds and personal information are better protected.

3.2 Critical infrastructures

3.2.1 Lack of SCADA/ICS vulnerability assessment tools

Vulnerability assessment aims at finding weak points in the security posture of an organisation. However, in an industrial system, there are a lot of open questions, such as which system should be tested. Real operational systems may not be testable, thus it is challenging to create a close-to-real environment for testing. Lack of methodology tailored for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition systems (SCADA) is also a problem. Moreover, closed protocols, unknown architectures, lack of documentation for systems of interest are also causing challenges. Finally, the lack of ICS ready pentest tools, and usable exploits, as well as the lack of competent pentest teams with ICS/SCADA experience create an additional challenge.

Challenge:

Industrial Control Systems (ICS) and SCADA systems are an integral aspect of the modern industrial environment and the Critical National Infrastructure (CNI). For many years, SCADA and ICS networks were a completely independent sectors of any business or agency, where the field devices and industrial mechanisms which interacted with physical assets were separate from the corporate networks or intranet. However, as Internet technologies became even more integrated into modern society, and as corporations began to grow exponentially around the globe, the demand for remote auditing and control of industrial systems increased.

This resulted in the merging of Internet Protocol (IP) and SCADA/ICS technologies, which in turn exposed the older field devices to a new set of attack vectors, leading to unpredicted vulnerabilities. In an age where threats from the cyberdomain are ever-evolving, the tools used to perform security audits and penetration tests against conventional systems are subsequently being used on the older SCADA/ICS networks. These tools, without the correct configuration, and built-in IT security solutions, could cause substantial damage to the SCADA devices connected to a business’s infrastructure, rather than helping to protect and audit them. The challenge is that these are old systems for which vulnerability assessment tools are non-existent or difficult to apply. As an example, setting up a test environment in a nuclear or water power plant is a challenging task given the criticality and the security policies in place.

Mitigation:

There are two widely accepted vulnerability assessment methods:

Passive vulnerability assessment: This technique aims to cross-reference specific characteristics, such as the OS version, with databases that contain known vulnerabilities. However, it is estimated that only 14% of software vulnerabilities disclosed in NVD are patched immediately after their release while 50% remain vulnerable after three months, and 30% remain vulnerable after six months. SCADA systems specifically, have an even lower patch rate of 10% compared to standard ICT systems (Samtani et al., 2016).

Active vulnerability assessment: In this technique, devices are probed to identify vulnerabilities. Examples of active assesment include port scanning, SQLi and HTML injection checks, attempts to brute-force password logins, monitoring network traffic, and dropping malicious or exploitative payloads.

Opportunities:

The guidelines provided by ENISA (Leszczyna et al., 2011) and NIST (Scarfone, K., & Mell, P. , 2012) are a step towards the right direction to descibe the best practices that the industry has to follow. One of the most promising techniques in this category is penetration testing in order to apply corrective actions and mitigation of any security weaknesses. Other promising techniques are simulation, modelling, and honeypots. This coupled with the desire of the SCADA vendors to provide integration with commercial database systems, will make it possible for real time data analytics to identify a threat vector before it strikes .

3.2.2 Configuration and patch management in ICS/SCADA

Configuration and patch management is an area of systems management that involves acquiring, testing, and installing multiple patches to an administered computer system. Patch management tasks include: maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required.

Challenge:

The biggest challenge in SCADA patch management, is that the settings of related devices may be corrupted and their functionality may change during the installation of the patch. Constraints on effort, cost and time imply that not all vulnerabilities can be fixed at the same time which implies that there is a necessity to prioritize vulnerable nodes and vulnerabilities of nodes, taking into account the system needs,resource constraints and severity of vulnerabilities (Yadav, G., & Paul, K. , 2019).

Mitigation:

Special consideration should be given to the following aspects of the patch management plan (Tom, S., et al., 2008):

- As a result of vulnerability assesment procedures, conducted by personnel knowledgeable of the system and its usage, a decision should be made regarding the urgency of patching activities.
- Urgency reviews should be conducted to evaluate the risk to operations and determine if immediate action is needed or if action can be delayed or deemed unnecessary at this time.
- Deployment of patches or other modifications to the system may nullify the warranty, thus arrangements should be made with vendors to address this issue before deploying the patch.

Opportunities:

An interesting research topic is the patch prioritisation method proposed by (Yadav, G., & Paul, K. , 2019). In their study, the authors present a system based on Viable System Model (VSM), Common Vulnerability Scoring System (CVSS), and Game Theory (GT) in order to provide a ranking of vulnerable SCADA subsystems as well as a ranking of subsystem vulnerabilities, thereby allowing a more well-informed strategy for patch management.

3.2.3 Perimeter defence of ICS/SCADA systems

Firewalls are the first line of defence within an ICS network environment. These components keep the intruder out while allowing through the legitimate traffic and the data necessary for an organisation’s operations. Thus, the concept of network segmentation applies to the network in layers to protect assets at all levels and this is the first point of control for validating access to internal systems.

Challenges :

Due to the requirement for low latency times and special protocols, traditional firewalls are not always suitable for an ICS environment, an in-depth defence is not feasible, and the proper use of DMZ’s not always applicable. Some typical tactics that malicious adversaries use are (Gonda, O., 2014): :

- Using a remote access port used by the vendor for maintenance.
- Intercepting a legitimate channel between IT systems and ICS/SCADA systems.
- Spear-phishing a user to click on a URL link in an email from a workstation that is connected to both the ICS/SCADA network and to the Internet.
- Infecting laptops and/or removable media while outside the ICS/SCADA network, later infecting internal systems when they're connected to the network.
- Exploiting configuration mistakes in the security of connected devices.

Mitigation:

As some parts of the ICS/SCADA systems are left unattended, physical access should be controlled by removing console-port cables and introducing password-protected console or virtual terminal access with specified timeouts and strict access policies. Also, commodity hardware should be avoided as the risk is high, as it could be seen in the VPN filter case (Kim, S. H., & Lee, K. H., 2018). Finally, deep packet inspection can provide an early warning without interrupting the SCADA/ICS network.

Opportunities:

Strengthening the perimeter of a networked system is an essential step towards defending a SCADA system from malicious activity. However, protective measures only serve to reduce the attack possibilities, which is not sufficient when dealing with an intelligent and highly adaptive adversary. The use of Activity Attack Graphs (AAG) and Course of Action (COA) matrices (Caltagirone, S., et al., 2013) considers the options available to an attacker and describes the characteristics of each attack event using a diamond model representation, developing a set of ’competing hypotheses’.

3.3 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 throughout the devices’ lifecycles.

3.3.1 Gain access to connected medical devices

In the latest years, the technology of Internet of Things (IoT) is used throughout the world in many areas. The connection of these microdevices helps workers optimise their work since the connected devices capture data across the processes. The rapid widespread adoption of IoT devices has an impact also in the healthcare industry since the connected medical devices in an average hospital room are up to 15 (O'Dowd, 2017). This means that the medical devices connected to the network of the hospital outnumber the smartphones in a hospital. While each of these devices has a specific mission to accomplish, which is inseparably connected with the health of a patient, each of them uses an open port to connect to the internal network of the hospital which can be used also for a malicious attack.

Challenge:

While the world clashes with the phenomenal pandemic of COVID-19, the hospitals are overcrowded with patients of severe pneumonia and the medical personnel is on the verge of exhaustion. Some people took advantage of the pandemic and performed attacks on hospitals; one of the most serious examples is the cyberattack on the Brno University hospital[1]. The attack caused an immediate computer shutdown and the hospital was forced to cancel operations and relocate patients to other hospitals. Also, it is worth pointing out that other cybercriminals took advantage of the fear around the pandemic and used phishing attacks at the

[1] https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

citizens. Under the mask of informational and health advice emails the cybercriminals try to spread malware and gain access to sensitive information.

Some of the most common type of cyber attacks which can lead to gaining access to a hospitals medical devices are:

- **Ransomware attacks**: A ransomware attack can compromise the data of a user and lock them in the system demanding ransom. If the ransom is not paid in time, all the data of the user will be destroyed. This type of attack is a massive threat for a hospital; thus all medical devices must secure the sensitive records of a patient.
- **Malware:** The malware software is programmed to damage a computer or device and even provide unauthorised access to the attacker who programmed it. It is also a massive threat for the health industry since 78% of providers reported that they experienced a healthcare ransomware or malware attack in the past 12 months (Snell, 2017).
- **Data breaches:** Data breaches in the healthcare industry are often related to the capture of patients records.
- **DDoS attacks**: A Distributed Denial of Service (DDos) attack can flood with traffic the servers of a hospital and ultimately bring down its system. Many of the medical IoT devices have open ports to communicate with external internet, so a DDoS attack on such devices can even become dangerous to a patient. For example, if a patient's insulin is controlled by a medical microdevice, a DDoS can shutdown the server that the microdevice is connected, resulting to a bad connection, loss of data and eventually to even loss of the patient's life.
- **Cryptojacking:** This type of attack leverages the processing power of a compromised device to mine cryptocurrency. In the healthcare system where most of the medical devices used for patients care, this attack can put the safety of the patient at risk.

Mitigation:

Indeed, the threats associated with connected medical devices create a severe risk in the modern healthcare system. This does not mean that it cannot be prevented with the continuous monitoring and updating of the connected medical devices as part of a wider secure network in a hospital. Some ways to secure a healthcare system are identified below:

- **Identify and monitor**: All the connected medical devices should be monitored in real-time, allowing the security team to find possible vulnerabilities. On this regard, when a hospital has a million of medical devices, this can only be achieved with tracking programs and Intrusion Detection Systems (IDS) that can check the network traffic of each device and the connection that they have.
- **Segment connected medical devices**: Using a partial connection on medical devices can reduce the risk of privilege escalation by an attacker in the hospital's network. For example, if an IT agent finds a possible rooted medical device, then he should immediately close all the connections of this device with the network to prevent the privilege escalation.
- **Keep devices updated**: Most of the software and hardware companies patch their programs/devices when a possible threat is identified. One fundamental rule to keep secure a large network is to keep it up to date. So every connected medical device should be patched to minimise the individual risk. A tragic example of unpatched machines was the WannaCry ransomware attack.

Opportunities:

Modern Connected Medical Devices (CMD) are designed to support monitoring and medical treatment over long-range wireless links in order to allow doctors to monitor patients remotely. Some works (Park, 2014; Sun, Zhu, Zhang, & Fang, 2011) proposed to connect the CMD proxy or the programmer to the Internet, in order to use an authentication server of a governmental health agency or hospital or establishing a secure channel over the Internet (Marin, Singelée, & Preneel, 2014).

Another trend in CMDs security is low-power and zero-power authentication methods, that aims at overcoming the computational and energy constraints of the CMDs. Proposed methods are harvesting energy from an external source (Halperin et al., 2008) without drawing energy from the primary battery or using Physical Unclonable Functions (low power hardware devices that have a very complex but stable input to output mapping) (T. Xu, Wendt, & Potkonjak, 2014). The rapid growth in physiological sensors and low-power communication has also enabled a new generation of wireless sensor networks called Body Area Networks, that can be embedded inside the body or surface mounted, and allow inexpensive and continuous health monitoring, which are exposed to several network and security issues (Dejon, Caputo, Verderame, Armando, & Merlo, 2019; Du, Guizani, Xiao, & Chen, 2008; Du & Lin, 2005; Du, Shayman, & Rozenblit, 2001; Du & Wu, 2006; Liang & Du, 2014).

According to the Transparency Market Research report, the US implantable medical devices market was expected to be worth $73,944 millions by 2018 (Wu et al., 2017). Connected medical devices are expected to become more common thanks to the recent development in IoT and Edge computing, and will be exposed to more cyberattacks.

Hospitals, in the centre of this crisis caused by the pandemic of COVID-19, are overcrowded and vulnerable targets because of this. By identifying and monitoring all the connected devices in real-time properly, running regular updates and preparing an incident response plan, the IT team can face all possible threats. It is worth pointing out that ENISA scheduled for June 2020, a real-time incident exercise in order to identify the cyber awareness in the healthcare sector.

3.3.2 Gain access to implanted medical devices

Challenge:

Implanted medical devices (IMDs) are electronic devices implanted within a human body for diagnostic, monitoring, and therapeutic purposes (Wu, Du, Guizani, & Mohamed, 2017). IMDs are usually small in size and have limited storage, computational, and energy capacities; they also have a wireless connection (through hospital networks or the Internet) with an external device known as programmer, that can change the IMDs' settings or extract health data. The wireless communication, combined with the IMDs constraints that limit the possibility of installing complex security mechanisms, long-range wireless transmissions and complicated cryptographic computations, expose them to a wide range malicious cyberattacks.

In fact, in recent years several cyberattacks to IMDs have been reported, compromising the privacy of health data or issuing fake commands. Works by (Halperin et al., 2008) showed the vulnerabilities of a commercial implantable cardioverter defibrillator, whose communication protocols were reverse-engineered in order to gain access to patient health data; commercial glucose monitoring and insulin delivery system have been revealed to have several security flaws, and it was demonstrated how adversaries can remotely take full control of some IMDs (Jack, 2013; C. Li, Raghunathan, & Jha, 2011; Marin, Singelée, Yang, Verbauwhede, & Preneel, 2016; Radcliffe, 2011).

Most IMD access control is proximity based, i.e., the programmer can generate the required key only if it is in proximity of the IMD, thus, the security of this model depends on the deterrence methods used to prevent adversaries from coming relatively close to the IMDs. Other opportunities are identity-based (password/secret, electronic health records for patient, family doctor, relatives), role-based (similar to the previous one, but only the role of the requested is checked, not the identity), attribute-based (a one-to-many encryption method that allows access only to users who possess a certain set of attributes) and risk-based (real-time and adaptable models, that can calculate the security risks from changes in certain parameters or anomalous patterns).

Mitigation:

The type of attacks and mitigation strategies can vary depending on the type of access control scheme implemented in the IMD; four categories have been broadly analysed in (Wu et al., 2017): i) direct access control with pre-loaded keys, ii) direct access control with temporary keys, iii) indirect access control via a proxy, and iv) anomaly-detection schemes.

Direct access control with pre-loaded keys: These schemes use a long-term key that was pre-loaded into the IMD for access control. There are different options when it comes to distributing the pre-loaded key to the authorised programmers, including a common master key for all programmers, and a specific device key for each IMD (C. Li et al., 2011), a rolling code authentication scheme in which the IMD and the programmer share an encryption key in order to encrypt the sequence number (Liu et al., 2010), and/or the possibility to use biometrics or items possessed by the patient to share the key (Cherukuri, Venkatasubramanian, & Gupta, 2003). All these methods are somewhat unfeasible or vulnerable since it is not realistic to require that all manufacturers use the same master key, nor it is feasible to share a IMD rolling code/encryption key with all possible hospitals, clinics, ambulances, and even bio-features may be socially engineered or stolen by an adversary. Finally, they all share a common vulnerability: the use of a permanent key. In fact, patients carrying IMDs may require treatment by other than their primary care physician, and the programmer used in these scenarios will gain unlimited access to the IMD unless the pre-loaded key is replaced, which is usually not done, since it would require too much effort.

Direct Access Control with temporary keys: The above-mentioned problems can be mitigated with the use of temporary keys to establishing an encrypted communication channel whereby either the IMD and the Programmer extract features from a common source and generate from them the common keys at the same time, or only one device generates the key, and then distributes it to the other. The key generation and distribution must be performed in the vicinity of the IMD, in order to reduce the chances of adversaries eavesdropping, and various methods have been implemented, such as biometrics (Bao, Zhang, & Shen, 2006; Cherukuri et al., 2003; Hu et al., 2013), body-coupled communications (C. Li et al., 2011), vibration (Kim, Lee, Raghunathan, Jha, & Raghunathan, 2015), audio and ultrasound (Halperin et al., 2008), and near field communication (Hei, Du, & Lin, 2014).

Indirect Access Control via a Proxy: Since IMDs have a limited battery capacity, it can be preferable to use an external device (proxy), with more computational and battery capacity, to implement an indirect access control between the programmer and the IMD. Based on symmetric encryption, it allows for more power consuming access control schemes, and multi factors access control. However, the use of a proxy device increases the vulnerability surfaces, for example allowing the adversary to launch an attack through malicious app on the proxy, or just physically stealing or removing the proxy (in case of an emergency some proxy-based access control are designed to be disabled simply putting the proxy device out of range). Friendly radio jamming or gateway-based schemes (Denning, Fu, & Kohno, 2008; Zheng, Fang, Orgun, & Shankaran, 2014) can be used to protect the communication in the presence of eavesdroppers, blocking packets sent by adversaries. Sensors in modern mobile devices such as accelerometers, barcode visible light communication, LED blinking sequences can be used to assist the generation/distribution of the temporary key, for example generating the key from biometrics parameters like the patient walking characteristics (M. Li, Yu, Guttman, Lou, & Ren, 2013; W. Xu, Revadigar, Luo, Bergmann, & Hu, 2016)

Anomaly detection: In this type of access control schemes, the aim is to identify resource depletion and unauthorised accesses, using machine learning and artificial intelligence techniques to extract normal behaviour patterns and thus, detect any present anomaly by comparison. These methods may use physiological changes, or IMD access patterns (commands, time, locations), but may not achieve a 100% accuracy. Many parameters can be used to extract a normal behaviour, such as resource consumption, physical characteristics of the wireless communication as received signal strength indicator, time of arrival, differential time of arrival, angle of arrival (Hei, Du, Wu, & Hu, 2010; Zhang, Raghunathan, & Jha, 2013) and even biometrics, such as bowel sound (Henry, Paul, & McFarlane, 2013).

Opportunities:

Given the quite similar nature of CMDs and IMDs, the opportunities described in Section 3.3.1.1 also apply to this case.

3.3.3 Weak encryption protocols on medical IoT devices

Weak encryption protocols are often used on medical IoT devices which allows attackers to gain access to the device or intercept the communication between the devices, and cause either interruption of the operation or act as a pivot point into the network.

Challenge:

Usually, medical IoT devices have quite limited computational resources, and therefore, secure modern algorithms and complex protocols cannot be used. Unfortunately, lightweight cryptography protocols do not provide a sufficient security level and sometimes old and insecure algorithms and protocols are implemented. Such an example is the DES algorithm which is susceptible to brute-force and differential cryptanalysis attacks. Hence, the conventional cryptographic primitives might not be suited for such low-resource smart devices.

Mitigation:

The common solution is to increase computational power and deploy bigger batteries. Unfortunately, such an approach decreases the mobility of these devices and increases their cost. Sometimes simple security protocols or modified encryption algorithms (i.e., simplified symmetric ciphers with limited rounds/iterations) are implemented.

Opportunities:

Development of new secure and lightweight algorithms/protocols is a quite emerging research topic, commonly referred to as lightweight cryptography. By implementing lightweight encryption algorithms that have a smaller key size, fast processing, and require less computation power, medical IoT devices can be resistant to cyberattacks and provide a sufficient level of security.

3.3.4 Resource exhaustion attacks on medical IoT devices

A resource exhaustion attack results in the consumption or allocation of resources in an unwanted manner accompanied by a failure to release these resources when they are no longer needed, eventually causing their depletion and subsequent unavailability of the underlying devices and systems.

Challenge:

Many commonly used protocols like TCP and IPsec base their security on cryptographic primitives. While secret-key primitives are computationally cheap, the same does not apply to public-key primitives which are significantly more expensive. This creates a problem since low powered devices like the medical IoT ones can have their resources exhausted even with some simple cryptographic primitives. Many protocols were identified as vulnerable to this kind of attacks during the past years, however, resource exhaustion attacks can be broadly classified into the following to categories (Groza & Minea, 2011):

- **Resource exhaustion DoS attacks due to excessive use:** In this type of attacks, the attacker does not exploit the protocol, however, they consume more resources than the other processes running on the medical IoT device.
- **Resource exhaustion DoS attacks due to malicious use:** In this type of attacks, the attacker tries to create an abnormal state at the protocol level in order to create a condition from which the protocol can no longer recover from.

Mitigation:

In order to mitigate such DoS attacks, it is necessary to provide an efficient filtering mechanism at the network level which will be able to distinguish legitimate from malicious traffic. Many of the solutions existing today are end-host filtering mechanisms which are responsible for detecting attack signatures and dropping the packets that are intended for the victim. However, this kind of solutions do not prevent flooding attacks when the objective simply is to send a large number of packets and exhaust the resources, either of the victim or of the filtering mechanism itself.

Opportunities:

The work of (Jan et al, 2019) proposes a scheme that verifies the identities between the server and the client by using a payload-based mutual authentication. In their approach, a lightweight handshake mechanism is implemented that utilises the features of the Constrained Application Protocol (CoAP) that in turn relies on Datagram Transport Layer Security (DTLS). However, since the DTLS uses computationally expensive features, the study proposed an alternative secure mechanism that does not rely on a separate protocol layer, further reducing the computation and communication cost.

3.4 Network and distributed systems

3.4.1 Fragmentation as IDS evasion technique

Fragmentation denotes a division of a packet into smaller subpackets. These fragmented subpackets are then reassembled by the recipient’s node at the IP layer. Afterwards, the subpacket is forwarded to the Application layer. In order to analyse the fragmented traffic properly, the network detector has to put together these fragments as it was before at the sender's node.

Challenge:

This requires keeping the data in the memory by the detector and matching the traffic with a signature database. The methods used by attackers in order to avoid the detection are fragmentation overlap, overwrite, and timeouts. Their aim is to hide attacks in such a way that they are treated as normal, allowed traffic. Fragmentation attack generates a malicious packet by replacing information in a sequence of fragmented packets. Knowing this fact, the attackers try to take advantage of this situation and generate malicious packets for a long time so that the attack might not be detected.

Mitigation:

In Anomaly-based Intrusion Detection Systems (AIDSw), 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 is treated as an anomaly, which can be regarded as an intrusion.

The statistics-based approach leads to the creation of a statistical model of normal user behaviour which is built by collecting and analysing every data record. However, knowledge-based approaches 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 in the area of AIDS. Some algorithms, such as genetic algorithms, clustering, artificial neural networks, association rules, decision trees and nearest neighbour methods can be applied in order to gain specific knowledge based on the intrusion datasets (Kshetri & Voas, 2017; Xiao, Wan, Lu, Zhang, & Wu, 2018).

3.4.2 Flooding as IDS evasion technique

The attacker begins the attack to overwhelm the detector and this causes a failure of the control mechanisms. When the detector fails, all traffic would be allowed. A popular method to create a flooding attack is spoofing the legitimate User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP).

Challenge:

The traffic flooding is used to disguise the abnormal activities of the cybercriminal. Therefore, IDS would have extreme difficulty to find malicious packets in a huge amount of traffic.

Mitigation:

[Same as in Section 3.4.1.]

Opportunities:

[Same as in Section 3.4.1.]

3.4.3 Not minding the gap: direct internet connections

Direct internet connections are typically established for obtaining software updates from the Internet instead of an internal server or to provide third-party constructors with access for maintenance purposes. In this way, additional pathways are available for attackers to compromise a network.

Challenge:

During the last years, we have seen a significant increment in the use of cloud technologies and mobile devices. This led an exponential increment of the Internet traffic generated from those devices that often operate outside the organisation’s network. This means that not all cybersecurity controls put in place to defend the organisation’s network are effective. Moreover, there is a set of services that do not work with security devices that inspect the traffic, like firewalls or proxies. For these reasons, it is necessary to introduce new solutions that secure both users and organisations.

Mitigation:

Security vendors have developed agents for secure mobile device that operate outside the organisation’s network. In this way it is possible to cover all the security controls that are put in place by an organisation, while keeping the same policy, such as DNS security, internet traffic monitoring, endpoint protection, vulnerability management and compliance, email security, and many more. At the same time, the analysis and configuration in a proper way of the local firewall could be very helpful in the process of restricting the Internet access perimeter.

Opportunities:

An emerging topic in cybersecurity is next-generation firewalls (NGFW). Typically, this kind of firewalls uses deep packet inspection that combines intrusion prevention systems and other more advanced network traffic flow controls (Neupane, K., et al., 2018). This is the core of all the new generation of stateful firewalls and creates interesting opportunities for cases in which traditional firewalls are not efficient.

3.4.4 Theft, sabotage, and fraud in SIEMs and analytics systems

Security Information and Event Management (SIEM) systems can be one of the most important components of an insider threat program. These systems receive log information from various devices across the enterprise. A SIEM system can help insider threat programs by consolidating logs into a central location, and automatically prioritising events, making those with a higher priority more visible to an analyst for action.

Challenge:

In the last few years more enterprises have moved their data to the cloud, thus de facto, transforming their infrastructure into a decentralised one, and therefore making more difficult to maintain visibility mostly when communications and connection increase. Without proper visibility, external actors may find weak parts of the IT environment in which to slip into the network or plant a dwelling threat.

Moreover, another insidious cybersecurity challenge faced by businesses involves insider threats. These occur when an employee either maliciously or accidentally acts against the enterprise digitally or creates a security hole (e.g., weak credentials). In this context, a SIEM adoption helps prevent these occurrences through its log management and aggregation capabilities.

Mitigation:

SIEM systems can help detect anomalies, which may lead to discovering potentially malicious insiders. The system's baselining and correlation components can perform a first order of rudimentary analysis that presents a more organised view of the raw log data. SIEM systems also aid in investigations by providing evidence that can be used for both internal incident response and external legal actions.

SIEM solutions provide user and entity behavioural analysis (UEBA). This critical capability helps establish behavioural baselines of normal workflows and activities. If a user or entity violates this baseline, it automatically triggers an alert and may also trigger an activity freeze. Therefore, a security team can investigate quickly and potentially mitigate any damage caused. Additionally, a SIEM can map:

- Network or host data exfiltration;
- Recruitment of insider via chat or email;
- Creation or use of fraudulent assets;
- Creation of unknown access paths (backdoor accounts);
- Deletion of logs;
- Introduction of unauthorised code in software; and
- Physical data exfiltration (print/scan/copy/fax).

Opportunities:

Easy-to-use and highly configurable interfaces for SIEM systems would be particularly valuable as they could simplify the interaction with such a system for user activity monitoring, thus allowing an organisation to understand how employees interact with all endpoints in their environment. Logs are valueless unless subjected to regular and random review, with a follow-up if anomalies are detected, and therefore there is need to study correlation techniques for log aggregation so as to provide an additional layer of confidence as anomalous activity across systems can be related, resulting in potentially identifying an attack pattern or other irregular activity that would not be apparent from a single log.

3.5 Cloud, edge and virtualisation

The security problem of cloud computing is intrinsically complex because cloud computing is based on existing technologies and architectures, such as SOA, SaaS, and distributed computing. Having all the advantages of these technologies and architectures, cloud computing also inherits almost all security problems from different levels of the system stack. The cloud computing model changes the trust model when cloud users move their applications from the boundaries of the enterprise or organisation to the open cloud.

In this case, cloud users may lose physical control over their applications and data, and traditional security mechanisms, such as firewalls, are not applicable to cloud applications. Cloud service providers must provide the necessary security services to meet the security requirements of individual cloud computing users while respecting the rules /and ensuring compliance using secure auditing mechanisms. Applications from different organisations and domains can be located on the same physical and computing resources, interact with each other, and any intentional or unintentional incorrect behaviour of one cloud user can cause victims for other users and will create more opportunities for cybercriminals from the Internet.

3.5.1 Hardware vulnerabilities

Hardware attacks aim at physically accessing a system to obtain stored information, determine the internal structure of the hardware, or inject a fault. The attacker explicitly triggers the deception mechanism by manually placing it in the target environment and, where applicable, explicitly responds to events when user interaction occurs. The attack procedure is flexible, because the attacker has full control over the process and may modify it during the attack.

Challenge:

A hardware attack is first classified by the goal for which it is launched. The goal is the malicious action that the attacker wants to take against an asset of the attacked hardware, defined as a target. The target can be the information that the hardware is treating, but also a property of the hardware itself, either functional or non-functional. A hardware attack is qualified depending on the modality in which it is carried out. The attack is invasive when the actions taken against the attacked hardware includes physical intrusions such as desoldering, depackaging, disconnection of its internal components.

Computers typically store secret data in DRAM, properly de-powered when the device is tampered with. It is common to think that once the power is down, the content of volatile memory is erased. However, it has been proven that the charge stored in a DRAM cell has a given decay rate which is not infinitive and strictly depends on temperature. At temperatures from −50◦ C down, the contents of RAMs can be “frozen” and kept for one or even more days. This is what usually happens in a cold-boot attack, in which the hacker uses spray cans or liquid nitrogen on a volatile device just disconnected from the original system, and gains precious time to perform a memory dump, i.e., a copy of the contents on a non-volatile device for subsequent analysis. Data remanence affects in a different way non-volatile types of memory such as EEPROM and Flash. Therefore, sensitive information thought to be erased can still be extracted.

The attack is characterised as non-invasive when it can be carried out without any physical contact with the device under attack. Non-invasive attacks are further split into passive and active. Passive non-invasive attacks are carried out by analysing and measuring one (or more) physical dynamic entities of the attacked hardware. A covert attack is when the victim is not aware that it is taking place. An attack is overt when the victim is aware that it is taking place. In this case, the attacker has one or more of the following goals:

- Disrupting the system to prevent it from working as expected.
- Preventing the system from working (denial of service).
- Reverse engineering the system, to later copy it.

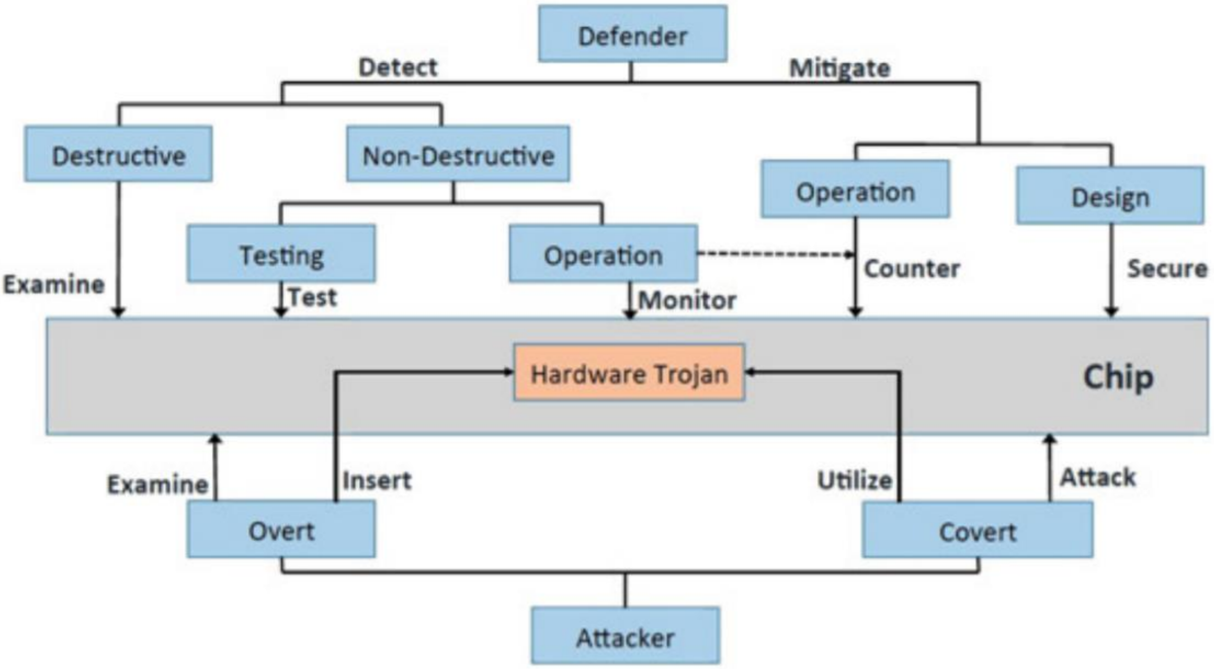

Figure 4: Hardware attack and defence strategies (source: Moein et al., 2017)

Mitigation:

The main hardware attack mitigation techniques are:

- **Hiding:** Hiding is a powerful technique that can be used against an attacker attempting to gain information from chip emissions; the following techniques can be used to hide chip emissions:
  - **Noise Generation:** The Signal-to-Noise Ratio (SNR) can be reduced by either lowering the signal strength or increasing the noise level. For example, noise generators decrease the SNR, which reduces the ability of an attacker to extract information from chip emissions.
  - **Balanced Logic:** Balanced logic is a technique used to make chip emissions independent of the data being processed. For example, Dual-Rail Pre-charged (DRP) logic can be used to create two outputs operating in different phases.
  - **Asynchronous Logic Gates:** Asynchronous logic gates can be used to lower electromagnetic (EM) emission levels by reducing or eliminating the need for clock synchronisation.
  - **Low Power Design:** Low power design is a method used to lower the SNR and hide chip emissions to reduce the ability of an attacker to obtain chip information.
  - **Shielding:** Shielding is an effective method to hide chip emissions and can be achieved via physical shielding or filtering of chip emissions. Metal layers on the outside of a chip can be used to shield EM emissions.
- **Masking (Blinding)**: Masking or blinding is a technique used to make it difficult for an attacker to determine the relationship between chip data and emissions. This can be accomplished on a per-gate basis using masking logic, or a per-block basis by randomising the input data and reversing this operation to obtain the results. The input data can also be masked with random data before any operations and the results obtained by removing the mask.
- **Design Partitioning:** Design partitioning prevents information leakage between chip regions. For example, regions that operate on plaintext can be separated from those that operate on the ciphertext.

- **Anti-tampering:** Anti-tampering or physical security is used to limit access by creating a secure zone around a chip. This also reduces the amount of emission data that can be collected.
- **Emission Filtering:** Hardware or software emission filters can be used to reduce the amount of data that is leaked.
- **Restricting Physical Access**: Restricting access to a device is a simple countermeasure against fault attacks. Encapsulating a device in a tamper-resistant case is an effective means of restricting access, which has been successfully implemented.
- **Randomised Computation:** Time Randomising the computation time of chip operations provides protection against fault attacks.
- **Deep Sub-micron Technology:** Data can be protected using storage devices covered with a top metal layer or constructed with deep sub-micron technology, which makes it difficult for an attacker to access the transistor level or recover data that has been erased.
- **Error Detection:** Error detection codes are used to generate check bits for input data and operation results. If the check bits at the output are incorrect, a fault is detected and the output data is discarded.
- **Duplicate Operations:** Chip operations can be executed multiple times and the outputs considered valid only when they are identical. If the results differ, an alarm is raised. This is not the best solution to defend against fault-based attacks since a fault may still go undetected. It increases the system complexity, but also the resources and time required by an attacker to obtain sufficient data, so while implementation is simple, the overhead is high.
- **Top Layer Sensor Meshes:** Sensor meshes are mainly used to protect against microprobing attacks. They are placed above the circuit to detect interruptions and short circuits. If procedures such as selective etching or laser cutting are sensed, an alarm can be raised and countermeasures taken such as erasing nonvolatile memory. These meshes can also protect against under-voltage or over-voltage analysis attacks.
- **Clock Frequency Sensors:** Robust low frequency sensors are used to detect tampering which slows the clock frequency. If a sensor raises an alarm, countermeasures, such as processor reset and bus line and register grounding, can be taken.
- **Randomised Clock Signal:** This technique can be used to prevent an attacker from predicting the execution time of specific instructions. Most covert hardware attacks require the attacker to predict the time at which a certain instruction is executed. Moreover, processors typically execute the same instructions with a fixed number of clock cycles after each reset, which makes processor behaviour predictable. This behaviour simplifies the use of protocol reaction times as a covert channel. Therefore, random time delays should be inserted between any observable action and critical operations that might be subject to an attack. If serial ports are the only observable channels, then random delay routine calls controlled by a hardware noise source can be employed. Random bit-sequence generator in conjunction with an external clock signal can be used to generate a random internal clock signal to make behaviour prediction more difficult.
- **Randomised Multi-threading:** The predictability of execution cycles in a processor can be decreased by implementing a multithreaded architecture, which randomly schedules execution on multiple threads. Randomised combinational logic can be used to determine the progression of thread execution in a processor.
- **Test Circuit Destruction:** Chip testing is done after production, and leaves residual test circuits, which can be exploited by attackers to gain access to buses and control lines. Therefore, the destruction of these circuits is an important attack countermeasure. To achieve this, the test interface for a chip can be placed within the area of another chip on the wafer. Then when the wafer is cut into dies, the connections between the chip and test circuitry are destroyed.
- **Restricted Program Counter:** The program counter can be used as an address pattern generator to simplify reading the memory contents via microprobing. To counter such attacks, watchdog counters can be used to reset the processor if no jump, call, or return instruction is executed for a number of cycles, but this requires additional circuitry. Another approach is to modify the program counter so that

offset counters are employed to cover the entire address space. Each call, jump, or return instruction writes the address of the destination in a register and resets the program counter.

- **Encrypted Buses:** Encrypted buses can be used to make it intractable for an attacker to obtain chip data. The encryption typically employs a Random Number Generator (RNG) which is initialised at the sender and receiver using a private key.
- **Light Sensor:** Light sensors can be employed to prevent chip operation after it has been decapsulated.
- **Glue Logic:** Glue logic can be used to transform standard building block structures, i.e., the ALU, I/O, registers, or CPU circuits to Application Specific Integrated Circuits (ASICs) with a similar logic design. This makes it very difficult for an attacker to find specific signals or circuitry within the IC. Glue logic design can be achieved using special design tools.
- **Obfuscation:** Obfuscation is a technique that transforms a circuit or design into one that is functionally equivalent but is significantly more difficult to reverse engineer. Thus, more resources and time will be required for an attacker to determine chip functions. Obfuscation can also be implemented using PUFs or programmable logic. In this case, the logic is configurable to functionally equivalent designs to conceal the signal paths.
- **Verification Difference:** Verification difference is used to test chips by comparing measurements with signature values to detect differences between genuine and altered chips. Altered chips will have a significant difference and thus can be identified. This technique includes power and time delay analysis as well as Scanning Acoustic Microscopy (SAM), IR thermography and X-Ray Fluoroscopy (XRF).
- **IP Watermarking Intellectual Property (IP):** Watermarking is a technique similar to paper watermarking and is used to protect against counterfeiting. This is achieved by inserting proprietary information into the IC design. The result is a unique design that includes the watermark within the chip functions. The watermark can be embedded in different abstraction levels of the design making it difficult to detect and/or remove.
- **IP Fingerprinting:** IP fingerprinting assigns a unique and hidden ID into each instance of the IP. It is typically employed to detect IP overbuilding by a factory.
- **IC Metering:** IC metering is a set of security protocols that enable designers to gain post-fabrication control of IC properties and use, including remote runtime disabling. A unique ID for each IC is included in the Finite State Machine (FSM) of the design. This is achieved by adding new states and transitions to the original IC FSM to create a Boosted Finite State Machine (BFSM). To bring the BFSM into the initial (reset) state, knowledge of the transition table is required. Since only the designer has this information, it will be difficult for an attacker to generate the input sequences required to bring the BFSM into this state. Another IC metering protocol is based on PUFs. It provides control over all hardware copies and allows counterfeit ICs to be disabled.

Opportunities:

Each type of hardware attack requires its own mitigation methods. Hardware designers systematically rely on Design-for Testability and Built-in Self Test (BIST) methodologies to improve testability of the target system both at the end-of-production and in-field. To protect the system against a timing attack, a defender needs to determine which mitigation techniques can be used to protect the system. This indicates that any one of the techniques such as noise generation, masking (blinding), design partitioning, anti-tampering (physical security), time/branch equalisation, adding random delays, constant time hardware, non-deterministic processor, and random computation time, can be used to counter a timing attack. Some of these techniques can be implemented during the design phase (e.g., design partitioning), while others can be implemented during the operation phase (e.g., noise generation).

3.6 AI and big data analytics

Artificial Intelligence (AI) is an attractive target for attackers. Attackers can attempt to manipulate algorithms or the data that they work with in order to influence the results. Malicious actors could influence the behaviour of the system and can also be used to launch cyberattacks (e.g., attackers could develop algorithms to discover what types of malware will be the most effective in a certain environment or what type of users are the most susceptible to spear-phishing).

3.6.1 AI in the military

There are numerous uses for AI in the military, but the boundaries around what constitutes acceptable uses are highly contentious. The issue of lethal autonomous weapon systems (LAWS) continues to be discussed at the international level under the United Nations Convention on Certain Conventional Weapons (CCW) by the Group of Governmental Experts (GGE). Annual meetings since 2013 have brought together representatives from dozens of countries to consider the possibility of an international ban on LAWS, a position officially supported by at least 26 countries. The CCW process requires full consensus, however, and while a majority of states favour moving toward a prohibition, five key states (the United States, Australia, Israel, South Korea, and Russia) have opposed a ban. Deliberations still continue.

In the meantime, weapon systems with certain degrees of automation are already in use. Israel Aerospace Industries has developed a warhead missile nicknamed Harpy that detects and attacks autonomously; Harpy has already been sold to the Air Forces of several countries. The French company Dassault Aviation has a highly autonomous combat air system with attack capabilities called NEURON. And BAE Systems, based in the United Kingdom, has developed Taranis, an advanced armed drone that can identify and target threats, although it is designed to seek verification by a human operator.

Other, non-lethal, applications of AI in the military also require consideration. For example, the US Department of Defense (DoD) has a program called Project Maven that uses computer vision machine learning to identify objects of interest from vast amounts of video footage from drones and other sources.

Challenge:

The AI systems have numerous applications for military use, nevertheless their main components (computer hardware, algorithms/programs and data) are similar to the other information systems. The technical cybersecurity challenges are related to the way the different AI systems are implemented. The functioning of these systems depends not only on their internal state, but also on the data they receive from the external systems (including the HMI) they are interfaced with, which depends on the application. Some of the main applications of AI systems in the modern warfare are:

- **Decision support systems:** Such systems aim at rocessing huge amounts the data, coming from all types on sensors on the battlefield in real-time (multi-sensor data fusion) so to be able to perform the best course of action propositions for given goals, set by the command staff.
- **Usage of AI-powered physical systems:** These include autonomous robots, operating in the space, air, water, and also on the ground.
- **Usage of AI systems for propaganda**: These systems can generate altered news based on real data so they can influence the sentiment of the population.

Since each of these systems uses some kind of network communications (to receive commands and data, to return results, to perform coordination among its sub-systems or its copies), one of the technical challenges is to ensure the security of these communications even on adversaries-controlled territory. Moreover, autonomous and semi-autonomous robots use navigation systems which might also be subjects of cyber-attacks. The protection of the navigation systems against cyber-attacks is a challenging topic, especially when the system is operating on the adversary territory.

Another challenge comes from the fact that commercial companies are the main investors in the AI systems, so the cutting-edge research and development happens in the private sector. The effect is that 'dual-use' commercial off-the-shelf (COTS) technologies make their way into military products. One of the development principles in the business stands "Quickly in production: A working prototype is much more valuable than a perfect plan". When the development must deliver a working prototype, one of the first things left for later is the cybersecurity. This might lead to the incorporation of not well-secured technologies in the military systems. The cybersecurity analysis of an AI system needs expertise in both the AI and the cybersecurity which might be challenging for the system integrators.

There are also examples which show that some neural networks can be deceived by using special (crafted) input, developed with the knowledge of their internal structure. The development of such techniques and protection from them requires high technical expertise and knowledge of the own and enemy`s military AI systems.

Mitigation:

While there is no universal solution to the cybersecurity challenges regarding the protection of the military AI-based systems, the usage of proven communication protocols, designed with protection in mind will help to mitigate some of the common threats like sniffing or in-flight network data modification. There can be implemented systems acceptance procedures so that the security of the AI systems for military usage to be evaluated by independent (from the development company) security experts.

In addition, since the human factor has proven to be one of the weak components of IT systems, it requires special care. The operators of the military AI systems must be aware of the potential risks, and motivated not to perform malicious actions against the systems.

Where there are data sets, which contain the "knowledge" (pre-trained data) of the AI system, they can be made read-only. The OS permissions or hardware means shall be used. The operating procedures can be modified to include check the systems software and firmware images for modification (with provided means to do it) before the beginning of a mission.

All of the entry points of the systems must be secured to allow only the intended data types and protocols. The AI-based weapon systems must not be connected to general purpose networks. The firmware update access ports can be sealed so unauthorised access can be detected by inspection of the stamp. In case of a successful attack/data modification, there should be implemented and tested backup and restore solutions that should be designed to allow for quick recovery.

To mitigate the GPS jamming or spoofing attacks, or at least to detect them and take predefined actions, there can be employed techniques for alternative navigation. Some of them are based on AI-assisted terrain-recognition technologies, while others rely on inertial navigation.

Opportunities:

While AI-based systems can be employed by the adversary forces in the digital (cyber) domain, own AI-systems can be created to face them and try to protect own networks, databases and other digital assets which might be under attack. Such AI systems should be developed with ability to give transparent answers, along with HMIs allowing to explore the reasoning behind their conclusions where possible. To protect the communications of the future, the possibility for development of quantum entanglement network technologies might be explored. On success, the technology can render the known man-in-the-middle (MITM) attacks impossible.

3.7 Data security and privacy

3.7.1 Credential stuffing attacks

Credential stuffing is a cyberattack in which credentials obtained from a data breach on one service are used to attempt to log in to another unrelated service. Criminals are essentially creating mini-botnets that exist solely to focus on validating massive lists of login credentials

Challenges:

Protecting accounts from credential stuffing attacks is a difficult task due mainly to the following reasons: (i) frequent reuse of usernames and passwords across multiple services; (ii) hackers' use of bots for automation; and (iii) lack of training among the employees which leads to poor digital hygiene.

Mitigation:

Some of the proposed mitigation techniques in order to alleviate or reduce this kind of attacks are the following:

- Multi-factor authentication;
- Adding additional steps to a login process;
- Using secondary passwords;
- Using services for identifying leaked passwords;
- Providing the user with a generated username;
- Using CAPTCHAs;
- Using PINs;
- Using security questions;
- Creating a blacklist for suspicious IP-addresses;
- Disallowing email addresses as user IDs;
- Blocking access to headless browsers;
- Device fingerprinting; and
- Rate-limit on non-residential traffic sources.

Opportunities:

An interesting opportunity that requires further research as a potential mitigation technique is presented in the work of (Thomas, 2019). In that study, the authors presented a design of a new privacy-preserving protocol that allows a user to learn whether their credentials appear in a data breach without however revealing the information queried.

3.7.2 Access to unencrypted data (finance, health records)

Challenge:

Access to unencrypted data leaves systems and services at risk and may cause real harm and distress to individuals including identity fraud; fake credit card transactions; exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence, fake applications for tax credits, and mortgage fraud.

Mitigation:

Techniques that can mitigate such risks include the following:

- The pseudo-anonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the data processing.
- Continuous network security monitoring with behavioural anomaly detection.
- Elimination of all unnecessary connections.
- Prioritisation of protection to the most critical systems

Opportunities:

Opportunities mainly arise through appropriate training, including responsibilities of controllers and processors, responsibilities for protecting personal data (including the possibility that staff may commit criminal offences if they deliberately try to access or disclose these data without authority), the proper procedures to identify callers, the threat presented by people trying to obtain personal data by deception, and any restrictions in place on the personal use of systems by staff.

3.7.3 Unauthorised modification of multimedia content

Attackers can easily alter some parts of multimedia content (images, video, sound) using available tools for multimedia processing. Such multimedia content can be used in security related applications, such as CCTV.

Challenge:

Unprotected multimedia content might be easily used or modified by other parties with no further consequences. Since the data is usually not marked in any way by its owner, any manipulation can be hardly detected. This may lead to modified content which can be used in an undesired manner.

Mitigation:

In order to avoid unauthorised multimedia manipulation, digital watermarking can be used. This technique may be used to verify the authenticity or integrity of the original signal or to show the information about its owners.

It is effectively used for tracing copyright infringements and for banknote authentication. Any manipulation of the original content might be also easily detected.

Opportunities:

Watermarking technology provides protection of the digital content against undesired manipulations, infringement of copyrights or disclosure of private information. Watermarking solutions may also be applied for steganography purposes or for private and sensitive data anonymisation and protection.

3.7.4 Ransomware against Electronic Medical Records (EMR)

Cybersecurity within the healthcare sector is often neglected due to lack of investment and understanding of the risks. Hospitals have undergone a spate of ransomware attacks on poorly protected electronic medical records (EMR). This includes both encryption of the data and lack of perimeter security controls. Due to the importance of the EMR and the urgency for which they are needed to be accessed, most victims pay the ransom, but this is resulting in even more attacks.

Challenge:

Ransomware is a malicious software (malware) that denies users access to their data unless they pay a ransom. Typically, hackers encrypt data and promise a decryption key in exchange for a ransom. Health care data are especially vulnerable, given the imperative of acute care interventions..

With the advent of IoT devices in the health care sector, these problems increase. Most vendors only deal with parts of the IoT ecosystem and, typically, their priorities have been providing novel functionality, getting their products to market soon, and making them easy to use, rather than securing their devices.

Mitigation:

No fail-safe solutions exist, and there are tradeoffs between data security and data access to essential patient care information. The most promising approach is for health IT companies to identify vulnerabilities in their operating systems and issue patches (which must be promptly installed) to prevent their exploitation. However, patches can themselves be problematic because they can be incompatible with existing software and must therefore be adequately tested.

So, one particularly popular line of IoT security research in health is IoT context-aware permission models, where collaborative models are designed to secure IoT environments from malicious actors. For instance, a policy abstraction language that is capable of capturing relevant environmental IoT factors, security-relevant details, and cross device interactions, could be built to vet IoT specific network activities. In addition, health organisations should check and monitor settings on cloud service architecture, i.e., they should not maintain default settings.

Opportunities:

Frameworks that take into account, when testing threats, the presence of smart objects with very limited hardware should be created. In addition, crowdsourced repositories where IoT operators can share derived attack signatures, which deviate from the captured benign policies, should be built. Also, in this case, using blockchain technologies for tracking data movement can be an interesting opportunity. A distributed access and validation system could be built using the blockchain to replace centralised intermediaries (e.g., https://medrec.media.mit.edu/).

3.7.5 Bio-hacks for multi-factor authentication

Given the pervasiveness of some technologies and their ability to exchange and disseminate data, one of the main factors to consider in the design of an IT architecture is user authentication. This process is important in many different areas such as online payments, communications, and access-rights management. In recent years, the interest around biometric authentication and its role in authorisation systems continue to grow.

Biometric fingerprint readers, facial recognition systems, and retinal scanners have proven to be effective in authenticating users in consumer devices. Many enterprises are using or exploring biometric authentication to safeguard their sensitive data. Despite the widespread use of biometric authentication systems being a highly debated topic at the scientific level, some researchers see these technologies as a security solution while others see them as part of the problem.

Challenge:

Attacks on biometric authentication systems can be divided into two macro-categories, direct attacks and indirect attacks. **Direct attacks** involve the use of techniques that are beyond a deep knowledge of the authentication system. Among these types of attacks, the following should be considered: the theft of the fingerprint, the use of systems for the re-production of fingerprints, and requests under threat to users for the use of their biometric parameters. **Indirect attacks** involve, instead, the knowledge of the IT architecture and the data exchange methods of the authentication system. In this case, the user does not steal the user's biometric data but uses it in his favour. Examples related to this type of attacks include (i) redirection to fake fingerprint servers, if they are online, (ii) theft of biometric information relating to the user not directly on the authentication system, but through hacking of third-party systems such as clinical laboratories, and (iii) MITM attacks in which the malicious user intercepts the communication channel to collect the biometric data, and (iv) human microchips are subject to all foreseeable attacks when using RFiD technology such as sniffing, cloning & spoofing, and DoS.

An important type of bio-hacks for multi-factor authentication is the theft of the authentication token or tokens. Authentication systems can always be attacked when a person authenticates, no matter if it is via password or the use of biometric data, because the result of the authentications is still the assignment of a token. In the case of the use of biometric or multifactorial technologies, the user can authenticate with his smartphone by entering a fingerprint and subsequently a confirmation code of his identity, and at that point, he is assigned a token that will use in subsequent identifications in the session. If a malicious user is able to hold that token, he can act as the authorised user.

Mitigation:

As previously described, malicious users may be able to intrude on all parts of the system that involve exchanging information between components. In this sense, cryptography, introduced on communication channels, can be seen as a mitigating element. Furthermore, it is necessary to know, where they are used, all third party the development chains and must be sure that they use secure development lifecycle, in addition to owning systems for account lockouts and management of bad attempts.

If there is a DoS attack or injection, is important to have a system alarm (SIEM) and force the activation of alternative or exception handling procedures. Also, the code signing technique can detect any tampering or alteration in the code, thus mitigating such attacks. Another form of mitigation may be the use of solutions, like Binding Tokens, that require bi-directional, server-side and client-side authentication.

Another way to mitigate the multi-factorial authentication bio attacks is to spread factors across different communication channels and adopt dynamic authentication, where additional factors are requested for higher risk circumstances. Finally, to avoid identity theft, the user can be asked to provide to the authentication system other factors such as share his location or use another device. Finally, conventional security measures could be adopted, such as CCTV cameras and anti-tampering alarms.

Opportunities:

One of the main problems in adopting multi-factorial authentication systems that contain biometric parameters is the usability of this type of authentication systems. At the moment, the performance of processing biometric parameters remains very high, lengthening the identification times and making the applicability of such solutions less attractive.

Optimising the hardware and software components remains an open challenge, which involves different sectors of information technology from computer vision to the electronic study of wearable micro components.

A technological improvement in the consumption of sensors and processors would make it possible to build biometric patterns, composed of multiple factors such as heart rate or respiratory rate, which would make up a permanent and difficult to imitate individual biometric signal.

Another open opportunity lies in computer vision field, and is the ability to recognise an image in any context has been detected. Being able to recognise low quality images with occlusions or other visual problems remains today, one of the most discussed study object of computer vision.

3.8 Incident handling and digital forensics

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

3.8.1 Lack of SCADA forensic tools

Industrial Control Systems (ICS) and SCADA systems are used in many different industrial sectors and critical infrastructures, including manufacturing, distribution, and transportation and run 24/7 to control and monitor processes.

Challenge:

Early SCADA systems were intended to run as isolated networks, not connected to the Internet. In order to save cost and facilitate connectivity, they have evolved and adopted current technologies such as Ethernet, and TCP/IP protocols. Therefore, the implementation of new technologies in ICS devices and the interconnection with the corporate network has opened the way for threats that target IT infrastructures. Moreover, the majority of industrial software and protocols were designed without security in mind and do not typically require any authentication to remotely execute commands on their control interfaces. All these new features have facilitated attacks targeting SCADA as demonstrated by the attacks carried out in 2010 by high skilled groups against the Iranian nuclear program (Langer, 2011). Faced with these new cyber weapons, the need to equip with tools to detect them or identify their presence on equipment already in production is evident.

A typical SCADA system is illustrated in Figure 5 and consists of the following subcomponents:

- **Control Server / Master Terminal Unit (MTU)** which initiates all communications with field sites and receives the data sent from the field devices.
- **Engineering Station** which is used to write, test and load software.
- **Human–Machine Interface (HMI)** which interprets and presents the data in a graphical user interface to a human operator and thus enables the operator to monitor the process remotely and make operational decisions to maintain safety and efficiency.
- **Program Logic Controller (PLC) / Remote Terminal Units (RTU):** PLCs are installed locally to monitor and control the physical processes (e.g., pump, level sensor, valve*)* and collect information and send it to the MTU. For instance, in a gas pipeline, a PLC monitors and controls the gas pressure. It obtains the current pressure of the compressed gas in the pipe. If the pressure exceeds a certain threshold, it opens a solenoid valve to release some gas, which reduces the gas pressure in the pipe.

As shown by forensic analysis of the Stuxnet worm, infections have mainly targeted HMI, Engineering Station and PLC components.

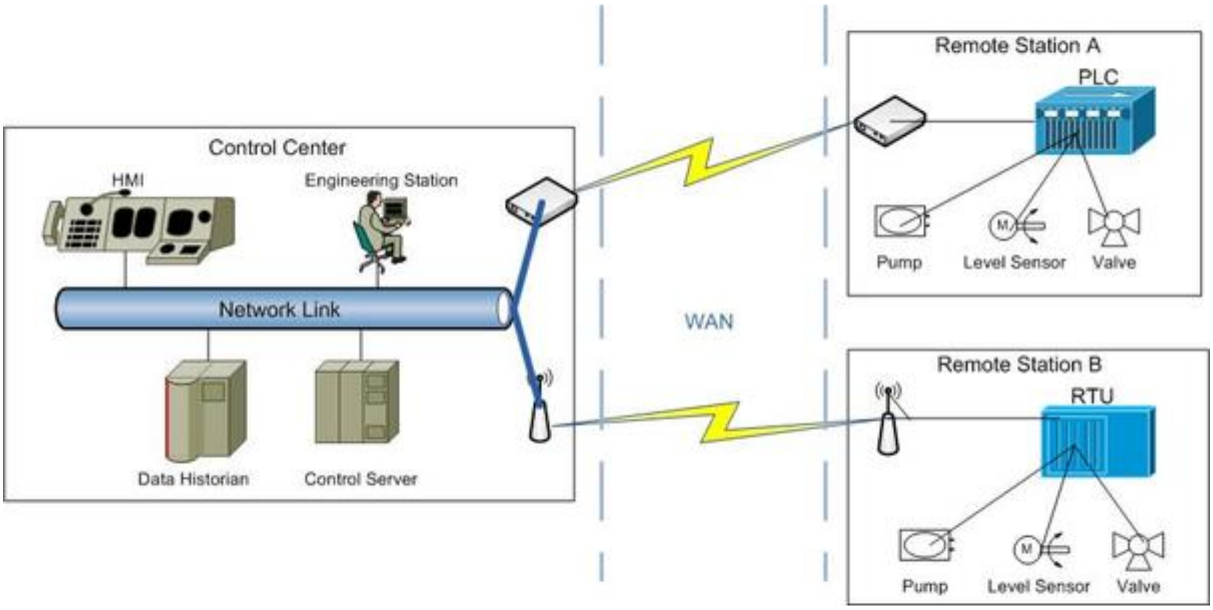

Figure 5: A typical SCADA Architecture in a simplified logical view

Mitigation:

There are several ways of tracing a compromise or collecting evidence and thus mitigating it.

- **Network:** Sensors installed at several strategic points in the network are able to analyse network traffic and decode industrial protocols. Coupled with artificial intelligence technology, it can be possible to detect an equipment alteration or abnormal behaviour.
- **Logs:** Each device is able to send backlogs (syslog for example). which must be stored in a SIEM. A detailed study of its logs can highlight an attempt to compromise or tamper SCADA equipments.
- **HMI & engineering workstations forensics:** Generally Windows, Unix and Linux systems are installed on these computers and therefore IT Forensic tools can be used. However it is important to

take into consideration that these devices are essential, they cannot be easily switched off, otherwise the system will become unstable. It is thus advisable to perform a live forensic by collecting important artifacts with a dedicated tool. A benchmark must first be performed on the spare machines to make sure it will not make production unstable..

- **PLC:** PLC is an industrial computer which has been ruggedised and adapted for the control of manufacturing processes. Most of PLCs run real-time OS such as the market leader "Vxworks".

Appropriate mitigation strategies can leverage on the following:

- Some real-time OS such as VxWorks is running on PLC and allows to perform RAM dumps, essentially for the benefit of support and diagnostic teams. Unfortunately, there is no dedicated analysis tool to dive into RAM dump and detect the presence of rootkit.
- Live memory of end-point device can also be dumped through Joint Test Access Group (JTAG) port. The extracted memory dump can be analysed offline without interrupting the SCADA system functionality.
- Network captures are used to check that the instructions sent by the HMI have not been altered.
- It is then necessary to download the PLC running program from a clean engineering workstation and compare it with the original program. The controller's logic (ladder logic), variables, and timers are critical artefacts in determining functional changes in a system.
- Finally the integrity of the firmware should be checked by comparing it with the original fingerprint.

Opportunities:

Digital forensics is still difficult to implement for industrial control systems. Currently, there is no standardised or well-documented strategy for collating data for SCADA systems to obtain evidence for criminal activities. Furthermore, research in the forensic domain often requires engaging SCADA device manufacturers, control centre operators, and other stakeholders in order to provide researchers with a view into the technical problems that arise in operation. However, the vital nature of most critical infrastructure organisations discourages industry staff from collaborating with the research community. Working jointly to create digital forensics tools and techniques is vital to counteract and detect the compromise of ICS / SCADA.

3.9 Vehicular systems

Vehicular Systems include aerial, ground and water transports of all kind, for people and goods, such as aircrafts, trains, metro, cars, buses, ships and submarines. Vehicular systems are highly interdependent with electrical power generation, transportation, telecommunication and satellite localisation and also generate and process large quantities of data, thus many data-driven services are available.

3.9.1 Detection of rogue or unauthorised autonomous systems

Developers shall be able to provide means to ensure that the agent has indeed been authorised to perform its tasks, that the confidentiality, integrity, and availability of data processed is preserved, depending on the operation and the context, that the agent cannot be tainted during its operation, and that its integrity is preserved and verifiable throughout its lifecycle.

Challenge:

The most severe situation that can happen to an autonomous vehicle is the total loss of control. It is assumed that complete loss of control is impossible if there is even a person physically present since they will be able to deactivate external control and take over control locally. Nevertheless, without anyone physically present such possibility is not available, and control may be lost completely or at least for some time. In theory, control may be reestablished by entering or boarding the vehicle, however this will take time, something that is not acceptable given how critical the situation may be.

It is, therefore, possible that an unmanned, autonomous ship that has been hacked may be used to ram into infrastructure systems. Even a small ship with a mass of 5,000 tons, travelling at a speed of 12 knots, has a kinetic energy of roughly around 200 MJ, which is excessive in relation to structural capabilities of most offshore structures; only the Condeep structures could be expected to survive. Larger ships will be a threat to all offshore structures.

Mitigation:

Traffic surveillance is one of the solutions adopted by the offshore oil and gas industry for protection of offshore installations against collision threats by passing vessels. For the Norwegian sector, there are several centers; two operated by offshore companies and several government-operated centers along the coast. The main principle is to detect a ship on collision course as early as possible, and thus to give the possibility to communicate with the ship and warn it to alter its course. If contact is not established, the approach implies to warn the installation early, such that safe evacuation of all personnel may be completed. In addition, available resources may be used to try to establish contact with the vessel if communication fails.

Safeguards need to be put in place to curtail broad discretionary autonomy, predict the behaviour of such systems and introduce specific limits and boundaries. Some operations should require explicit human authorisation that shall be given only by authenticated users. Another option would be to limit the operational area of an unmanned autonomous ship for instance by limiting the available fuel stored onboard. This is to some extent used for aircrafts, although the main approach in this case is to limit the weight the aircraft is carrying. But this would also be an option with some other risks. If the ship due to weather or other unforeseen events is significantly delayed, it could run out of fuel, if this is limited. If such risks are judged to be tolerable, however, it may provide an effective manner to avoid that hackers turn a ship into a threat to goals far away from the intended route. A battery powered ship will have such limitations in any case.

If the vehicle is completely unmanned, it is essential to avoid any vulnerabilities in the control and communication systems onboard that may be used in a cyber-attack to gain control. This implies that complete control over the construction, procurement, management, operation and maintenance of autonomous vehicles. At all times, no unauthorised organisations nor individuals should get the opportunity to install software or hardware which may provide a “backdoor” into the control system and software available to hackers.

Opportunities:

Behaviour-based anomaly detection could be employed to detect rogue or unauthorised autonomous systems by leveraging evidence from diverse sources, including visual inspection, but also information obtained from radars and other sources monitoring the trajectory of such vehicles. To this end, AI-based techniques could be exploited.

3.9.2 Interference

The provider shall design and pre-configure the delivered product such that functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations.

Challenge:

The challenge can be seen at different levels, from hardening of each single component (i.e., install and start only the OS services/modules needed on a specific computer) to the hardening of whole complex vehicular system. Depending on the complexity and variability of the operational scenarios, the hardening of vehicular systems may be non-trivial. Taking a naval ship as example, it may be used for patrolling and surveillance of international waters and suddendly be ordered to perform a rescue or an anti-piracy mission. These operational scenarios are different in the number and types of systems involved.

Mitigation:

While for the components, hardening is a well-established practice that shall be carried out during system configuration, the "system hardening" is way more complex and still needs to be optimised. Having baseline "mission profiles", with well tested, pre-configured, systems capabilities that are activated by an operator, allows to reduce the risk of misconfigurations leading to potential unsafe situations. Usually these tests are performed at functional level, often manually, with reduced coverage

Opportunities:

Development of an automated test methodology, based on modern software development techniques such as Test-Driven Development (TDD) or Behaviour-Driven Development (BDD) may allow to increase the coverage and ensure that the system works as expected.

3.9.3 Transparency and accountability

The manufacturer shall be able to offer comprehensive and understandable documentation about the overall design of the agent, describing its architecture, functionalities and protocols, their realisation in hardware or software components, the interfaces and interactions of components with each other and with internal and external services, in order to be able to implement and deploy the agent in the most secure way possible.

Challenge:

Manufacturers usually provide the minimum information needed by the owner to operate and maintain the system. Additional information is often subject to IPR protection and restrictions.

Mitigation:

The use of Common Criteria, for example, would increase the level of confidence that the delivered product has been developed and tested formally and that it will perform as required. ENISA has provided a European cybersecurity certification framework for ICT products while for OT products and systems it is possible to achieve the ISASecure certification for conformance to IEC 62443. To prevent successful cyberattacks to autonomous vehicles, it is crucial to maintain control and sufficient quality assurance over the whole software development process. This might become costly and reduce some of the expected cost savings related to autonomous vehicles. However, it is still the responsibility of designers and vehicle manufacturers to implement the very strict control outlined above.

Opportunities:

Blockchain properties of immutability can be applied to any data no matter what the content of the record. Each use case which necessitates connecting a user action to record or virtual transaction provides an instance of accountability. Capabilities offered by blockchain in many cases are still theoretical, however, the new approach outlined in (Gorog, 2018) begins to connect solutions with real-life use cases.

3.9.4 Unauthorised access to autonomous cars and unmanned vehicles

An attacker can gain control of an unmanned vehicle through the different connected sensors or hacking the network which controls it. IoT devices are open to vulnerabilities, many of which remain unpatched even today. Also, IoT devices are prone to install malicious Apps on top of IoT OS. From a maritime perspective, the most critical issue is represented by the communication channel.

Challenge:

Firmware and Application patch management for IoT devices is far from being as refined as other commercial software. Moreover, it has been demonstrated that even centralised patch management can be used for malicious purposes by injecting malicious code into a legitimate update. In the maritime sector, security patches and updates are previously tested in a demo environment and then deployed at defined intervals according to update & maintenance policies and contracts established between the shipbuilder or shipowner and the manufacturer. However, these activities can be performed by the manufacturer or an authorised service dealer, therefore shifting the security focus on the supply chain.

Mitigation:

Current approaches for software updates on unmanned vehicles focus on ensuring integrity and confidentiality but do not analyse the content of the software update. More generally, including the maritime domain, the systems shall perform integrity checks of software and firmware at startup, secure the development environment from hackers who can inject malicious software into legitimate builds and secure the supply chain to ensure that updates are properly deployed avoiding insider’s threats.

Opportunities:

An interesting approach is the development of an automated software analysis framework for systematically verifying the security of the applications contained in IoT software updates with regards to a given security policy (Dejon et al., 2019).

3.10 Summary

Overall, this section provided a detailed review of the identified inter-sector technical cybersecurity challenges, while the discussion on the potential opportunities indicated the need to develop solutions that are tailored to particular sectors, thus cybersecurity solutions should be developed in a customisable manner so that they can be adapted to particular sectors. Moreover, similar to the transversal challanegs, the opportunities that arise need to leverage a combination of advanced technology (including the latest advances in AI/ML technologies), clear processes, and qualified and informed people. 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.

4. Conclusions and next steps

This deliverable is the first version of the deliverables reporting on inter-sector technical cybersecurity challenges and will be validated, updated, and revised in D4.9. 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.