EUROPEAN CYBER SECURITY ORGANISATION

European Cyber Security Organisation

ECSO Technical Paper on Internet of Things (IoT)

July 2022 – v1.0

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) is a non-for-profit organisation, established in 2016. ECSO gathers more than 270 direct Members, including large companies, SMEs and start-ups, research centres, universities, end-users, operators, associations and national administrations. ECSO works with its Members and Partners to develop a competitive European cybersecurity ecosystem providing trusted cybersecurity solutions and advancing Europe's cybersecurity posture and its technological independence. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please contact wg6_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

Executive summary

The Internet of Things (IoTs) ecosystem is evolving very fast due to the wide adoption of IoT devices in different domains, driving the need to progress towards a more secure IoT landscape. In the wake of this IoT adoption trend, several challenges arise that need to be properly addressed to guarantee that all the potential behind IoT becomes a reality. The efforts are not only linked to the technical development, but many other dimensions should be addressed by involving multiple actors. The lack of trust in IoT appears as one of the most important roadblocks preventing a massive IoT take-up by consumers in the EU, industries and critical infrastructure managers. In parallel, European regulators are also concerned about the pervasiveness of IoT in the future. Cybersecurity attacks are indeed expected to have large impacts on all sectors, from home appliances, smart cities (mobility, pollution, waste and, sustainability), connected or autonomous cars, planes, smart farming or smart water.

The scope of this technical paper is to identify current and foreseen challenges related to IoT cybersecurity at technical level (both from the IoT supply point of view and the IoT adopters' point of view), at regulatory level, and in relation to certification.

This document analyses several IoT technical challenges and the vertical domains cyber-security challenges. This document also reviews the current state of the concept and approaches towards cybersecurity certification and analyses the current implications of legislations and regulations. Finally, a set of recommendations are proposed as a basis for further discussions.

Table of Contents

1. Introduction

The Internet of Things (IoT) is a central element in the global digitalisation trend that is reaching our industry, economy, and society. The adoption of IoT devices and applications entails benefits in the form of improved efficiency, safety or flexibility that will translate into desired outcomes such as economic growth, regulatory compliance, personal safety, or wellbeing, among others. The foreseen massive adoption of IoT will have a large transformational impact in our infrastructures, industrial production (across all verticals), and consumer market. Furthermore, IoT enables new collaborative *as-a-service* business models that, when fully developed, will extend its impact beyond what other technological revolutions have impacted before.

In the wake of this IoT adoption trend, several challenges arise that need to be properly addressed to guarantee that all the potential behind IoT becomes a reality. On a purely technological perspective, IoT security concerns are probably one of the key open challenges, if not the most important.

Europe and its industry are taking positions in the IoT market, both on the IoT supply side (as global provider of IoT technologies and services) and on the IoT demand side (as adopters of IoT in their processes, products, and services). However, the lack of trust in IoT appears as one of the most important roadblocks preventing a massive IoT take-up by EU's consumers, industries, and critical infrastructure managers.

In parallel, European regulators are also concerned about the pervasiveness of IoT in the future and the need to address cybersecurity challenges to ensure trust of consumers in emerging technologies and protect critical infrastructures. The EU's Cybersecurity Strategy for the Digital Decade[1] paves the way for a more comprehensive approach towards an internet of Secure Things to ensure overall resilience and improve the cybersecurity of all connected products and associated services placed on the Internal Market. The study "Liability for emerging digital technologies"[2] provides a first mapping of liability challenges applicable to IoT technology.

In light of the current state of play, ECSO considers that it is of utmost importance that IoT cybersecurity is addressed in a comprehensive manner, involving stakeholders from all the vertical domains. The scope of this technical paper is to identify current and foreseen challenges related to IoT cybersecurity at technical level (both from the IoT supply point of view and the IoT adopters' point of view), at regulatory level, and in relation to certification.

[1] European Commission. The EU's Cybersecurity Strategy for the Digital Decade. JOIN(2020) eighteen final. December 2020. Available at https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 Last accessed 19 July 2022.
[2] European Commission. Liability for emerging digital technologies. SWD (2018) 137 Final. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0137&from=en Last accessed 19 July 2022.

2. The relevance of IoT technology

2.1. The current ecosystem

Most of smart and connected devices lack basic security and privacy functionalities having an impact on the trust in connected solutions, and consequently on their market opportunities. With the growing number of hacked devices[3,4] and formerly unregulated and non-transparent data usage, consumers are becoming increasingly reluctant to invest in smart appliances. To foster trust as a core principle in the development of IoT products and services, regulatory initiatives are under preparation at the EU-level and on a global scale.

IoT infrastructure is typically installed to transform an existing environment. It is therefore necessary to bring a system from an untrustworthy or unconnected state into a trustworthy mode of operation and maintain it throughout its lifetime. While personal computers and servers are maintained with security updates for their entire lifespan, IoT devices are typically sold and installed in the field. Security fixes and functional upgrades have to be incorporated into IoT infrastructures, while the corresponding business models should provide a sustainable ecosystem.

In 2019 the number of connected devices reached 26.66 billion and it is expected to grow up to 74.44 billion devices in 2025[5]. As more devices become connected through the Internet of Things, integrated security solutions providing the latest and up-to-date cryptographic techniques are critical for preventing sophisticated system attacks and protecting private user information. System security can only be achieved at system-level by collaborating with the actors governing and advancing the respective sectors. Financial institutions, manufacturers, insurers, retailers, governments and public service providers depend on secure embedded systems that defend their critical infrastructure against IoT security breaches.

While many of today's always-connected technological devices take advantage of cloud computing, future architectures will see more computing and analytics on the devices themselves. This on-device approach helps reduce latency for critical applications, lower dependence on the cloud and better manage the massive deluge of (personal) data being generated by IoT. Edge computing encompasses sensors that collect data (such as RFID tags), which can be then processed in an on-site or off-site data centre, for instance, being connected to power local computing deployed within the 5G continuum. Data processing happens at the source, far away from or at the "edge" of the cloud, allowing anonymisation or pseudonymisation of personal or corporate data. Edge computing networks can still connect to the cloud, when necessary, but they do not require the cloud to function. Edge computing, however, demands considerably more attention to deal with cybersecurity threats at the device level compared to what has been done until today. This includes the need for closer interaction and mutual strategic developments between large cloud service

[3] Dallon Adams, R., 2022. IoT device attacks double in the first half of 2021, and remote work may shoulder some of the blame. TechRepublic. Available at: https://www.techrepublic.com/article/iot-device-attacks-double-in-the-first-half-of-2021-and-remote-work-may-shoulder-some-of-the-blame/ Last Accessed 19 July 2022..

[4] Fadilpašić, S., 2021. IoT attacks are now becoming more frequent than ever. [online] TechRadar. Available at: https://www.techradar.com/news/iot-attacks-are-now-becoming-more-frequent-than-ever Last Accessed 19 July 2022.

[5] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. Available at https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ Last accessed 19 July 2022.

providers and device and component manufacturers (e.g., RFID chip developers), as well as joint standardisation efforts, as traditional value chains begin to transform into value networks.

2.2. IoT reference architectures

IoT is a umbrella term that covers different technologies and various application domains. Therefore, there is a great variety of different solutions, and the terms adopted vary from one technological solution to the other. In scientific literature, few survey papers outlined the IoT layers and main architectural components, among which a discussion of open challenges and main issues[6], a comparison of existing reference architectures[7], which outlines differences and security issues including known challenges[8], with a special focus on industrial context.

From an industrial perspective, all the vendors that aim at producing devices and solutions for the IoT market, propose their reference architecture to outline how to set up an IoT application relying on the hardware/software components they produce. As an example, a three-layer architecture[9] (*Things*, *Insights* and *Action)* focuses on a Data processing, Analytics and Management layer, addressing all the services needed to develop a new IoT solution on top of the cloud. The lower layer (Device connectivity) is just relegated to the role of data collection and sharing. Other approaches[10] consider a six-layer architecture, depicting many different ways of deploying and assigning roles to the different devices.

There is also a concrete ongoing standardisation effort and two of the most relevant are probably the ITU-T [11] and ISO [12] . The remaining of the section considers the four-layer logical stack, synthesised as in Figure 1, that both standards support.

IoT-A[13] proposes the creation of an architectural reference model for IoT, as well as the definition of a set of key building blocks to lay the foundation for a ubiquitous IoT.

[6] Borgia, Eleonora. The Internet of Things vision: Key features, applications and open issues. Computer Communications, 2014, 54: 1-31.
[7] Di Martino, M. Rak, M. Ficco, A. Esposito, S.A. Maisto, S. Nacchia, Internet of things reference architectures, security and interoperability: A survey, Internet of Things, Volumes 1–2, 2018, Pages 99-112, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2018.08.008.
[8] L. D. Xu, W. He and S. Li, "Internet of Things in Industries: A Survey," in IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233-2243, Nov. 2014, doi: 10.1109/TII.2014.2300753.
[9] Microsoft Docs, Microsoft Azure IoT Reference Architecture Azure, Version 2.0. Available at https://aka.ms/iotrefarchitecture Last accessed 19 July 2022.
[10]IoT Joint Reference Architecture from Intel and SAP, Available at https://www.intel.com/content/dam/www/public/us/en/documents/reference-architectures/sap-iot-reference-architecture.pdf Last Accessed 19 July 2022
[11] Recommendation Y.2060: Overview of the Internet of things
[12] ISO/IEC 30141:2018 Internet of Things (IoT) — Reference Architecture
[13] Cordis.europa.eu. 2022. CORDIS | European Commission. Available at: https://cordis.europa.eu/project/id/257521 Last accessed 19 July 2022.

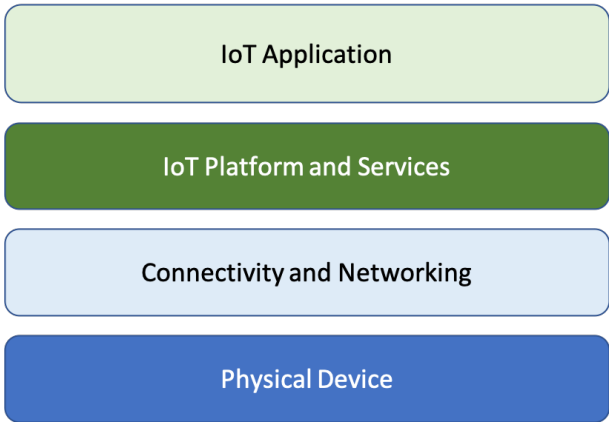

Figure 1: Internet of Things Layers

The ARMOUR project[14], which aimed at providing duly tested, benchmarked, and certified Security & Trust technological solutions for large-scale IoT, does not propose a specific IoT architecture, but it adopts the typical IP/TCP layered model with four layers.

Industrial Internet Reference Architecture (IIRA)[15] is based on the ISO/IEC/ IEEE 42010: 2011, and it considers four layers or viewpoints: Business, Usage, Functional (divided in control, operations, information, application, and business) and Implementation.

The Reference Architecture Model Industry 4.0 (RAMI 4.0)[16] is the German standard DIN SPEC 91345:2016-04. It considers six layers: Business, functional, information, communication, integration and asset.

Figure 2 briefly summarises the main concepts involved in any IoT System[17]. The **physical entities** are real-world thing controlled by **IoT devices**, which may act as actuators (modifying the state of the physical entities) or as sensors (reading the state).

A **Service** is a capability offered to **IoT users** based on interaction with one or multiple IoT devices. Services are commonly able to store data, perform analytics and automate behaviour of IoT devices, controlling them remotely.

An **IoT gateway** is a digital entity that connects one or more IoT devices to a wide-area network. The IoT gateway interacts through the network and exposes the endpoint to enable remote services to interact with devices.

IoT users are the users of the IoT System, they can be human or non-human (digital systems). IoT users can interact directly with IoT devices or use the system through services and IoT gateways.

[14] ARMOUR Project. Deliverable D4.5 ARMOUR Benchmarking and certification center
[15] IIC, "The Industrial Internet of Things, Volume B01: Business Strategy and Innovation Framework," 2016.
[16] Dr. Kartsen Schweichhart, "Reference Architectural Model Industrie 4.0 (RAMI 4.0): An Introduction," in Publikationen der Plattform Industrie 4.0, 2016, vol. 0, no. April.
[17] The picture is a simplified and adapted version of the conceptual model proposed in standard like ISO 31041. The goal of the picture is to offer a simplified view, not a full reference standard.

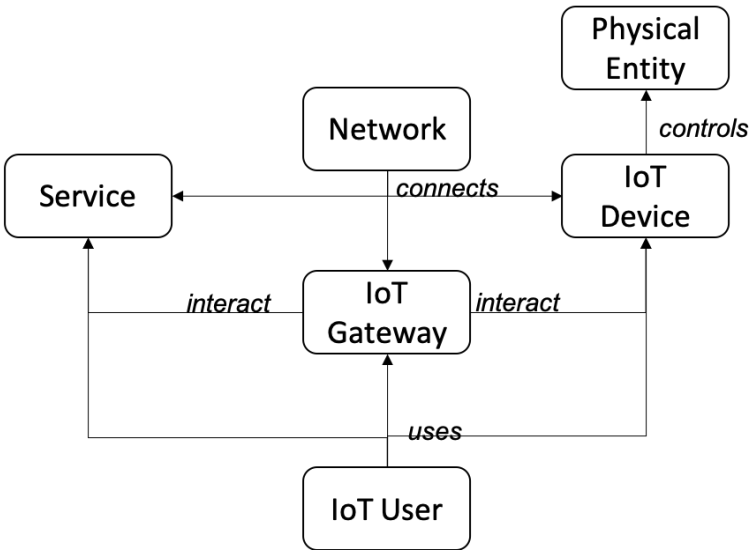

Figure 2: IoT Main Concepts

It is worth noticing that different technological solutions may impose distinct interaction rules among components, but the simplified diagram in Figure 2 applies in almost all cases. The conceptual diagram helps identify all the assets involved in an IoT System and coherently, pinpoint possible security issues.

2.3. Technological aspects

IoT settlement in daily activities require a high level of security and reliability, which is only possible with the certainty that no cybersecurity risks are at hand. This implies awareness, as well as training of professionals and users. However, the key to success is the adequate implementation of technical enablers. The following sections discuss some of the main critical technical aspects that should be addressed to enable IoT cybersecurity deployment.

2.3.1. Secure and trusted physical devices

Physical IoT devices have few characteristics in common. The value of IoT is best realised in environments with a large number of heterogeneous devices interacting directly, or through a cloud platform. The typical issue in an IoT ecosystem arisen from the limitations in the device cost, size, computational power, power consumption, and longevity. Continuous technological advancement does help find the best balance with these aspects, but it all depends heavily on the application and the orchestration of resources. For instance, it is not simply possible to rely on more computing power as new categories of devices will come into existence through miniaturisation that will bring in other constraints.

IoT devices that are deployed in the field provide a large attack surface, as they are also susceptible to physical tampering and attacks. This can not only leak or corrupt sensitive data but also expose the intellectual property of the device manufacturer. Depending on the use case and the device, attacks can span from a rather coarse tampering to highly sophisticated side-channel or fault attacks. Even further, privacy mechanisms should be provided in the field devices as to address, among others, the identity explosion, in which a set of mobile and localised devices (sensors and

actuators) identify a citizen for a while in continuously reassigning processes. There are plenty of countermeasures available to protect not only against known vulnerabilities but also beyond, by taking the precaution principle into account.

For the sectors with the highest security requirements, specialised tamper protection mechanisms allow to further raise the bar for attackers. While today's countermeasures typically provide a gradual improvement or protection against specific classes of attacks, new resilient architectures are required to increase security in IoT fundamentally.

Trust starts with the processors at the core of each IoT device to create trustworthy platforms. Recent open-source instruction sets, such as RISC-V, consider European sovereignty over the implemented circuits and facilitate modifications at the core of the architecture to tackle device, sector, or application-specific security constraints[18].

IoT security must be designed and architected from the beginning for all types of IoT devices and sensors. It should not be an optional add-on feature. The manufacturers should provide built-in security functionalities and guidance on best practices to facilitate architects in building secure IoT systems IoT security can be achievable from the power, cost, and budget perspectives.

2.3.2. Secure and trusted connectivity and networking

The wide range of connectivity options creates unique challenges, especially for generic IoT platforms. The physical connection layer for IoT devices can be a wired Ethernet connection, either directly to the internet or through a gateway device. Alternatively, devices can establish the connection using wide variety of wireless technologies. These can be roughly categorised according to range, bandwidth, and power requirements, with each category bringing different challenges. For example, low power, long range technologies such as LoRa, Sigfox and NB-IoT cannot provide bandwidth for over the air (OTA) firmware updates, whereas low power, short range technologies such as ZigBee and Bluetooth have the capability. The protection of data in transit also depends on the features and bandwidth provided by the physical layer.

With billions of new connected devices, it becomes inevitably important to secure these devices and services independently from their complexity. In the last few years, there have already been attacks on critical facilities around the world, from the injection of Triton into the control and security systems of an oil and gas plant, to the shutting down of NotPetya's pharmaceutical production, or the SolarWinds attack. The IoT devices cannot just "simply" be connected without incorporating appropriate cybersecurity functionalities and end-to-end security: the financial costs are not the only risk, also people' lives and data could be impacted.

Trusted networking relies on the capabilities of the trusted hardware and connection layer. Networking must provide mutual authentication and traffic encryption to ensure security. Credentials must be kept secure from the creation of the credentials, through injection into the devices until secure network on-boarding process. Those securely-stored credentials shall then also be used to secure any device interface. All this reduces the attack surface, but nonetheless

[18] Open Source Hardware & Software Working Group.2021. Recommendations and Roadmap for European Sovereignty in Open Source Hardware, Software, and RISC-V Technologies. Available at: https://7de8a762-9d0e-4da8-a5a8-0e8d68aae359.usrfiles.com/ugd/7de8a7_7c025f0b533146d9bf726fb36dd384af.pdf Last accessed 19 July 2022.

the stack is the external interface of the device, and as such, it must be updateable in case of discovered vulnerabilities.

Furthermore, advanced privacy mechanisms are needed to enable people, organisations, machines, and applications to request access/authorisation confirmation, consent and confirm transactions based on already agreed and defined authentication, authorisation and access models to access and use IoT devices and data (existing platforms, resources and authentication services available).

2.3.3. Secure and trusted IoT platforms and services

Another important technological aspect for IoT is interoperability. The increasing number of devices, protocols, and data models, each designed with its own particularities in mind, poses a problem of total understanding between all the IoT components. This is also a relevant problem regarding cybersecurity as different protocol implementations and unavailable cyphers, or algorithms may impede communications between devices/services and even also compromise security if communications default to plain text. In addition, all employed protocols in a system have to be maintained and updated so that this heterogeneity increases the cost of operating a secure IoT network.

Hardware trust anchors form the foundation to create a trusted platform that ensures confidentiality and integrity of the acquired data and ensure a trustworthy operation. Especially in the context of legacy devices, less trustworthy devices have to be separated to protect the network and to protect the device as well.

2.3.4. Secure and trusted IoT applications

One of the core drivers of IoT is the opportunity to collect and analyse large amounts of real-world data. Keeping control over the data at the manufacturer can be a core asset for European technology to provide secure IoT applications, especially in sensitive sectors, such as the medical one. Ensuring privacy by design as a key tool for the development of cyber secure IoT applications is the way to ensure the required society's trust in IoT. Further, citizens should be empowered with the ability to specify/update/modify/trace the privacy policy over the exchanged data, also on those devices they do not own.

3. Technical challenges

3.1. Cybersecurity challenges

This section details the most significant cybersecurity technical challenges in relation to IoT technologies. The challenges are grouped into five different categories: four of them correspond to the different layers in the IoT stack (device, connectivity, platform and application), and a fifth category groups the challenges that cut across different layers or IoT systems as a whole.

3.1.1. Challenges at device level

The current constraints that IoT devices configure, such as power consumption, low cost and lifecycle increase the challenge to provide cyber secure IoT environments. These three axes must be considered to ensure the return on investment of cybersecurity usage.

Power consumption: Many IoT devices have no direct permanent power supply and need to use external batteries that must live for years. These rely on hardware design focused on battery consumption and will lack capabilities to devote to encryption or hardware security mechanisms. More recent applications of IoT devices consider the deployment of dedicated ecosystems, e.g., Industrial Internet of Things, where power supply is available, or where the lifespan of the device is limited.

Low cost: The IoT market is very competitive, which often translates into high pressure for lowering the costs of the designs. In many cases, a low-cost hardware design leaves little room for processing power, memory, or storage. Being this so, little or no effort is devoted to security since the cost poses barriers to security capabilities due to limitations in hardware space or processing power.

Lifecycle management: There are devices designed for a short life span while there are others that must be alive for decades. So, the range of possibilities is very wide. There may be devices which simply will get to a time where they will have hardware issues that may not allow being updated or others that may have security incorporated but since they have no maintenance may be deprecated in the future. Also, lifecycle expectations may vary, as some devices (e.g., cars) or environments (e.g., plants) will need regular maintenance schedules where software can be reconfigured and updated. Maintenance frequency is typically in the 1-to-2-year timescale, sometimes even more, compared to the three-six months software releases of major IT vendors. This provides an opportunity for software maintenance but also introduces constraints in between two scheduled maintenances, where devices must operate as is. Furthermore, there is a risk of misalignment and discrepancy between a wide range of IoT devices running several versions of their embedded software providing different capabilities, and a possibly unified pure-software backbone, which is updated at regular intervals.

Some specific challenges are listed below:

- Secure execution and trust of IoT devices and services to be connected to an ICT infrastructure.
- Firmware and application integrity, and delivery updates. Scalable remote attestation procedures.

- Protection against advanced physical attacks such as side-channel and fault attacks for data and intellectual property protection.
- Protection against micro-architectural attacks such as Spectre or Meltdown in devices with low computing power constraints.
- Availability of an open-source hardware that allows a European sovereignty over the deployed circuits
- Secure migration to post-quantum cryptographic algorithms, especially for high-assurance devices or devices with a long-expected lifetime. Support of hybrid approaches PQ and classical in the migration period.
- Automate, facilitate and drastically speedup the overall process within IoT ecosystem through distributed ledger (blockchain-type) technologies, along with contracts that can translate conventional agreements into smart contracts (for automated transactions)

Building highly secure and trusted devices is challenging. Regardless of the industry, seven properties can be considered to incorporate highest levels of security in every network-connected device[19]:

- *Hardware Root of Trust* – Is the device's identity and software integrity secured by hardware?
- *Compartmentalisation* – Can the device's security protections improve after deployment?
- *Small, trusted computing base* – Is the device protected from bugs in other code?
- *Defence in depth* – Does the device remain protected if a security mechanism is defeated?
- *Certificate-based authentication* – Does the device use certificates instead of passwords for authentication?
- *Security renewal* – Does the device's software update automatically?
- *Failure reporting* – Does the device report failures to its manufacturer?

The implementation of these properties might require the hardware and firmware software of the device to work together, with device security rooted in hardware and guarded with secure software, e.g., for microcontroller-based devices.

3.1.2. Challenges in connectivity and network layer

The wide range of IoT communication protocols or not using adequate channels may contribute to increase the vulnerability of the IoT ecosystem and the attack surface. In this direction, there is still some work to do in securing both the communication channels within a IoT ecosystem, both in the field, when capturing sensor data, but also when using the data within the IoT management applications link to specific local networks.

Anyone of the interactions depicted in Figure 2 may be affected by security issues. Therefore, it is very important to identify which sections of the networks supporting such interactions may or may not be insecure. To this end, the nature of the attacker must also be considered. For instance, private network sections are indeed more secure and therefore less protected, but may be easily jeopardised by an insider attack threats.

Therefore, a major challenge is to guarantee proper isolation between different network sections with different levels of exposure and of vulnerability. Different solutions must be devised for the various communication layers, either between IoT devices and IoT gateways or between the IoT gateways and the IoT applications. Moreover, the location of the IoT applications has to be considered, since it may be either local or remote in the cloud.

[19] Microsoft Research: The seven properties of highly secure devices, 2017.

Two main drivers should be considered, securing the channels, but also securing the data being transmitted from and to the IoT management system, to ensure the adequate level of privacy of the data being transmitted. Some of the relevant challenges are:

- Secure data transmission (encryption data in motion)
- Secure data storage – needs to be securely stored on the devices as well as in the cloud (encryption data at rest)
- Secure software/firmware updates
- Security and privacy (including anonymisation) of data retrieved from IoT devices and processed in cloud IoT platforms
- Transition to edge/fog computing
- Secure key management for a high number of distributed devices
- Secure network onboarding processes
- Network security improvements (secure routing, cryptography, network-level privacy)
- Standardisation of IoT communication protocols, which should embed proper security capabilities
- Embedding proper security capabilities in IoT communication standards

3.1.3. Challenges at IoT platform and IoT service layer

A key attack surface is still linked to the actual implementation of the solutions and services, which in many cases are still not addressing a secure by design approach for cybersecurity aspects. At the IoT Platform level, it is relevant to address the security of the platform itself and the one of the interconnected legacy systems. This increases the attack surface. Below, some specific aspects that should be carefully considered are presented:

- Platform security “as a whole” needs to be considered one of the most important security challenges for IoT
- Security audits for distributed devices with constrained capabilities
- Development of specific resistance methods and models to not only counter active (faults) attacks but also counter passive (side-channel) attacks; with the latter becoming a more relevant scenario for many IoT use cases[20]
- Managing security and resilience when allowing interaction of legacy systems with new devices
- Enable secure self-management of IoT ecosystems, including i) situational awareness (allow humans and devices to understand the state of their surroundings), ii) predictive systems (models that analyse the state of the resources, detect errors, and find potential alternatives), and iii) reactive systems (mechanisms that allow the system itself to react against failures)
- Mitigating DDos Attacks
- Shifting security checks and controls to the IoT device level releases constraints on backend IoT applications and services. To this end, the design of lightweight security solutions deployed on the IoT that provides advanced protections, usually offered by backend security servers (e.g., data access control solutions) is needed. Some of these solutions can benefit from other enablers, such as Cloud/Edge computing, for example with respect to off-loading intensive computation of security functionalities without undermining IoT security and its secure operation
- Secure lifecycle to establish, operate and update IoT networks with a special focus on the integration of legacy devices

[20] Side-channel attacks on the internet of things: Threats and challenges | Request PDF. Available at: https://www.researchgate.net/publication/325090884_Side-channel_attacks_in_the_internet_of_things_Threats_and_challenges. Last accessed 19 July 2022.

- Integration of more advanced security mechanisms in existing IoT platforms, such as FIWARE, and protocols, such as MQTT and CoAP

3.1.4. Challenges at application layer and related to end-users

An incipient aspect in current times is to leverage the data quality provision while preventing data privacy principles and regulations in IoT ecosystems and globally. From the cybersecurity perspective, the following available data can be used to enhance IoT ecosystems and societies at no costs for the user privacy rights:

- Data protection and compliance with legislations and directives
- Usability of security solutions in IoT ecosystems
- Robustness due to an increased attack surface emerging from the pervasive use of the technology
- Additional security considerations are required to tackle risks of exposure of sensitive information (private personal or business confidential data) in the IoT environment.
- Interaction between multiple involved parties in an IoT network (users, device manufacturers, network operators, cloud service providers, etc.)
- Define usable mechanisms for citizens to understand and decide for themselves how to protect their privacy in a smart context.

3.1.5. Cross-cutting challenges

There are technical challenges related to IoT cybersecurity that affect all previously mentioned layers and levels to varying degrees. Some of these challenges are described below:

Identity explosion and authentication. Besides the huge number of entities, since the interactions can be dynamic, these might not know each other in advance, as in the case of vehicular networks circulating on roads with sensors. Additionally, as in many scenarios, instead of who, the entities might be identified by their own or the context's attributes. Furthermore, the heterogeneity of the entities in IoT which can be computers, servers, application gateways, sensors, actuators, RFID tags, etc., leads to the differentiation of three categories of identifiers: object identifiers, communication identifiers and application identifiers. Moreover, some entities might have multiple identities in different contexts and applications, or some users might have their identity replying on devices minimal entities that act and identify on behalf of the user. Moreover, traditional user-password authentication might not be suitable. Finally, in some scenarios, a user might delegate credentials to some virtual entities under the concept of digital shadow.

There are scenarios where things belong to a local spatial area, where local identity providers can manage the identities and even set trusted relationships with external entities for more agile inter-domain authentication processes. These relying identity providers allow to avoid the authentication logic in the devices since the authentication can be based on proofs of identity when interacting with external entities. However, besides the absence of a unique central directory, different identity providers need to be dynamically integrated into a collaborative scenario, so distributed authorisation mechanisms are required as conveyed below.

Privacy. A data provider expects to be able to decide whether to share or not a particular data set. In distributed IoT scenarios each entity should define the granularity of the generated and shared data and enforce a proper access control policy on them. This entity-centric approach needs to be aligned with the user-centric approach that might interact with several devices around.

Each user might indeed need proper and usable interfaces to define the granularity and the access control policy on each device. This might be achieved by relying on privacy-preserving distributed data mining algorithms, multiparty computation, or active isolated bundles containing data, metadata and application. In any case, legal privacy regulations need to be mandatorily considered. There is another issue related to the potential entities that might track and profile users' activities without their consent. These misbehaving environmental entities also might work collaboratively in the network, so a user-centric approach might scan any active device prior to any operation to be aware at least of surrounding devices and eventually rely on the privacy coach concept. Some of the relevant cross-cutting challenges are:

- Distributed authorisation and authentication mechanisms. Scalability of authentication in resource-constrained devices
    - Lightweight authentication, scalable identity management solutions, secure digital identities solutions and distributed and trust management
    - Holistic Identity Management for IoT objects: personal identity ("who I am"), core identity ("what I am"), association identity ("whom I am associated with" or "who is my owner"), and location identity ("where I am")
    - Development of blockchain privacy-preserving approaches following a self-sovereign identity management approach (i.e., allowing for the possibility of using non-interactive zero-knowledge proofs), while maintaining the capacity of unveiling the real identity of the owner when the inspection grounds are met (e.g., identity theft or associated crimes)
- Definition and implementation of secure software engineering principles to facilitate the definition and development of secure IoT devices, infrastructures and applications.
- Definition of forensics procedures in the context of IoT (e.g., device forensics, platform forensics, application forensics) from a technical and legal standpoint
    - Provide mechanisms for smart devices capable of enabling forensics investigations while preventing access to personal data when the devices are borrowed or disposed of
- Intrusion detection and management
    - Development of Intrusion Detection Systems (IDSs) able to cope with a variety of IoT devices, networks and platform capabilities
    - Development of specific threat intelligence tools that can support multiple IoT devices and protocols. Examples of such tools are security information and event management (SIEM) tools and configuration and vulnerability analysers
    - New vulnerabilities linked to the future evolution of the dynamic IoT environment (large variety of communication protocols, APIs and standards)
    - Development of Intrusion Detection Systems (IDSs) suitable to the specific requirements of IoT networks while accommodating the shortcomings of IoT nodes.
    - Develop methods to efficiently create, disseminate and consume threat intelligence in a standardised, usable and legal way
    - Risk management and understanding of the evolution of attacks
    - Adaptive countermeasures

3.2. Current status and foreseen directions

The challenges identified in Section 3.1 represent a snapshot of what concerns IoT technology experts in relation to security and trust. Several challenges arise at different layers of the IoT stack and across the full IoT stack. Tapping into the challenges identified above, several IoT cybersecurity aspects that are critical for the IoT vision are discussed as follows:

Awareness

- Security risks for professionals and the need to increase awareness: ENISA has published a study on the need to raise awareness of cyber security threats of IoT in critical infrastructures and provides recommendations to face cyber threats.[21]
- Consumers' awareness of IoT cyber security risks: IoT devices are increasingly pervasive in the life of citizens. Security risks range from potential personal data breaches to affecting the daily life of citizens due to the potential misuse and attacks on IoT devices (e.g., smart homes, etc.)

Security by Design

- Simulation and cyber range tools need to address emerging technologies. Tools need to be extensible and able to easily incorporate domain specificities, including different types of devices and systems from IoT to more complex cyber-physical systems, and address different scenarios with various levels of cyber-attacks
- Adaptability and reconfigurability must be supported to guarantee the possibility to dynamically adapt the architecture or the infrastructure. SDN seems to be one of the best enabling technologies thanks to the support of network isolation and configuration decoupled from hardware and specific interfaces. Examples that support these statements includes Security Policy Enforcement over SDN architecture[22], Enhancing SDN security for IoT-related deployments through blockchain[23] and Secure stateful SDN data planes [24]
- Integration of distributed ledger technologies to provide security services, such as decentralised access control management and secure decentralised firmware updates.
- Integration of technologies providing a root of trust (e.g., ARM TrustZone) to facilitate the implementation of security services (e.g., credentials storage, secure boot, code integrity testing)
- Use of edge/fog computing solutions to delegate the execution of security and privacy services (e.g., privacy helpers)
- IoT devices hardened against physical attacks
- Secure firmware updates for scenarios with lots of distributed devices with constrained capabilities
- Secure lifecycle management for IoT
- Secure policies for the lifecycle of an IoT device based on established Information Security Standards
- Privacy-preserving schemes for IoT

Detection and prevention

- Special protection measures against botnet malware Management of IoT data and control flows in agreement with the process for the detection of anomalies (fake IoT devices, false data injection, IoT device take over, etc.)
- Distributed/collaborative intrusion detection
- Lightweight machine learning primitive for on-node intrusion detection
- Development of novel intrusion detection strategies, including not only advanced mitigation techniques (honeypots, SDN-based solutions, derivation of anomaly rules by parsing

[21] ENISA. 2017. Baseline Security Recommendations for IoT. Available at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot Last accessed 19 July 2022.
[22] D. Berardi, F. Callegati, A. Melis and M. Prandini, "TechNETium: Atomic Predicates and Model Driven Development to Verify Security Network Policies," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), 2020, pp. 1-6, doi: 10.1109/CCNC46108.2020.9045145.
[23] C. Tselios, I. Politis and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2017, pp. 303-308, doi: 10.1109/NFV-SDN.2017.8169860.
[24] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi and M. Conti, "A Survey on the Security of Stateful SDN Data Planes," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1701-1725, thirdquarter 2017, doi: 10.1109/COMST.2017.2689819.

manufacturer usage descriptions such as IETF MUD), but also the exchange of standardised threat information between different IoT actors
- Integration of security services in gateway devices, which will act as trusted third parties – implementing security services on behalf of the IoT devices they supervise
- Easy reset of devices in case of compromise

Cryptography

- Cryptography for low-end devices which will be constrained due to several causes (low computing power, low bandwidth, low battery, etc.)
- Transition to post-quantum cryptographic algorithms (Energy-efficient cryptography, or lightweight cryptography)
- Pairing-based cryptographic schemes (e.g., attribute-based encryption) to extend the security features of IoT devices
- Post-quantum computing schemes as currently being standardised by the U.S. National Institute of Standards and Technology (NIST)[25] to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks
- Multi-party computation (MPC) with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private
- Cryptographic functions in compliance with proven industry standards

Auditability/Liability

- Scalable security audits for distributed devices with constrained capabilities
- Supply chain management and liability: Integration of IoT devices in more complex products
- Management of responsibilities in case of cyber-attacks, including the maintenance of the product and the data protection.
- Risk management system and prioritisation of safety measures according to their application and potential impact
- Mechanisms and processes to inform the users in the event of threats

3.2.1. A roadmap towards a European cybersecure Internet of Things

The concept of trusted and resilient IoT devices and how they can easily be identified by consumers and integrators is driving some of the future challenges for Europe. Major efforts must embrace multiple directions, e.g., novel cyber secure IoT development processes and methodologies, and a new generation of cybersecurity-ready developers, analysts and entrepreneurs who are ready to create new added value cyber secure solutions. These areas of improvement, both involving manufacturers as well as software developers, should be part of a roadmap promoting a secure by design approach, in which cybersecurity is addressed at the design phase considering all basic principles in hardware and software development. Innovation will play a key role in future cyber secure IoT solutions, as the one-for-all principle is no longer valid. The hardware has to be agile enough to adapt to deployment scenarios, which currently are self-contained and have their own personalised characterisations, making current products in the plug & play form no longer working.

[25] Csrc.nist.gov. 2022. Post-Quantum Cryptography | CSRC. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography Last accessed 19 July 2022.

Today, no matter the size, an IoT deployment is composed of various tiny, embedded networks that have their characterisations and needs. "*An urgent prerequisite for securing IoT is the development of efficient security mechanisms for tiny embedded networks with scarce resources*[26]." Being this so, there is a need to invest in efficient, robust and low-consumption cryptography, improved key management, authentication mechanisms, credential management and new security solutions that can adapt to the environment. Cybersecurity in IoT and beyond must be considered as a need and self-adaptive at the edge.

3.3. Challenges of IoT on vertical sectors and their needs

The following table highlights the relevant challenges for the usage of IoT devices across different vertical sectors.

Challenge	Description	Potential impact
Trust	Establishing, negotiating, updating and revoking trust among entities in the IoT context is an essential task.	The lack of trust reduces entry to market or can even exclude one
Privacy	It refers to the fact that a user is able to control how and when personal information is collected, shared and used.	The lack of compliance to this implies being taken out of the market, as well as having to face demands and other issues
Resilience	Systems must be built according to security by design principles to withstand attacks	No deployment in security and privacy sensitive sectors
Attack surface	All sectors represent critical verticals where the additional attack surface of IoT systems increases the risk of a successful cyber attack	Disruption of a critical service
Domain-specific regulations	Critical sectors are heavily regulated; Platforms may not be able to adapt to concurrent sets of differing regulations	Barrier of entry to the market; Fragmentation of the market with domain-specific solutions
Security Certification	Security certification should guarantee a minimum-security level, but it is more important to guarantee homogeneity between different	Higher acceptance and trust in IoT devices and solutions

[26] Riahi Sfar. A, Natalizio E., Challal Y., Chtourou Z., "A roadmap for security challenges on the Internet of Things", Digital Communications and Networks (4) 2018, p. 118-137.

	evaluations and facilitate the end-user with the comparison between different devices	

Table 1: Cross-sectorial challenges and needs

The integration of IoT devices in the vertical sectors has introduced some intrinsic challenges linked to their usage, as discussed in Table 2.

Vertical sector	IoT Specificities and challenges
Industry 4.0 and ICS	Long component lifetime, legacy support; critical systems and real-time needs; industry's resistance to change.
Energy and smart grid	High interconnectivity and the risk of cascading effects; security, fraud detection and early blackout detection.
Financial services	Trust, real-time needs, reliability and resilience.
Public services, e-government, digital citizenship	Privacy preservation and need to guarantee trust.
Healthcare	The growth of distributed and connected medical devices brings new challenges for the advanced security evaluation within the product lifecycle (manufacturers to continuously manage and maintain their device's cybersecurity throughout the product's lifecycle) and requires advanced security access controls, built-in security, etc. Privacy preservation: needed trust for shared and retrieved data Coordinated response systems
Smart cities and smart buildings	Large attack surface, devices may be publicly accessible, privacy issues due to aggregation.
Telecom, media and content	The 5G infrastructure (towers, gateways, networks) and the third parties involved (mobile devices, IoT devices, VNF providers) present several problems about the partner's responsibility. Contracts oblige the SP to offer the agreed-upon QoS but if there are accidents or frauds in a critical service using a slice (e.g., due to an insecure product or operation), the SP or any Slice Component Provider can be liable. In this multi-party and multi-layer 5G architecture, the definition of liability and responsibilities when security breaches occur is essential to support confidence between parties and compliance with regulation.
Transportation/Mobility	Challenges are connected to self-driving vehicles and the risk of ECU hacking, in addition to mobility and roaming issues, possible loss of connection with

	cloud systems, privacy of data retrieved from personal cars (e.g., geolocation), etc. Focus on safety and security: Currently, people in the automotive industry are skilled and are used to deal with safety issues during the development of the vehicle, mainly due to the existence of previously well-established automotive safety standards. However, when talking about security, there is a lack of knowledge on how to deal with protection of the system. It is no longer acceptable to think that safety-critical domains, such as the automotive one, are immune to security risks. For instance, when attackers affect the physical operation of the smart vehicle, network cybersecurity and physical safety become interdependent. Despite initiatives to include security in these processes, there is still a lack of a common standard allowing a complete integration of safety and security in the car development lifecycles[27]. IEC 61508 is an under-development standard that provides a first effort of integrating safety and security, but threat analysis is lacking details[28]. The last edition of ISO 26262 also tries to face this challenge by providing some recommendations for the interaction between safety and security. Liability: The smart vehicles context involves many stakeholders, among them are car manufacturers, system suppliers, users and road operators. A vehicle can have around 30k components[29]. The supply chain involves OEMs and a tier layered system. Manufacturers, also known as Original Equipment Manufacturers (OEMs) produce some original equipment, but their focus is on designing, promoting, and assembling the vehicles. Inside the tier system there are tier 1, 2 and 3 suppliers. Given this scenario, in case of a cybersecurity incident occurs in the vehicle, who is responsible? All the stakeholders involved in the supply chain can blame each other. There is therefore a need to ensure traceability throughout all stages of the supply chain, ensuring adequate flows of liability and distinguishing between assembly issues and component issues. If an organisation cannot precisely establish the limits of its domain, the network it controls, this has important implications for the way it conducts its risk assessments.

Table 2: Summary of impact of IoT on verticals

[27] ENISA. 2017. Cyber Security and Resilience of smart cars. Available at https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars Last accessed:19 July 2022

[28] G. Macher, C. Schmittner, O. Veledar, and E. Brenner, "ISO/SAE DIS21434 Automotive Cybersecurity Standard - In a Nutshell," in Lecture Notes in Computer Science, vol. 12235 LNCS. Springer Science and Business Media Deutschland GmbH, 2020, pp. 123–135

[29] Amatechinc.com. 2022. OEMs, Tier 1, 2 & 3 - The Automotive Industry Supply Chain Explained - Returnable Packaging | Reusable Packaging | Amatech Inc. Available at: https://www.amatechinc.com/resources/blog/returnable-packaging/tier-1-2-3-automotive-industry-supply-chain-explained Last accessed 19 July 2022.

4. EU policy and regulation developments

IoT amplifies and reintroduces many regulatory and legal questions pertaining to digital technologies. Due to its foreseen massive and ubiquitous penetration, its rapid rate of technological change may outpace the ability of associated policy, legal and regulatory structures to adapt. Crucially, IoT devices that are components of Cyber-Physical Systems need to address both safety and cybersecurity concerns. Because IoT devices operate in a more complex way than stand-alone products, more complex scenarios need to be contemplated.

The European Commission and the Member States have an important role to play in securing IoT. By using their market power and carefully creating and implementing policies and regulations, they can encourage better outcomes for IoT security in the EU and in the world. The EU's Cybersecurity Strategy for the Digital Decade[30] highlights the need to build resilient Internet-connected things that are secure by design, resilient to cyber incidents and quickly patched when vulnerabilities are discovered.

Currently, the main pieces in the legislative and regulatory toolbox at EU level are the following:

- The **Cybersecurity Act (CSA)**[31] promotes a cybersecurity certification framework and the establishment of voluntary cybersecurity certification schemes for ICT products, ICT services and ICT processes with three assurance levels (basic, substantial, and high). The Union Rolling Work Programme (URWP), currently under definition, sets the areas for future candidate schemes and their prioritisation, as well as the inclusion of an IoT scheme, which is under consideration to address industrial and consumer IoT.
- The **General Data Protection Regulation (GDPR)** [32] requires the implementation of appropriate technical and organisational measures to protect personal data whenever they are collected or processed. GDPR concerns both companies that are part of the IoT supply ecosystem as well as end-user organisations.
- The **Regulation on electronic identification and trust services (eIDAS)**[33] does not seem to imply direct consequences on the IoT ecosystem, as it concerns mainly natural and legal persons, although it is listed here for completeness, considering potential indirect effects when trust services are employed. To address some of the shortcomings of the eIDAS Regulation, the EC has recently proposed a new regulation on digital identity[34] that could also have a potential impact on IoT, for instance potentially linking the devices with - legal persons.

[30] Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade. 16 December 2020. JOIN (2020) 18 final.
[31] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[33] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[34] Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. COM(2021) 281 final.

- The **Directive on security of network and information systems (NIS)** [35] introduces baseline requirements for security and obligations to report incidents. It mainly concerns companies operating essential services in sectors such as energy, transport, banking, financial market infrastructures, health, drinking water and digital infrastructures. The revised NIS Directive[36] concerns manufacturers with the intent to address the supply chain.
- The **Cyber Resilient Act (CRA)**[37], currently under definition, aims to address market needs and protect consumers from insecure products by introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services.
- The **New Legislative Framework (NLF)** Decision No 768/2008/EC defines the safety requirements that a product needs to comply with to enter the EU market.
- The **Radio Equipment Directive** 2014/53/EU (RED) establishes a regulatory framework for placing radio equipment on the market. Radio protocols are used by IoT devices to transport data where a physical or wired connection does not exist, therefore the RED will essentially cover all data-transmitting IoT devices.

Due to the heterogeneous nature of the Internet of Things, other directives are of interest, such as the Machine or the Medical Devices Directives. The Council of the European Union stresses the importance that "cybersecurity requirements should be defined in line with the relevant Union legislation, including the CSA, the NLF, the Regulation on European Standardisation and a possible future horizontal legislation, to avoid ambiguity and fragmentation in legislation."[38]

4.1. Cybersecurity certification

Nowadays, there is an increasing interest to establish a general basis for cybersecurity certification and labelling for Internet of Things devices. The Cybersecurity Act sets the basis for the definition of the future EU cybersecurity certification schemes. A certification scheme for cybersecurity, covering the requirements and the methodology to check the compliancy of the IoT device against the requirements, must overcome different obstacles. The first obstacle is the management of the security updates during the lifecycle of the product; the other big requirement of the Cybersecurity Act is that any certification scheme should be defined according to the risks in the intended use. For IoT devices, this intended use could be very different from one domain to another, thus adding complexity to the definition of the certification scheme.

Supply chain lays the foundation of IoT devices security, because the majority of these devices are comprised from a multitude of components from different suppliers (both hardware and software). At the same time, supply chains present a weak link for cybersecurity because organisations cannot always control the security measures taken by supply chain partners[39]. The security of the device should be monitored during the whole life cycle, to identify new potential vulnerabilities, and

[35] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[36] Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities. COM(2020) 829 final.
[37] European Commission. Cyber Resilience Act. Call for evidence for an impact assessment - Ares(2022)1955751.
[38] Council Conclusions on the cybersecurity of connected devices. 2 December 2020. 13629/20
[39] ENISA. 2020. Guidelines for Security the Internet of Things. Available at: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things. Last accessed: 19 July 2022.

updated due to a security change or update/patch of the product. This makes a lightweight recertification process and a smart certification composition very relevant for a successful approach.

While some of the previous challenges are being currently addressed by European organisations, the continuous evolution of the threats and cybersecurity challenges makes the adoption of a cybersecurity certification framework challenging. ECSO has published a state of the art[40] focusing on standards and certification schemes that can be (potentially) used as the basis for assessing the overall cybersecurity of a product or component, an ICT service, a service provider, organisation, or a critical infrastructure. In the context of IoT, ENISA has mapped standards against requirements on security and privacy with the intent to evaluate whether or not there is a significant gap in standardisation to bring secure IoT to the market[41]. The following sections provide an overview of the current state of the art for certification of IoT and some preliminary considerations.

4.1.1. Towards a combined approach of testing and risk assessment

Security risk assessment and testing processes are envisioned as the main building blocks for security certification and evaluation by different international organisations. Indeed, NIST[42] and CNSS[43] employ the terms of assessment and evaluation to define cybersecurity certification. The evaluation has a binary output, pass or fail, and it is in general done by an independent third party, while the assessment, such as a risk assessment, is an indication of the "status" at a given point, which can be done by the owner.

The NIST created in 2014 a Cybersecurity Framework (NIST CPS framework) to provide guidelines to support the management of cybersecurity risks. This framework was based on the Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"[44], and was updated in 2018 to address security requirements in emerging scenarios. Subsequent NIST publications, such as the NIST 800-37-R2 "Risk Management Framework for Information Systems and Organizations", have been aligned to the framework. NIST 800-37[45] also considers explicitly both processes as part of the certification.

NIST is also developing a series of documents, known as the NISTIR 8259 series, which goal is to define various cybersecurity best practices and guidance for IoT device manufacturers. These documents address the challenges described in the new IoT Cybersecurity Improvement Act of

[40] ECSO. 2017. State-of-the-Art Syllabus: Overview of existing Cybersecurity standards and certification schemes. Available at: https://www.ecs-org.eu/documents/uploads/state-of-the-art-syllabus-v1.pdf. Last accessed: 19 July 2022.
[41] ENISA. 2019. IoT Security Standards Gap Analysis Mapping of existing standards against requirements on security and privacy in the area of IoT. Available at https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis. Last accessed: 19 July 2022.
[42] NIST. Glossary of Key Information Security Terms
[43] CNSSI. 2015. CNSSI No. 4009: Committee on National Security Systems (CNSS) Glossary. Available at: https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf; Last accessed: 20 July 2022.
[44] Homeland Security. Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD-21 Critical Infrastructure Security and Resilience. Available at https://www.cisa.gov/publication/eo-13636-ppd-21-fact-sheet Last Accessed 19 July 2022
[45] Joint Task Force Transformation Initiative. 2014. Guide for applying the risk management framework to federal information systems: a security life cycle approach. Technical Report NIST SP 800-37r1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r1[9

2020[46]. The first document in the series, NISTIR 8259, provides specific recommended activities to help manufacturers address customer needs for IoT cybersecurity in their product development processes. The second document in the series, NISTIR 8259A, identifies a core baseline of IoT device cybersecurity capabilities for manufacturers. Such device capabilities are i) device identification, ii) device configuration, iii) data protection, iv) access to interfaces, v) software updates, and vi) cybersecurity state awareness.

Additionally, NIST recently published[47] a draft of a future IoT project, focused on the trusted network on boarding for IoT devices covering the device attestation, the network layer on- boarding and the application layer on boarding. The bootstrapping is enhanced with an optional step in which the device can generate or receive an attestation token with claims about it that allows to decide if the device is trustworthy enough to be on boarded.

ETSI[48] also provides a framework for security evaluation considering security risk assessment and testing, which explicitly states the integration of the two processes to assess the security of an ICT system based on ISO 29119 and ISO 31000 standards[49]. The benefit of the interaction between risk assessment and testing is mutual. On the one hand, in an agile approach, the tests can be prioritised according to the impact of the vulnerability and/or threat that they verify, and on the other hand, the risk estimation can use the results of the tests to refine the measurement and obtain objectives and empirical metrics. Furthermore, the ETSI standard also considers a process of treatment to deal with the encountered vulnerabilities, and transversal activities to communicate and monitor the security throughout the lifecycle of the target.

4.1.2. The approach to conformity assessment

Common Criteria (CC)[50] is a well-known security *certification* scheme, where the security functional and assurance requirements are specified for a class of ICT products, i.e., what is expected as protection for a specific class/type of product, through Protection Profiles (PPs). However, several limitations have been identified[51,52], which have been taken into account by the CC community, e.g., the time and effort requested to execute an evaluation or the management of changes in the certified product. Other important schemes are the Commercial Product Assurance (CPA)[53], the Cybersecurity Assurance Program (UL CAP)[54], the Certification de Sécurité de Premier Niveau (CSPN)[55], the ULD Datenschutz-Gütesiegel[56], the Certificación Nacional Esencial de Seguridad

[46] CONGRESS.GOV. 2020. H.R.1668 - IoT Cybersecurity Improvement Act of 2020. Available at : https://www.congress.gov/bill/116th-congress/house-bill/1668. Last accessed: 19 July 2022.
[47] NIST.2022. Trusted IoT Device Network-Layer Onboarding and Lifecycle Management. Available at: https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding. Last accessed:19 July 2022.
[48] ETSI. 2015. ETSI EG 203 251: Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies. Available at : https://www.etsi.org/deliver/etsi_eg/203200_203299/203251/01.01.01_50/eg_203251v010101m.pdf. Last accessed: 19 July 2022;
[49] International Organization for Standardization. ISO/IEC 31000 - Risk management. IEC. Available at: https://www.iso.org/iso-31000-risk-management.html. Last accessed: 19 July 2022.
[50] CCRA, Common criteria. About the Common Criteria. Available at :https://www.commoncriteriaportal.org/ccra/. Last accessed : 20 July 2022.
[51] M. B. a. Y. R. S. P. Kaluvuri, "A quantitative analysis of common criteria certification practice," in International Conference on Trust, Privacy and Security in Digital Business, 2014.
[52] F. K. a. D. Sullivan, "Applying the common criteria in systems engineering," IEEE Security Privacy, 2006.
[53] NCSC 2022. Commercial Product Assurance (CPA). Available at https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa. Last accessed: 19 July 2022.
[54] Underwriters Laboratories, Cybersecurity Assurance program UL 2900, 2016.
[55] ANSSI, Certification de Sécurité de Premier Niveau (CSPN), 2008.
[56] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, ULD Datenschutz-Gütesiegel.

(LINCE) [57] and the "Beschleunigte Sicherheitszertifizierung" (BSZ, Accelerated Security Certification)[58]. Despite the above, none of them address the challenges related of the dynamism of security, involving completely heavy recertification in case there is a security change. ENISA has completed the draft of the European Common Criteria (EUCC) certification scheme, which aims at replacing the SOGIS Common Criteria. The EUCC proposes to simplify the SOGIS Common Criteria by using the vulnerability analysis to define the level of certification, by introducing patch management to cope with the changes, and by addressing the certificate maintenance through “Assurance Continuity”.

IoT devices could be deployed in different contexts and integrated into different products or services, thus justifying the need for a cybersecurity certification scheme able to cope with all the challenges inherent to cybersecurity. In this sense, a desirable property is the comparison between different solutions in terms of security and assurance considering existing standards. Another property is coping with the dynamism existing in cybersecurity, i.e., automating the process, whenever possible, and performing it in a scalable, simple, fast, and affordable way for the manufacturers. In addition, being risk assessment and evaluation (or conformity assessment) two independent tasks, a risk assessment of the class of IoT devices in their intended use should be performed to define the requirements of the cybersecurity certification scheme. This is the initial step to define consistent and objective metrics to estimate the risk. Finally, cybersecurity should be reviewed during the whole lifecycle. In this sense, there is also a need for a verification system that checks the security level and a monitoring process to detect those changes, allowing the update of the risk mark.

To address some of these challenges, ECSO has recently developed the Composition Approach[59] that consists of a set of guidelines to reuse evidence from previous certifications and allow a fast certification process. An IoT device is considered an example to show in practice the implementation of the composition approach.

One of the complexities of the Internet of Things is the integration in systems which might require considering other functional standards, such as safety, privacy, and data protection standards, in addition to security standards during the development processes. These considerations should be taken upfront in the certification process. For example, in the industry domain, the components should comply with IEC 61508 for functional safety issues, but should also comply with IEC 62443 to ensure that security activities are considered. From the automotive domain, another example is the compliance with the ISO 21434 for cybersecurity in addition to the safety standards in that domain. There is an emerging need to provide co-engineering activities not only between the safety and the security teams to deal with issues but also with the quality team, who are commonly the ones in charge of standard compliance management.

Having a variety of standards to comply with is not an isolated case. Suppliers need to consider that there are many regulations that must be complied with for different domains (aerospace, rail, energy, etc.) and at a different technical level. In addition, the suppliers should reflect on how an

[57] Certificación Nacional Esencial de Seguridad (LINCE). Available at: https://oc.ccn.cni.es/en/types-of-certification/functional-certification/evaluation-methods-and-criteria. Last accessed: 19 July 2022.
[58] The "Beschleunigte Sicherheitszertifizierung" (BSZ, Accelerated Security Certification). https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Beschleunigte-Sicherheitszertifizierung/beschleunigte-sicherheitszertifizierung_node.html. Last accessed: 19 July 2022.
[59] ECSO. 2020. European Cyber Security Certification: Product Certification Composition. Available at: https://www.ecs-org.eu/newsroom/ecso-publishes-its-product-certification-composition-document. Last accessed: 19 July 2022.

IoT device will be used at system functional level to ensure the correct application of the standards. This translates into potential barriers for the suppliers to enter into new domains. When a supplier is interested in offering his/her product to a different domain, the investment might be high. The supplier might re-certify the products as the standards, the system-level functions, and the authorities may differ. Similarly, the developers should also consider other "norms/regulations" when trying to address different domains at once, because they may impact their input requirements for certification. The European Council has recently stressed the importance of a coherent definition of cybersecurity requirements across directives and legislations to avoid ambiguity and fragmentation[60].

From the research and innovation perspective, some research projects have analysed or have in their roadmap the definition of solutions to certify security but also to ensure the possibility to achieve the reusability of hard/soft components cross domain, such as OPENCOSS, SafeCer, AQUAS, AMASS, and CERTIFY.

4.1.3. Conformity assessment and Certification in the IoT Domain

The complexity of the definition of a unique certification scheme for IoT devices stands in the need to cover their wide spectrum of application. IoT devices provide their functionality as part of bigger systems by interacting with various subsystems. IoT usually operates in uncertain environments, some of which can be categorised in common safety-critical domains. The constituent devices are developed by different stakeholders, who, in most cases, cannot fully know the composing parts at development time. Furthermore, devices and the system of systems integrating IoT components may reconfigure and update themselves during runtime, for instance to face new threats and attacks. The information needed for certification is only available at composition or reconfiguration time. These are just few elements to show the complexity of defining a certification scheme suitable for IoT.

Regarding standardisation and evaluation, the IoT context has attracted a lot of attention. In December 2020, the ETSI TS 103 701 was released, which specifies a conformance assessment methodology for consumer IoT devices, their relation to associated services and corresponding relevant processes against ETSI EN 303 645, addressing the mandatory and recommended provisions, as well as conditions and complements these two ETSI standards. ETSI EN 303 645 describes a standard for cybersecurity on the Internet of Things. This document specifies 13 cybersecurity provisions for IoT devices and services, establishing a security baseline for this kind of products and providing a basis for future IoT certification schemes. This standard is designed to prevent attacks against smart devices, also includes data protection for consumers and will be complemented by the European Telecommunications Standards Institute (ETSI) with the development of a test specification and an implementation guide.

Specifically, for the IoT domain, there are initiatives such as the IoT Security Testing Framework[61] developed by ICSA labs. An IoT system that passes all the test cases is awarded with the ICSA

[60] Council of the European Union. 2020. Cybersecurity of connected devices – Council adopts conclusions. Available at: https://www.consilium.europa.eu/en/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/. Last accessed: 19 July 2022.

[61] ICSA. 2016. Internet of Things (IoT) Security Testing Framework. Available at: https://www.icsalabs.com/sites/default/files/body_images/ICSALABS_IoT_reqts_framework_v2.0_161026.pdf. Last accessed: 19 July 2022.

Labs IoT Certification. The approach is based on a periodic assessment and update of the certification criteria. However, there is not a Mutual Recognition Approach (MRA) for this approach, and the criteria and processes are not standardised. In addition, there are currently few IoT products certified with this approach. CTIA also developed an IoT Cybersecurity Certification Program [62] with the aim of verifying the device security features against a set of standard cybersecurity best practices. The program considers three levels of certification depending on the device and the security characteristics desired or needed for its use.

Another initiative is the Eurosmart IoT Security Certification Scheme (e-IoT-SCS), which focuses only on the Substantial security assurance level defined by the Cybersecurity Act. In particular, this scheme uses the notion of Security Profile (SP) based on the CC to define the security functional requirements and security assurance activities. It follows a risk-based approach, including the demonstration of the absence of publicly known vulnerabilities and also including testing, to demonstrate that IoT Devices implement the necessary security functionalities. From the labelling perspective, researchers from the University of Carnegie Mellon developed a security and privacy label[63] to share some general information regarding security and privacy with consumers in an easy and understandable way.

In an effort towards security evaluation, SESIP (Security Evaluation Standard for IoT Platforms)[64] methodology, currently under standardisation by CEN CENELEC, specifies requirements the requirements for the security evaluation of IoT platforms and parts thereof, including a set of Security Functional Requirements, and the definition of Security Assurance Requirements packages that define five assurance levels. These requirements are based on the Common Criteria standard (ISO 15408, v3.1) and are refined for the specific purpose of the evaluation of IoT platforms and parts thereof.

The Japanese Cyber/Physical Security Framework was created by the Working Group 1 (Systems, Technologies and Standardization) of the Japanese Ministry of Economy, Trade and Industry. This group is focused on the cyber/physical security in the new supply chains under the Society 5.0 policy and the Connected Industries policy. The security framework contains some guidelines for assuring security in supply chains from three different perspectives: Connections between organisations, Mutual connections between cyberspace and physical space and Connections in cyberspace. The document describes the three-layer model structure followed by the framework, a list of risk sources and security requirements to address these risks and some examples of the application of the security measures. This framework represents a high Japanese government effort to improve the security of its products, quite in line with the European initiatives derived from the Cybersecurity Act.

Researchers from the University of Carnegie Mellon[65] developed a security and privacy label to share with consumers in an easy and understandable way some general information regarding security and privacy of IoT devices. For more expert consumers, they include a second layer with more detailed information. Whereas the first layer (non-experts) is intended to be linked to the

[62] CTIA. 2019. CTIA IoT Cybersecurity Certification Program Certifies First Device. Available at: https://www.ctia.org/news/ctia-iot-cybersecurity-certification-program-certifies-first-device. Last accessed: 19 July 2022

[63] Carnegie Mellon University.2020. IoT Security & Privacy Label. Available at: https://www.iotsecurityprivacy.org/. Last accessed:19 July 2022.

[64] GlobalPlatform.2021. Security Evaluation Standard for IoT Platforms (SESIP) v1.0 | GP_FST_070 . Available at : https://globalplatform.org/specs-library/security-evaluation-standard-for-iot-platforms-sesip-v1-0-gp_fst_070/#collapse- Last accessed: 19 July 2022.

[65] Carnegie Mellon University.2020. IoT Security & Privacy Label. Available at: https://www.iotsecurityprivacy.org/. Last accessed:19 July 2022.

product, the second layer can be accessible via a QR code. The information reflected in the label includes security and best practices of smart devices and it was obtained not only from standards and guidelines, but also from studies and interviews with security and privacy experts from industry, academia, government and public policy organisations.

From the previous analysis, there is not a silver bullet certification scheme that copes with the requirements associated to the IoT paradigm. IoT cybersecurity certification sets out unique challenges that must be addressed through the current schemes by adapting the certification process accordingly. On the one hand, IoT is currently realised through a fragmented landscape of technologies and protocols that in some cases are not standardised. Consequently, the certification process must deal with heterogeneous systems and devices. On the other hand, the heterogeneous nature and abundance of IoT requires lightweight and flexible approaches that are able to provide an effective and efficient certification approach throughout the lifecycle of such components. Furthermore, privacy aspects should be considered since IoT systems could handle sensitive data, and they will be often managed by non-expert users.

4.2. Lifecycle approach

Risks must be managed throughout the complete lifecycle of a product. Cybersecurity is itself a dynamic concept. Indeed, at the end of the design phase or after a cybersecurity certification process, a product can be considered secure, but this condition could change during its life cycle. A security change caused by an update, a patch or a new vulnerability can put the system in check, requiring immediate action to avoid bigger damages. Therefore, security management is crucial to guarantee the security of the entire system, not only during the installation of the device on the network, but also throughout its entire life cycle.

The approved CSA in Europe explicitly mentions security management during the life cycle of a device as a fundamental tool of security management, and it also references to Regulation (EC) No 765/2008[66] and Decision No 768/EC[67], which includes the market surveillance throughout the product's lifecycle. ENISA has also released a set of guidelines with a particular focus on securing the Software Development Lifecycle[68] and on the IoT Supply chain[39], including a summary of the most relevant and applicable standards. The intent is to help IoT manufacturers, developers, integrators and in general all stakeholders involved in the IoT supply chain to build and deploy secure IoT technologies and serve as a reference point for a secure IoT supply chain. Moreover, ENISA has also issued other documents, e.g., regarding IoT security in critical infrastructures[69].

There are also several security standards and frameworks focused on risk management during the life cycle of a system. Some of the best known are the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) supporting the Federal Information

[66] EUR-Lex. 2008. REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93. Available at : https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF. Last accessed:19 July 2022.

[67] EUR-Lex. 2008. ECISION No 768/2008/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0768&from=EN. Last accessed 19 July 2022

[68] ENISA. 2019. Good Practices for Security of IoT - Secure Software Development Lifecycle.Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1. Last accessed: 19 July 2 2022.

[69] ENISA. 2017. Baseline Security Recommendations for IoT. Available at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot Last accessed 19 July 2022.

Security Management Act (FISMA), the International Standards Organization (ISO) 31000 series, addressing risk management standards, or Security lifecycle SANS management. Such frameworks generally include the following phases or activities: i) requirements definition/ specifications, ii) assessment, iii) configuration or deployment and iii) maintenance / monitoring and management. Although all the processes are described, none of the frameworks provides an explicit instantiation through specific techniques and methodologies.

4.2.1. Risk Assessment and Risk Classification

A starting point for the manufacturer of IoT Devices and Services is an associated risk assessment. Evaluated risks result in certain risk classification of the IoT device, The context in which the device will operate during its life cycle, or the nature of the data to be managed, are also important factors that determine the security level required in those contexts.

Evaluated risks must be mitigated through the implementation of various cybersecurity features reducing those risks to an acceptable risk level associated with the risk classification.

The risk classification can also be mapped to a certain assurance level. As an example, the European Cyber Security Act (CSA) defines 3 Assurance levels (basic, substantial, high) which also take different risks into account. Other examples are the Trust Assurance Levels (TAL) defined by the Car 2 Car Communication Consortium (C2C-CC), the security levels of the HEAVENS approach, or the Automotive Safety Integrity Level (ASIL) levels defined within the ISO 26262 standard.

Currently, such risk assessments and impact assessments requested by e.g., current European Directives applicable to products like the Radio Equipment Directive (RED) or General Product Safety Directive (GPSD), focus on the intended use only. Unfortunately, attackers are less interested in the intended use, and are more interested in the non-intended use to make use of vulnerabilities for their cyberattacks.

Manufacturers are used to risking assessments related to safety by looking at the functionalities of the device related to the intended use. Risks associated with cybersecurity require cybersecurity expertise not necessarily available at HW and SW developers dealing with the functionality of the device. Mitigating cybersecurity risks require cybersecurity expertise related not only to the functionality associated to the intended use, but also to taking the non-intended use into account.

While there are many standards and mechanisms available for Risk Assessments, each of them uses different metrics and procedures, and some of them are complex, requiring plenty of formal documentation. Consequently, this makes the comparison of different devices and systems more complex. In this sense, a “Guiding document on the Risk Classification of IoT devices” for manufacturers and operators could be valuable.

4.2.2. Market Surveillance

Market surveillance as part of Regulation EC 765/2008 and Decision 768/2008/EC is an important task after the manufacturer puts a product to the market. Indeed, the manufacturer is obliged to monitor the use and behaviour of his/her products in the market, which includes the obligation to check whether a product can potentially harm citizens.

A pre-requisite before putting a product to the European market is to run a conformity assessment based on the principles of the New Legislative Framework (NLF) to assess whether the product

might cause harm to citizen. Several European Directives, such as the Radio Equipment Directive (RED), are about to add mandatory harmonised baseline requirements related to cybersecurity as part of the product's conformity usually evaluated in a product conformity assessment.

In case of connected products, there are different possibilities to generate harm to people, whether it is about putting people's life, assets, or privacy at risk, all multiplied with a certain probability. The manufacturer needs to reduce immediately such possible harm to citizens and take actions accordingly. Such action might include the reduction of an IoT device's field functionality until the problem can be solved (e.g., via firmware or software update), or even ask to return the product for further refurbishment or change. This process is supported by the European RAPEX system [70] to reach citizen using such dangerous non-food products, but cannot be addressed personally.

The European Cyber Security Act (CSA) offers certification schemes to demonstrate the proper implementation of cybersecurity features into products, services and processes always taking published vulnerabilities into account.

Conformity Assessment Bodies (CABs) accredited by National Cybersecurity Certification Authorities (NCCA) are able to run conformity assessments for devices, services and processes whenever a third-party conformity assessment is imposed or recommended. Certificates like CE marks or labels demonstrate the responsible behaviour of the manufacturer on their go-to-market approach. Market surveillance mechanisms support the customer confidence in the safety and cybersecurity through the product's lifecycle. From a legislative approach, a Horizontal Regulation is currently under development by the European Commission to address the lifecycle approach related to IoT devices and services.

Threat intelligence sharing and vulnerability disclosure in relation with IoT devices is another important task. It can be part of the Market surveillance that the manufacturer (or importer) should perform in relation to a continuous risk assessment during the complete product life cycle.

New services such as IoT Device Vulnerability Database Services (as described in more detail below) will support users of IoT devices and related services in their own continuous risk assessment and impact assessment related to their networks and assets.

Participation in threat intelligence programs support not only CISOs, allowing them to receive information about vulnerabilities at an early stage, but also share such information in a responsible manner. Many countries and Member States have related frameworks either already in place or in preparation. The OECD recently published a guidance document on responsible vulnerability disclosure[71] supporting policy makers in the preparation of this important activity.

4.2.3. Vulnerability and Attack Repository for IoT

The IoT cybersecurity data landscape is extremely fragmented, with different data formats and gaps in available information. This makes the cost of obtaining data for all interested entities very high. As a consequence, it contributes to insufficient care for the security of IoT devices.

The multitude of existing vulnerabilities, the lack of common knowledge about them, and weak patching processes pose a serious threat to both the security of citizens and the economy. Infected

[70] European Commission. 2022. Safety Gate: the EU rapid alert system for dangerous non-food products. Available at: https://ec.europa.eu/safety-gate-alerts/screen/webReport. Last accessed: 19 July 2022;
[71] OECD. 2021. Encouraging vulnerability treatment: Overview for policy makers. Available at: https://www.oecd-ilibrary.org/science-and-technology/encouraging-vulnerability-treatment_0e2615ba-en Last accessed 19 July 2022.

IoT devices can be used for distributed attacks on other services and digital resources. Solving the above issues is difficult due to the lack of rich common sources or useful information on IoT vulnerabilities and known exploits. Services providing information about vulnerabilities and exploits are important for vendors and service providers to develop services and products with increased security for end users. Obtaining such information is also important from the point of view of national and sectoral CSIRTs (Computer Security Incident Response Team). However, although current databases (e.g., the National Vulnerability Database (NVD) in the U.S) include vulnerabilities associated with IoT, there is a lack of a common vulnerability database with a strong focus on IoT to facilitate risk analysis tasks in Europe.

All of the above indicates that it is extremely advisable to have a database of information about vulnerabilities and exploits on the Internet of Things. For this reason, the VARIoT project (Vulnerability and Attack Repository for IoT, https://www.variot.eu) was initiated, resulting in the creation of a repository of information on vulnerabilities and exploits in IoT devices. This repository has been published on the https://www.variotdbs.pl/ website, where information about vulnerabilities and exploits related to IoT devices (aggregated from many sources) can be found. Data is also easily accessible through an API, which utilises well-structured JSON and JSON-LD format. The *variotdbs* website also provides news about the security of IoT devices. News is selected with a solution based on Natural Language Processing (NLP) and Artificial Intelligence (AI). The developed mechanisms are able to obtain information from unstructured sources, such as blogs and articles. Additionally, *variotdbs* website calculates trust in selected news for a better relevancy assessment. The repository is also publicly available via data.europa.eu and the Polish open data portal https://dane.gov.pl/en.

4.3. Areas for policy discussion

Inspired by the material from the Internet Society[72], this section discusses some issues that would benefit from policy intervention.

Accountability should be strengthened by providing well-defined responsibilities and consequences for inadequate protection of IoT devices. For this reason, it is crucial to assign liability, strengthen consumer protection and ensure legal certainty. GDPR introduces such accountability principles in EU legislation, but only concerning data protection. The whole field of legal liability in case of harm to humans or a property is still mostly empty, even though the European Commission has started addressing the issue, for instance, with its staff working document published in the framework of its communication on AI[73]. In the above, the Commission states that “emerging digital technologies, such as IoT, AI-powered advanced robots and autonomous self-learning systems, must meet the essential health and safety requirements laid down in the applicable EU safety legislation”.

Incentives should be increased or created to invest in security, for instance, by encouraging credible security certification schemes and promoting independent reviews and ratings, including from users. In this respect, the Cybersecurity Act is paving the way toward such incentives.

[72] Internet Society. 2018. IoT Security for Policymakers. Available at https://www.internetsociety.org/wp-content/uploads/2018/04/IoT-Security-for-Policymakers_20180419-EN.pdf Last accessed 19 July 2022.

[73] Commission staff working document Liability for emerging digital technologies, Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial intelligence for Europe, April 2018.

A culture of security among IoT stakeholders should be fostered, and this should be applied during all stages of the product lifecycle, including design, production and deployment. To achieve this goal, stakeholders should think of "Systems" security, which should include the backend, often out of the users' control. In addition, security risk analysis should be promoted, along with best practices and guiding principles. Crucially, protections for security researchers must be part of the legal framework. Here again, the Cybersecurity Act may contribute to this landscape, because a number of amendments proposed by the European Parliament promote Coordinated Vulnerability Disclosure, as envisaged in a report by the CEPS think-tank.[74]

Strong market incentives should be used for better security practices. These include public procurement practices for IoT, consumer education, a greater role for consumer groups and partnerships with the insurance industry, among others.

Technology and vendor neutral solutions should be fostered. Security solutions should not be based on specific technical standards or vendor products, but instead based on desired outcomes, such as better security, privacy and interoperability. Accordingly, policies and procurement requirements for IoT security should specify outcomes, not methods, while data portability should be encouraged. Here again, GDPR sets some guidelines for the desired outcomes.

International cooperation will bring economies of scale to IoT security. As the Department of Homeland Security (DHS) stated: "IoT is part of a global ecosystem, and other countries and international organisations are beginning to evaluate many of the same security considerations. It is important that IoT-related activities not splinter into inconsistent sets of standards or rules." [75]

But above all, **smart use of any policy or regulatory tools must be ensured**. As security is expensive and users may have difficulty recognising or valuing security, policy and legislation have an important role to play in shaping security practices in the IoT industry. Policies should be developed with the goal of influencing the IoT ecosystem to promote better security practices, rather than mandating specific technical solutions. Therefore, policies and regulations should be developed in a transparent manner and prioritise the interests of users. Regulating by industry sector may lead to better outcomes because IoT systems are developed and used in a wide range of industry sectors and applications that have different constraints and requirements.

[74] Software Vulnerability Disclosure in Europe: Technology, Policies, and Legal Challenges. L Pupillo, A Ferreira, and G Varisco. Centre for European Policy Studies (CEPS), June 2018.
[75] U.S. Dept. of Homeland Security. 2016. DHS Releases Strategic Principles For Securing The Internet Of Things. Available at: https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-internet-things#:~:text=The%20principles%20focus%20on%20the,ecosystem%3B%20and%20connecting%20carefully%20and Last accessed 19 July 2022.

5. Recommendations and Conclusions

This section discusses the research and innovation efforts that should be prioritised over the following 5-7 years in Europe to deliver a more secure Internet of Things. When building such a vision one must consider the highly dynamic nature of both the IoT and the cybersecurity domains worldwide. Rather than providing specific priorities with defined timelines, several general recommendations are presented to serve as a basis for further discussion.

The Interplay between regulation, certification, and technology:

- Regulations that are currently being developed must consider the state of play and foreseen directions of IoT security technologies. IoT cybersecurity providers should be involved during the development phases of new regulations and future certification schemes.
- There is a need to progress in the development of and adoption of common criteria, common practices, and standards at all levels, from risk classification guidance and related built-in security capabilities of IoT devices, to end-to-end IoT security.

Developing and maturing IoT cybersecurity technologies:

- At the technological level, there is a clear need for significant investments in the development, maturing and progressing of the market readiness of many different technological tools, capabilities, and solutions. Section 3 provides a detailed overview of the most important challenges foreseen and the corresponding technological needs.
- Demonstration (at lower TRLs) not only to test technical capabilities or regulatory compliance but also to raise awareness among stakeholders (for example, industrial end-users across different verticals, citizens, governments, and critical infrastructure operators).
- Pilots (at higher TRLs) as an adequate tool not just to validate (higher TRL) technology, but mainly to provide early market validation and user acceptance of cybersecurity solutions, standards, or common practices. Mid and large-scale piloting exercises are also an invaluable source of evidence and input to policymakers and regulators, as they provide an advanced glimpse of what is expected to happen in the near future at all levels.

A pervasive cyber-insecure IoT calls for generous multi-stakeholder effort:

- The road to a (European) cyber secure IoT calls for a joint effort among many parties. In our vision, all stakeholders must have their share of effort and responsibility in the progress towards the future cyber secure IoT.
- Technology experts (market players providing cybersecurity solutions, universities, RTOs), IoT supply chain actors (from device to platforms and applications), end-users (vertical industries, citizens, critical infrastructure operators), policymakers and governments, all of them must be involved adequately during the process.
- In this sense, ECSO represents the adequate stakeholder ecosystem where all types of actors meet thus providing the perfect conditions to accelerate.

6. Glossary

CoAP: Constrained Application Protocol

DoS: Denial of service, a type of cyberattack

DDoS Attack: Distributed denial-of-services attack.

eIDAS: electronic identification, authentication and trust services

ICT: Information and communication technologies

GDPR: General Data Protection Regulation

IoT: Internet of Things

LoRa: Long range digital wireless

MPC: Multi-party computation

MQTT: Message Queuing Telemetry Transport

NB-IoT: Narrowband IoT

OTA: Over the air

RFID: Radio-frequency identification

SDN: Software-defined network

SIEM: Security information and event management

Sigfox: A proprietary low-power wide-area network protocol.

Acknowledgments

The European Cybersecurity Organisation's (ECSO) WG6 aims to contribute to define the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem. From the analysis of the challenges of digitalisation of the society and industrial sectors this WG identifies what are the capacities and capabilities to sustain EU digital autonomy by developing and fostering trusted technologies.

The following is a special acknowledgement of the active contributions in various capacities from ECSO WG6 members.

EXPERT CONTRIBUTIONS: Jason Mansell (TECNALIA), Afonso Ferreira (CNRS), Ana Maria Merino Aguado (ICE-Castilla y Leon), Angela Nicoara (HSLU), Anna Felkner (NASK), Antonio Skarmeta (University of Murcia), Boutheina Chetali (Huawei), Costanza Pestarino (ECSO), Csaba Virág (Talgen), Franco Callegati (University of Bologna), Giorgio Giacinto (CINI), Guillaume Têtu (ANSSI), Herve Debar (IMT), Jacques Kruse-Brandao (SGS), Janusz Pieczerak (ORANGE), Javier López (University of Malaga), Jeroen Doumen (Sandgrain), Konstantinos Votis (CERTH/ITI), Manuel Lianos (NXP), Marcos Álvarez (Gradiant), Massimiliano Rak (CINI), Matthias Hiller (Fraunhofer), Mikel Uriarte Itzazelaia (S21SEC), Nouha Oualha (CEA), Philippe Massonet (CETIC), Roberto Cascella (ECSO), Roland Atoui (RedAlert Labs), Sara Matheu (University of Murcia)

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU