

C&ESAR'23: Cybersecurity of Smart Peripheral Devices – Mobiles / IoT / Edge (Preface)

C&ESAR'2: Cybersécurité des équipements périphériques intelligents – Mobiles / IoT / Edge (Préface)

Gurvan Le Guernic^{1,2}

¹ DGA Maîtrise de l'Information, Rennes, France

² Univ Rennes, Inria, CNRS, IRISA, Rennes, France

Abstract

C&ESAR is an educational, professional and scientific conference on cybersecurity whose specific topic changes every year. This year C&ESAR is focused the cybersecurity of “Smart Peripheral Devices”, i.e. mobiles, IoT and Edge devices. The scope covers all issues related to the cybersecurity of semi-autonomous connected devices deployed at the periphery of an information system close to its data sources and sinks. Those devices include mobiles, smartphones, IoT devices, and lightweight Edge devices. Those devices often have less computation power than devices in the core of an IT or OT network, and are more exposed to external threats. Hence, attacking or securing them may require different means than for attacking or securing the core of an IT or OT network. C&ESAR 2023 received 18 submissions for peer-review. Out of these, 9 papers were accepted for presentation at the conference. After the conference, 4 were short listed for inclusion in this volume.

Keywords

Cybersecurity, Mobile, IoT, Android, C&ESAR, Conference, Preface

Résumé


C&ESAR est une conférence pédagogique, professionnelle et scientifique sur la cybersécurité dont le thème spécifique change chaque année. Cette année, C&ESAR se concentre sur la cybersécurité des « appareils périphériques intelligents », c'est-à-dire les appareils mobiles, IoT et Edge. Le périmètre couvre toutes les problématiques liées à la cybersécurité des objets connectés semi-autonomes déployés en périphérie d'un système d'information à proximité des producteurs et consommateurs de données. Ces équipements incluent les appareils mobiles, les smartphones, les appareils IoT et les appareils Edge légers. Ces équipements ont souvent moins de puissance de calcul que les appareils situés dans le cœur d'un réseau informatique ou OT, et sont plus exposés aux menaces externes. Ainsi, les attaquer ou les sécuriser peut nécessiter des moyens différents de ceux pour attaquer ou sécuriser le cœur d'un réseau IT ou OT. C&ESAR 2023 a reçu 18 soumissions pour examen par les pairs. Parmi ceux-ci, 9 articles ont été acceptés pour présentation à la conférence, dont 4 pour inclusion dans les actes.

C&ESAR'23: Computer & Electronics Security Application Rendezvous, Nov. 21-22, 2023, Rennes, France

✉ gurvan.le_guernic@inria.fr (G. Le Guernic)

🆔 0000-0003-0387-9738 (G. Le Guernic)

© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

1. C&ESAR

Every year since 1997, the French Ministry of Defense organizes a cybersecurity conference, called C&ESAR. This conference is now one of the main events of the European Cyber Week (ECW) organized every fall in Rennes, Brittany, France.

The goal of C&ESAR is to bring together governmental, industrial, and academic stakeholders interested in cybersecurity. This event, both educational and scientific, gathers experts, researchers, practitioners and decision-makers. This inter-disciplinary approach allows operational practitioners to learn about and anticipate future technological inflection points, and for industry and academia to confront research and product development to operational realities. Every year, C&ESAR explores a different topic within the field of cybersecurity.

This year's topic is: *Cybersecurity of Smart Peripheral Devices (Mobiles / IoT / Edge)*. This topic is subtitled: Cybersecurity of semi-autonomous connected devices deployed at the periphery of an information system, close to its data sources and sinks.

2. Cybersecurity of Smart Peripheral Devices (Mobiles / IoT / Edge)

There is a trend to move more and more information processing towards the edges of information systems, close to the data sources and sinks, and to the end-users [1]. In 2018, Gartner evaluated that 10% of “enterprise-generated data is created and processed outside a traditional centralized data center or cloud” [2], and predicted in 2021 that this number would increase to 50% in 2025 [3] (which it originally predicted at 75% in its 2018 report [2]) while the number of IoT devices will triple [3] or quadruple [4] between 2020 and 2030 reaching “more than 15 billion IoT devices [that] will connect to the enterprise infrastructure by 2029” [4] (IoT analytics even forecasts 27 billions connected IoT devices by 2025 [5]). There are varying reasons for this trend, among which: improving latency, relieving the network bandwidth from part of the huge amount of data generated, and bringing some autonomy to the end-users interacting at the periphery of the information system. This trend exists in the civil world, and in particular in industry with the specific concept of Industrial IoT (IIoT) [6, 7, 8, 9], but also in the military one with the concepts of the Internet of Battle Things (IoBT) [10, 11, 12] or Internet of Military Things (IoMT) [13, 14], which aim in part to increase local information exploitation [15, 16, 17]. To develop those concepts in the military domain, among other initiatives, the Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA) [18, 19, 20] was established in 2017 for a 10 years period.

In this call, devices handling those peripheral computations are called **Smart Peripheral Devices** (SPDs). Those SPDs are quite different from, and have more variability, than devices found in the “core” of information systems (servers, desktops and laptops). They range: from somewhat expensive and powerful devices, such as **smartphones** or communication equipment of military vehicles [17]; to low cost low power devices, such as

disposable **wearable devices** or disposable vessels [21, 22]; through **Internet of Things (IoT)** devices [23], and some lightweight **Edge Computing** devices [24]. While quite different, SPDs share some characteristics: they reside at the periphery of the system and are more susceptible to loss and theft; they have to comply with specific constraints limiting the resources they can use; they run on specific hardware usually not found in “core” devices; they use connection technologies not found in the core of the system to communicate with the core and between themselves; they handle some information processing directly, independently from the core of the system; they have to allow for “temporary” disconnections from the core, while still being able to function properly; and they are not continuously visible and monitored by the core of the information system.

Those specifics raise some concerns over their resilience to cybersecurity attacks [25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36], and even the faithfulness of their supply chain [37]. As stated by Verizon for IoT [38], but applying to all SPD, “an [SPD] can be an attack vector (a weak point that can be exploited to mount an attack), a vehicle for attacks (like a part of a botnet used to carry out a distributed denial-of-service (DDoS) attack) or a target in its own right”. For example, the Mirai botnet [39] infected many IoT devices and has been used to attack many other systems. Mobiles are also an interesting target for attackers [40, 41, 42, 43]. Over a one year period, half of companies recently surveyed by Verizon suffered a compromise involving a mobile device [38]; for half of the companies concerned, applications were involved (in 2021, the percentage of organizations experiencing the installation of a malware on a remote device doubled [44]); and half of SMBs that suffered a mobile-related hack said that it had a major impact. Attackers do design applications and phishing campaigns specifically for mobiles [38], and if they do its because there is a benefit in doing so. As a consequence, more than 8 companies out of 10 have a specific budget for mobile security [38]. Last year C&ESAR addressed the concept of Zero Trust, among others. From the point of view of the security of the core of the information system, an SPD can be disconnected if the core has lost trust in it. However, the features carried by this SPD will also be lost. It is therefore important to be able to secure those SPDs.

However, cybersecurity technologies and methodologies applied to the core of information systems are not necessarily directly applicable to SPDs. Adapting standard Endpoint Detection and Response (EDR) solutions to the vast variety of SPD and integrating them to the core IT system SIEM is not a simple task. The specific technologies used for SPDs may contain weaknesses and vulnerabilities different from those of core system technologies [45, 46]. Ensuring the cybersecurity of SPDs may also require specific methodologies [47].

For example, SPDs use specific technologies in their processing stack (hardware and software). Among the various hardware used, they rely more commonly on ARM platforms and technologies. Those hardwares and deployment environment have specific characteristics impacting their cybersecurity [48, 49]. Among the various hardware support for securing SPDs [50], we can cite Secure Elements (SE) [51] or Tusted Execution Element (TEE). SPDs also use specific operating systems, such as Android and iOS for smartphones [52, 53]. And, for some of them, they allow end-users (hopefully the device administrator) to pull computing payloads from application stores populated

by softwares coming from various, sometimes obscure, sources. The low confidence in the cybersecurity level of those application stores has pushed some institutions such as Google to launch initiatives to improve the state of affairs [54] or to launch projects aiming at standardizing the cybersecurity requirements for those applications [55, 56]. This state of affairs with regard to the low cybersecurity level of mobile applications pushes for much need improvements [57].

SPDs also use different technologies to connect to the core of the information system and to connect between themselves. One promising technology is the 5G one [58, 59, 60, 5, 61], and 6G in the future [62, 63]. However, this technology, as well as the others, have raised cybersecurity concerns among researchers [64], institutions [65, 66, 67, 68, 69, 70, 71, 72] and industry [73, 74]. For example, even the specification of Bluetooth contains vulnerabilities [75, 76, 77]. The deployment environment and ability of SPDs to create device-to-device connections result in networks, such as ad hoc or mesh ones, having different shapes and behaving differently than core information system networks, and having specific cybersecurity concerns.

To secure communications in those networks, SPDs can rely on cryptography. However, the low level of infrastructure support some of them receive and low computation power some of them have may require some specific cryptographic solutions, such as lightweight cryptography [78] or specific key agreement protocols [79].

Another challenge that comes with SPDs is their deployment “far away” from the core of the information system, and with an intermittent connection to it. This setting prevents the implementation of security policies centered around the core of the information system. SPDs require specific security policies that require specific means for deployment, management and enforcement. Those means need to be secured in their own right in order to prevent attackers from exploiting them to take control of the managed SPDs.

Finally, the peripheral deployment of SPDs, their proximity to information sources, and their common reliance on information collection imply concerns over privacy and data protection issues [80, 81, 82, 83]. As a consequence, policymakers have published specific and generic laws and regulations that apply to SPDs [84, 85, 86, 87, 88, 89, 90, 91].

3. Solicited Papers

In this context, C&ESAR solicited submissions presenting **didactic surveys, innovative solutions, or insightful experience reports** on the subject “Cybersecurity of Smart Peripheral Devices (Mobiles / IoT / Edge)”.

The scope covered:

- all steps of cybersecurity, from system design to operational cyberdefense or pen-testing, including DevSecOps loops and disposal/retirement of equipment and systems;
- all types of systems and devices related to Smart Peripheral Devices (SPDs): mobiles (including smartphones), IoT and lightweight semi-autonomous Edge computing.

The topics included (without being limited to them, and in relation to cybersecurity and SPDs) those mentioned above and below:

- Wireless connectivity technologies (5G/6G, Bluetooth, Zigbee, Z-Wave, LoRa, NB-IoT, Cat M1, Starlink, ...)
- Peripheral network protocols (ad hoc networks, mesh routing protocols, 5G network protocols, ...)
- Cryptography (lightweight cryptography, multi-party key agreement with little infrastructure support, 5G cryptography, ...)
- Hardware support (ARM, Trusted Execution Environment, Secure Element, ...)
- Lightweight security mechanisms
- Smartphones OS (iOS/Android) and other lightweight OS
- Supply chain, including application stores
- Attack surface of SPDs (Mobiles, IoT, Edge)
- Forensic of SPDs (Mobiles, IoT, Edge)
- Malware and phishing specifics relating to SPDs (Mobiles, IoT, Edge)
- Security policies and their management
- Privacy and data protection
- Laws and regulations
- Domain specific issues (Industrial IoT, UAV, health devices, autonomous vehicles, ...)

The topic also covered all the following keywords applied in the context of peripheral devices: Cybersecurity, Mobiles, Smartphone, Internet of Things (IoT), Edge Computing, Internet of Battle Things (IoBT), Internet of Military Things (IoMT), Android, iOS, 5G, 6G, LoRa, StarLink, (Lightweight) Cryptography, Mobile Ad Hoc Network (MANET), Device to Device (D2D) Connections, Malwares, AppStore, Forensic, Trusted Execution Environment (TEE), Secure Element (SE), Security Policies, Law, Regulation.

4. Review Process

C&ESAR received 18 submissions. Among those, 12 proposals have been selected for the final round of reviews (67% pre-selection rate). Out of those pre-selected proposals, 12 final versions were submitted; out of which, 9 have been selected for presentation at the conference (a 75% acceptance rate for the final round of reviews, and a 50% overall acceptance rate for the conference). Finally, 4 of the presented papers have been selected for inclusion in the proceedings (an overall acceptance rate of 22% for the proceedings).

5. Program Committee

This peer review has been made possible thanks to the dedication of the members of the following program committee:

- Erwan ABGRALL
- José ARAUJO, Orange Cyberdéfense
- Christophe BIDAN, CentraleSupélec

- Frédéric CUPPENS, Polytechnique Montréal
- Herve DEBAR, Télécom SudParis
- Ivan FONTARENSKY, Thales
- Jacques FOURNIER, CEA
- Julien FRANCO, Naval Group
- Brittia GUIRIEC, DGA MI
- Gurvan LE GUERNIC, DGA MI & Université de Rennes
- Frédéric MAJORCZYK, DGA MI & CentraleSupélec
- Guillaume MEIER, Airbus R&D
- Laurence OGOR, DGA MI
- Marc-Oliver PAHL, IMT Atlantique & Chaire Cyber CNI
- Yves-Alexis PEREZ, ANSSI
- Ludovic PIETRE-CAMBACEDES, EDF
- Louis RILLING, DGA MI
- Eric WIATROWSKI
- Olivier ZENDRA, Inria

References

- [1] European Commission, Europe's Internet of Things Policy, Webpage, European Commission, 2022. URL: <https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy>.
- [2] R. van der Meulen, What Edge Computing Means for Infrastructure and Operations Leaders, Article, Gartner, Inc., 2018. URL: <https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders>.
- [3] A. Neff, Predicts 2022: The Distributed Enterprise Drives Computing to the Edge, Technical Report, Gartner, Inc., 2021.
- [4] K. Costello, Gartner Predicts the Future of Cloud and Edge Infrastructure, Article, Gartner, Inc., 2021. URL: <https://www.gartner.com/smarterwithgartner/gartner-predicts-the-future-of-cloud-and-edge-infrastructure>.
- [5] M. Hasan, State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally, Blog post, IoT Analytics GmbH, 2022. URL: <https://iot-analytics.com/number-connected-iot-devices/>.
- [6] Wikipedia contributors, Industrial internet of things — Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Industrial_internet_of_things, 2023. [Online; accessed 6-January-2023].
- [7] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial Internet of Things: Challenges, Opportunities, and Directions, *IEEE Transactions on Industrial Informatics* 14 (2018) 4724–4734. doi:10.1109/TII.2018.2852491.
- [8] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, D. Pelusi, U. Ghosh, J. Nayak, Industrial Internet of Things and

- its Applications in Industry 4.0: State of The Art, *Computer Communications* 166 (2021) 125–139. URL: <https://www.sciencedirect.com/science/article/pii/S0140366420319964>. doi:10.1016/j.comcom.2020.11.016.
- [9] M. Serror, S. Hack, M. Henze, M. Schuba, K. Wehrle, Challenges and Opportunities in Securing the Industrial Internet of Things, *IEEE Transactions on Industrial Informatics* 17 (2021) 2985–2996. doi:10.1109/TII.2020.3023507.
- [10] A. Kott, A. Swami, B. West, The Internet of Battle Things, *Computer* 49 (2017) 70–75. doi:10.1109/MC.2018.2876048.
- [11] S. Russell, T. Abdelzاهر, The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making, in: *Proc. IEEE Military Communications Conference (MilCom)*, 2018, pp. 737–742. doi:10.1109/MILCOM.2018.8599853.
- [12] T. Abdelzاهر, N. Ayanian, T. Basar, S. Diggavi, J. Diesner, D. Ganesan, R. Govindan, S. Jha, T. Lepoint, B. Marlin, K. Nahrstedt, D. Nicol, R. Rajkumar, S. Russell, S. Seshia, F. Sha, P. Shenoy, M. Srivastava, G. Sukhatme, A. Swami, P. Tabuada, D. Towsley, N. Vaidya, V. Veeravalli, Toward an Internet of Battlefield Things: A Resilience Perspective, *Computer* 51 (2018) 24–36. URL: <https://doi.org/10.1109/MC.2018.2876048>. doi:10.1109/MC.2018.2876048.
- [13] Wikipedia contributors, Internet of Military Things — Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Internet_of_Military_Things&oldid=1130011550, 2022. [Online; accessed 6-January-2023].
- [14] L. Cameron, Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT, *IEEE Computer Society* (2018).
- [15] M. Pesqueur, L'aïlier de demain : le partenariat homme-machine dans l'armée de Terre, Notes de l'Ifri, Ifri, 2021. URL: https://www.ifri.org/sites/default/files/atoms/files/pesqueur_partenariat_homme_machine_2021.pdf.
- [16] Ministère des Armées, SICS (Système d'information du combat de SCORPION), Webpage, Ministère des Armées, 2022. URL: <https://www.defense.gouv.fr/eurosatory/poles-thematiques/scorpion/connectivite/sics-systeme-dinformation-du-combat-scorpion>.
- [17] Ministère des Armées, The SCORPION programme, Webpage, Ministère des Armées, 2022. URL: <https://www.defense.gouv.fr/eurosatory/the-scorpion-programme>.
- [18] Office of Strategic Communications, Internet of Battlefield Things (IoBT) CRA, Website, U.S. Army DEVCOM Army Research Laboratory, 2023. URL: <https://www.arl.army.mil/cras/iobt-cra/>.
- [19] T. Abdelzاهر, Alliance for IoBT Research on Evolving Intelligent Goal-driven Networks (IoBT REIGN), Website, University of Illinois at Urbana-Champaign, 2022. URL: <https://iobt.illinois.edu/>.
- [20] Wikipedia contributors, IoBT-CRA — Wikipedia, The Free Encyclopedia, <https://en.wikipedia.org/wiki/IoBT-CRA>, 2022.
- [21] MeriTalk Staff, DARPA Floats a Proposal for the Ocean of Things, MeriTalk (2018). URL: <https://www.meritalk.com/articles/darpa-floats-a-proposal-for-the-ocean-of-things/>.

- [22] DARPA Staff, Ocean of Things Aims to Expand Maritime Awareness across Open Seas, Technical Report, DARPA, 2017. URL: <https://www.darpa.mil/news-events/2017-12-06>.
- [23] Wikipedia contributors, Internet of things — Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Internet_of_things&oldid=1128546461, 2022. [Online; accessed 6-January-2023].
- [24] Wikipedia contributors, Edge computing — Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Edge_computing&oldid=1127185952, 2022. [Online; accessed 6-January-2023].
- [25] Check Point, Mobile Security Report 2021, Technical Report, Check Point Software Technologies Ltd., 2021. URL: <https://resources.checkpoint.com/cyber-security-resources/mobile-security-report-2021>.
- [26] Check Point, Mobile Security Trends in 2022, Blog Post, Check Point Software Technologies Ltd., 2022. URL: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-security/mobile-security-trends-in-2022/>.
- [27] M. b. Mohamad Noor, W. H. Hassan, Current research on Internet of Things (IoT) security: A survey, *Computer Networks* 148 (2019) 283–294. URL: <https://www.sciencedirect.com/science/article/pii/S1389128618307035>. doi:10.1016/j.comnet.2018.11.025.
- [28] H. Awan, Mobile Security Threats Prediction for 2023, Technical Report, efani, 2022. URL: <https://www.efani.com/blog/mobile-threats-prediction-2023>.
- [29] G. Rowlands, The Internet of Military Things & Machine Intelligence: A Winning Edge or Security Nightmare?, Technical Report, III, 2017.
- [30] P. S. Bangare, K. P. Patil, Security Issues and Challenges in Internet of Things (IOT) System, in: *Proc. Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2022, pp. 91–94. doi:10.1109/ICACITE53722.2022.9823709.
- [31] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, A. Refoufi, A Review of Security in Internet of Things, *Wireless Personal Communications* 108 (2019) 325–344. URL: <https://doi.org/10.1007/s11277-019-06405-y>. doi:10.1007/s11277-019-06405-y.
- [32] B. Liao, Y. Ali, S. Nazir, L. He, H. U. Khan, Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review, *IEEE Access* 8 (2020) 120331–120350. doi:10.1109/ACCESS.2020.3006358.
- [33] P. Delgado-Santos, G. Stragapede, R. Tolosana, R. Guest, F. Deravi, R. Vera-Rodriguez, A Survey of Privacy Vulnerabilities of Mobile Device Sensors, *ACM Computing Surveys* 54 (2022) 1–30. doi:10.1145/3510579.
- [34] Y. Mekdad, A. Aris, L. Babun, A. E. Fergougui, M. Conti, R. Lazzeretti, A. S. Uluagac, A Survey on Security and Privacy Issues of UAVs, 2021. URL: <https://arxiv.org/abs/2109.14442>. doi:10.48550/ARXIV.2109.14442.
- [35] M. Aqeel, F. Ali, M. w. Iqbal, T. Rana, M. Arif, M. Auwul, A Review of Security and Privacy Concerns in the Internet of Things (IoT), *Journal of Sensors* 2022 (2022) 1–20. doi:10.1155/2022/5724168.
- [36] S. Sendhil, The security impact of IoT on business transformation, *Insights, ManageEngine*, 2023. URL: <https://insights.manageengine.com/digital-transformation/the-security-impact-of-iot-on-business-transformation/>.

-
- [37] C. Parton, Chinese Cellular IoT technology: An analysis of threats and mitigation measures, White paper, OODA LLC, 2023. URL: <https://www.oodaloop.com/globalrisk/2023/01/23/chinese-cellular-iot-technology-an-analysis-of-threats-and-mitigation-measures/>, full report "Cellular IoT modules – Supply Chain Security" available at https://www.oodaloop.com/wp-content/uploads/2023/01/Cellular_IoT_Paper_JAN_Master_PDF.pdf.
- [38] Verizon, Verizon 2022 Mobile Security Index, Technical Report, Verizon, 2022.
- [39] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, et al., Understanding the Mirai Botnet, in: Proc. USENIX security symposium, 2017, pp. 1093–1110. URL: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>.
- [40] Pradeo, Mobile security predictions for 2022, Blog post, Pradeo, 2022. URL: <https://blog.pradeo.com/pradeos-predictions-2022>.
- [41] Wikipedia contributors, Mobile security — Wikipedia, The Free Encyclopedia, 2022. URL: https://en.wikipedia.org/w/index.php?title=Mobile_security&oldid=1127644660, [Online; accessed 6-January-2023].
- [42] C. Brown, S. Dog, J. M. Franklin, N. McNab, S. Voss-Northrop, M. Peck, B. Stidham, Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue, NIST Interagency Report 8144, National Institute of Standards and Technology (NIST), 2016. Draft.
- [43] NIST, Mobile Threat Catalogue, Website, NIST, 2023. URL: <https://pages.nist.gov/mobile-threat-catalogue/>.
- [44] Jamf, Security 360 Annual Trends Report, Technical Report, Jamf, 2022.
- [45] P. Weichbroth, L. Łysik, Mobile Security: Threats and Best Practices, Mobile Information Systems 2020 (2020). doi:10.1155/2020/8828078.
- [46] A. Qamar, A. Karim, V. Chang, Mobile malware attacks: Review, taxonomy & future directions, Future Generation Computer Systems 97 (2019) 887–909. doi:10.1016/j.future.2019.03.007.
- [47] B. Liao, Y. Ali, S. Nazir, L. He, H. U. Khan, Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review, IEEE Access 8 (2020) 120331–120350. doi:10.1109/ACCESS.2020.3006358.
- [48] Arrow, Hardware Security for IoT Devices and Types of Hardware Security Attacks, Technical article, Arrow, 2020. URL: <https://www.arrow.com/en/research-and-events/articles/understanding-the-importance-of-hardware-security>.
- [49] M. K. Pratt, Bolster physical defenses with IoT hardware security, News article, TechTarget, 2021. URL: <https://www.techtarget.com/iotagenda/tip/Bolster-physical-defenses-with-IoT-hardware-security>.
- [50] W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, H. Li, An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 40 (2021) 1010–1038. doi:10.1109/TCAD.2020.3047976.
- [51] E. Bernard-Moulin, Protect your IoT device with hardware-based Secure Ele-

- ments, Blog post, IC'ALPS, 2021. URL: https://www.icalps.com/news/blog_post/embedded-security-iot/.
- [52] M. Zinkus, T. M. Jois, M. Green, Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions, 2021. URL: <https://arxiv.org/abs/2105.12613>. doi:10.48550/ARXIV.2105.12613.
- [53] S. Garg, N. Baliyan, Comparative analysis of Android and iOS from security viewpoint, *Computer Science Review* 40 (2021) 100372. doi:10.1016/j.cosrev.2021.100372.
- [54] Google, App Defense Alliance, 2023. URL: <https://appdefensealliance.dev>, [Online; accessed 4-January-2023].
- [55] B. Mueller, S. Schleier, J. Willemsen, C. Holguera, OWASP Mobile Application Security Verification Standard (MASVS), Technical Report, Open Web Application Security Project (OWASP), 2022. URL: <https://mas.owasp.org/>, version 1.4.2.
- [56] ioXt Alliance, The Global Standard for IoT Security, Online, 2023. URL: <https://www.ioxtalliance.org/>, [Online; accessed 4-January-2023].
- [57] Build38, Mobile application security trends for 2023, Blog post, Build38, 2022. URL: <https://build38.com/trends-app-protection-2023/>.
- [58] R. Khan, P. Kumar, D. N. K. Jayakody, M. Liyanage, A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions, *IEEE Communications Surveys & Tutorials* 22 (2020) 196–248. doi:10.1109/COMST.2019.2933899.
- [59] H. Attar, H. Issa, J. Ababneh, M. Abbasi, A. A. A. Solyman, M. Khosravi, R. Said Agieb, 5G System Overview for Ongoing Smart Applications: Structure, Requirements, and Specifications, *Computational Intelligence and Neuroscience* (2022) 1–11. doi:10.1155/2022/2476841.
- [60] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, M. Yi, Overview of 5G security technology, *Science China: Information Sciences* 61 (2018). doi:10.1007/s11432-017-9426-4.
- [61] X. Huang, T. Yoshizawa, S. B. M. Baskaran, Authentication Mechanisms in the 5G System, *Journal of ICT Standardization* 9 (2021) 61–78. doi:10.13052/jicts2245-800X.921.
- [62] S. Dang, O. Amin, B. Shihada, M.-S. Alouini, What should 6G be?, *Nature Electronics* 3 (2020) 20–29.
- [63] C. D. Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, M. Liyanage, Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research, *IEEE Open Journal of the Communications Society* 2 (2021) 836–886. doi:10.1109/OJCOMS.2021.3071496.
- [64] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, V. Stettler, A Formal Analysis of 5G Authentication, in: *Proc. Computer and Communications Security (CCS)*, 2018, pp. 1383–1396. doi:10.1145/3243734.3243846.
- [65] CISA, 5G Security and Resilience, Website, Cybersecurity and Infrastructure Security Agency (CISA), 2023. URL: <https://www.cisa.gov/5g>.
- [66] Enduring Security Framework (ESF) working group, Potential Threat Vectors to 5G Infrastructure, Technical Report, National Security Agency (NSA), the Cybersecurity

- and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI), 2021. URL: <https://www.cisa.gov/5g-library>.
- [67] Enduring Security Framework (ESF) working group, ESF Potential Threats to 5G Network Slicing, Guidance, National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI), 2022. URL: <https://www.cisa.gov/5g-library>.
- [68] MITRE, the Department of Defense (DoD), FiGHT™ (5G Hierarchy of Threats), Knowledge Base, MITRE and the Department of Defense (DoD), 2022. URL: <https://fight.mitre.org/>.
- [69] MITRE, MITRE and the Office of the Under Secretary of Defense Announce FiGHT™ Framework to Protect 5G Ecosystem, Press Release, MITRE and the Department of Defense (DoD), 2022.
- [70] European Commission, Member States publish a report on EU coordinated risk assessment of 5G networks security, Press release, European Union (EU), 2019. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.
- [71] NIS Cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks, Technical Report, European Union (EU), 2019. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.
- [72] V. Oeselg, R. Šalaševičius, H. Ploom, A. Palm, Military Movement: Risks from 5G Networks, Research Report, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2022.
- [73] NIST, 5G Cybersecurity: Volume B: Approach, Architecture, and Security Characteristics, Special Report (SP) 1800-33B, NIST, 2022. URL: <https://www.nccoe.nist.gov/5g-cybersecurity>, preliminary Draft.
- [74] D. Hutchins, Making the Move to 5G, Playbook, Government Business Council (GBC), 2022. URL: <https://www.verizon.com/business/resources/reports/making-the-move-to-5g.pdf>, underwritten by Verizon Communications Inc.
- [75] CERT-FR, Multiples vulnérabilités dans Bluetooth Core Specification, Avis du CERT-FR CERTFR-2022-AVI-1107, ANSSI, 2022. URL: <https://www.cert.ssi.gouv.fr/avis/CERTFR-2022-AVI-1107/>.
- [76] Bluetooth SIG, Inc., Bluetooth SIG Statement Regarding the “Pairing Mode Confusion in BR/EDR” Vulnerability, Technical Report, Bluetooth SIG, Inc., 2022. URL: <https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/confusion-in-br-edr/>.
- [77] Bluetooth SIG, Inc., Bluetooth SIG Statement Regarding the “Pairing Mode Confusion in BLE Passkey Entry” Vulnerability, Technical Report, Bluetooth SIG, Inc., 2022. URL: <https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/confusion-in-ble-passkey/>.
- [78] S. Ganiev, Z. Khudoykulov, Lightweight Cryptography Algorithms for IoT Devices: Open issues and challenges, in: Proc. Information Science and Communications Technologies (ICISCT), 2021, pp. 01–04. doi:10.1109/ICISCT52966.2021.9670281.
- [79] M. Miettinen, N. Asokan, Ad-hoc key agreement: A brief history and the challenges ahead, Computer Communications 131 (2018) 32–34. URL: <https://www.sciencedirect.com/science/article/pii/S0140366418302007>. doi:10.1016/j.

- comcom.2018.07.030, cOMCOM 40 years.
- [80] FTC Staff, FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks, Press Release, Federal Trade Commission (FTC), 2015. URL: <https://www.ftc.gov/news-events/news/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices-address-consumer-privacy-security>.
 - [81] A. Karale, The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws, *Internet of Things* 15 (2021) 100420. doi:10.1016/j.iot.2021.100420.
 - [82] K. Kollnig, R. Binns, M. Van Kleek, U. Lyngs, J. Zhao, C. Tinsman, N. Shadbolt, Before and after GDPR: Tracking in Mobile Apps, *Internet Policy Review* 10 (2021). doi:10.14763/2021.4.1611.
 - [83] T. Klosowski, How Mobile Phones Became a Privacy Battleground—and How to Protect Yourself, *The New York Times: Wirecutter* (2022). URL: <https://www.nytimes.com/wirecutter/blog/protect-your-privacy-in-mobile-phones/>.
 - [84] M. Nelson, Understanding Global IoT Security Regulations, Blog Post, *Security Boulevard*, 2021. URL: <https://securityboulevard.com/2021/06/understanding-global-iot-security-regulations/>.
 - [85] Thales, IoT Cybersecurity: regulating the Internet of Things, Webpage, Thales, 2021. URL: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations>.
 - [86] P. Nolan, The 'Internet of Things': Legal Challenges in an Ultra-connected World, *Insights: Privacy & Data Security*, 2016. URL: <http://www.mhc.ie/latest/blog/the-internet-of-things-legal-challenges-in-an-ultra-connected-world>.
 - [87] I. Brown, Regulation and the Internet of Things, *Oxford Internet Institute*, 2015. URL: https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf.
 - [88] California Senate, California Senate Bill No. 327, Technical Report, California Senate, 2018. Référence 209 dans la page wikipedia sur IoT.
 - [89] Office of the Privacy Commissioner of Canada, Privacy guidance for manufacturers of Internet of Things devices, Guidance, Office of the Privacy Commissioner of Canada, 2020. URL: https://www.priv.gc.ca/en/privacy-topics/technology/gd_iot_man/.
 - [90] ETSI, Cyber Security for Consumer Internet of Things: Baseline Requirements, European Standard EN 303 645, ETSI, 2020. URL: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf, version 2.1.1.
 - [91] ETSI, Guide to Cyber Security for Consumer Internet of Things, Technical Report 103 621, ETSI, 2022. URL: https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf, version 1.2.1.