Internet of Things

Sébastien Ziegler *Editor*

Internet of Things Security and Data Protection

Springer

Internet of Things

Technology, Communications and Computing

Series editors

Giancarlo Fortino, Calabria, Italy
Antonio Liotta, Eindhoven, The Netherlands

More information about this series at http://www.springer.com/series/11636

Sébastien Ziegler
Editor

Internet of Things Security and Data Protection

Springer

Editor
Sébastien Ziegler
Mandat International
Geneva, Switzerland

ISSN 2199-1073 ISSN 2199-1081 (electronic)
Internet of Things
ISBN 978-3-030-04983-6 ISBN 978-3-030-04984-3 (eBook)
https://doi.org/10.1007/978-3-030-04984-3

Library of Congress Control Number: 2018968445

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

About this Book

The Internet of Things (IoT) is disruptively shifting the paradigm of cybersecurity, privacy, and data protection toward new territories. With tens of billion connected devices, the information gathering is becoming omnipresent and deeply pervasive. Simultaneously, networks are becoming exposed to new threats with an unprecedented surface of risk.

The security risks associated with IoT systems are extremely challenging to overcome given the highly dynamic nature, heterogeneous nature of hardware, global connectivity, changing parameters, and wide accessibility. These factors often result in IoT ecosystems being physically unprotected and susceptible to manipulation by external parties. As such, there are a number of security threats that can affect IoT "objects." These threats include attacks targeting diverse communication channels, denial of service, physical threats, eavesdropping, and identity fabrication among others.

In view of these challenges, this book intends to provide an overview of complementary approaches, methodologies, and tools to better protect IoT infrastructures and personal data. It leverages recent research results from research projects. It has been made possible thanks to contributions from various international experts and research teams. Our acknowledgments go more specifically to the following European research projects: Privacy Flag, ANASTACIA, Synchronicity, U4IoT, SAINT, F-Interop, IoT Lab, and IoT6.

Contents

List of Figures

List of Tables

Chapter 1
Internet of Things Cybersecurity Paradigm Shift, Threat Matrix and Practical Taxonomy

Sébastien Ziegler

1.1 Cybersecurity Threats Taxonomy for the Internet of Things

In order to categorise and profile the various cybersecurity threats posed by the emergence of the Internet of Things, we start by differentiating the network into four areas or segments as illustrated by the following Fig. 1.1.

The four areas are defined as follows:

P **The Personal Area Network** (PAN) usually connects most Internet of Things devices. The PAN may use IP protocols such as 6LoWPAN and non-IP protocols such as ZigBee, KNX and EnOcean. In both cases, the PAN is usually connected to the LAN (or directly to the WAN) through a gateway or border router.

L **The Local Area Network** (LAN) usually interconnects the company equipment including computers, printers and servers. Most of the time, the LAN is protected from the WAN by a firewall.

W **The Wide Area Network** (WAN) is accessible to everyone including, obviously, black hat hackers. To keep the model simple and easily manageable, we will assume that the WAN describes any large network that is shared by many users, such as the cellular network.

C **The Cloud and Remote Servers** gather online resources and services. While these resources may be accessible to the public, they are always under the control of a specific entity with specific security policies. Despite the fact that not all companies are using such resources, they're sufficiently common to be included as a basic segment. We can also include public servers of companies and their DMZ areas as part of this category.

S. Ziegler (✉)
Mandat International, Geneva, Switzerland
e-mail: sziegler@mandint.org

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_1

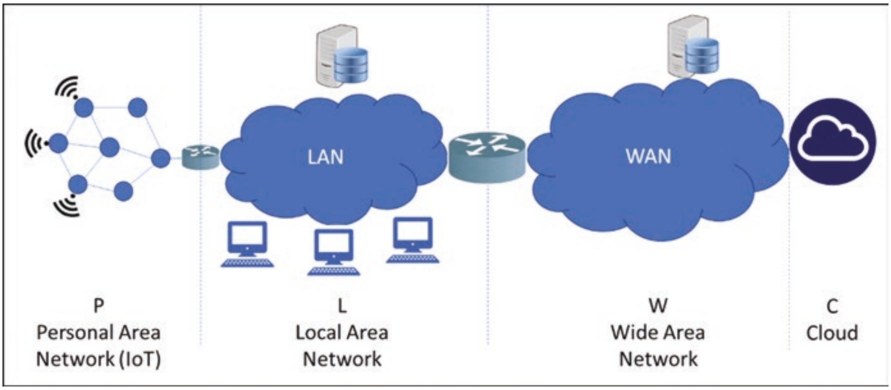


Fig. 1.1 Network segmentation

We can start using these four segments and their corresponding short notation (P, L, W and C) in order to categorise patterns of attack. We will specify for each attack:

– The source of the attack: the segment of the network used by the hacker to enter and access the network.
– The destination of the attack: the segment of the network that is targeted by the attack.

By identifying and specifying the source of each category of attack and its ultimate target, we can differentiate several profiles and patterns. For instance, a hacker trying to remotely access a company's private server is performing a WAN-to-LAN attack or "WL" attack. If he is intending to hack a public server or service, it would be a WAN-to-cloud attack or "WC" attack. If the attack is more complex, for instance, a hacker remotely attacking IoT devices in order to launch a distributed denial of service (DDoS) attack on the public server of a company, the attack can be noted as WAN-to-PAN-to-cloud or a "WPC" attack.

A second axis of categorisation relates to the intention behind the attack, i.e. the intended impact pursued by the hacker. We will segment the attacks in four categories:

A **Access of information**: where the hackers only look to access private information without intending to impact the information's accessibility by the legitimate owner(s) and by usually adopting strategies that hide any trace of such access.
B **Temporarily disrupt activity (or create bother)**: where the hackers intend to disrupt accessibility to information by the legitimate owner(s) or their customers/clients.
C **Change code, files or information**: where the hacker intends to modify code, data or files belonging to their target. Such attacks may have a deeper, long-lasting impact on the target's information management system.

Table 1.1 Possible impact levels

A	Access	Read	Access information
B	Bother	Post	Temporarily disrupt activity
C	Change	Write	Modify key code or information
D	Destroy	Delete	Destroy the target

D **Destroy the target**: where the hacker intends to attack the core capabilities of the target. Such attacks are likely to emerge in the case of ransomware, economic competition or warfare.

These four categories are summarised in the following Table 1.1.

1.2 Traditional Cybersecurity Threat Matrix

If we look at traditional network hacking, it relies on two main entry points: the WAN and the LAN. The main targets are usually the LAN and the cloud.

As depicted in Fig. 1.2, traditional attacks usually follow WL and WC categories of attack when performed by remote hackers, as well as LL attacks from hackers who can physically access the targeted LAN or manage to successfully use a bring your own device (BYOD) exploit by infecting the device of an employee (e.g. a compromised USB dongle or smart phone). Other patterns of attack exist, but they appear to be less prevalent. The following matrix summarises the traditional threat matrix where the deep blue cells represent the main risks:

1.3 Internet of Things Cybersecurity Paradigm Shift

The Internet of Things is triggering a major paradigm shift in terms of cybersecurity threats for several reasons:

1. **Scalability and surface of risk**: With an expected 50 billion plus connected devices, Internet of Things deployments will be massive. It will substantially extend the surface of risk and increase the likelihood that a hacker will find a weak point. Moreover, it will become a very attractive target for launching massive DDoS attacks.
2. **Energy and computing constraints:** Internet of Things devices are often constrained devices. The prime concern for Wireless Sensor Networks (WSN) technology is energy-saving (and energy-harvesting when applicable). This leads to simplified code and protocols in order to minimise computing processes and related energy consumption. Such constraints directly impact the security enablers and solutions deployed on such devices and networks.

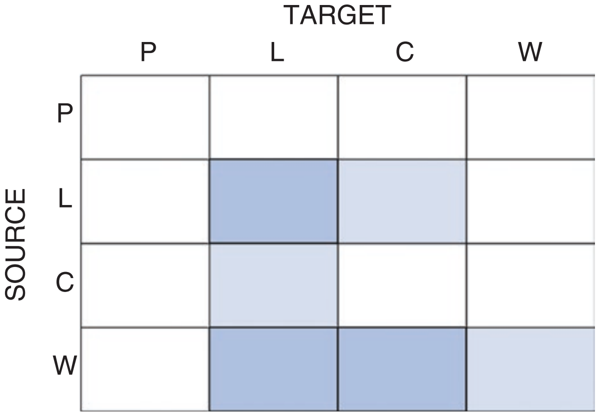


Fig. 1.2 Traditional cybersecurity threat matrix

3. **Physical accessibility:** Internet of Things devices are deployed in diverse environments including publicly accessible areas. A CCTV camera is expected to increase a company's security, but it also constitutes an easily accessible entry point to the network of the same company; certainly more easily accessible than a server located in a secured room with adequate access control.
4. **Protocol communication heterogeneity and weaknesses**: Internet of Things devices often rely on specific communication protocols, which can be categorised in two main groups:

   (a) IP-based IoT protocols such as 6LoWPAN, CoAP and 6TiSCH, which have been optimised for constrained networks. These protocols tend to use asymmetric communication models, based on UDP, in order to save bits and associated energy consumption. Despite important progress achieved by the IETF community, there is an unavoidable trade-off and cost in terms of security and reliability.
   (b) Non-IP IoT protocols such as ZigBee, KNX, BACnet and EnOcean to name a few. Such protocols have been designed and optimised to address specific application domain requirements. They bring a discontinuity in the network deployment between IP-based and non-IP-based network segments. They may also carry specific weaknesses, in particular when the data transmission on the PAN is asynchronous and unencrypted.

5. **Manageability and the human factor**: As a direct effect of the massive scale and heterogeneity of Internet of Things deployments, the manageability of networks is becoming a growing issue. It constitutes a challenge for chief information security officers (CISOs) and for network engineers to secure larger and more eterogeneous networks. They will be less likely inclined to adopt individual and differentiated passwords for each individual Internet of Things device,

as they would for a server. Hence, we can add the human factor, which may exacerbate any potential weaknesses of Internet of Things networks.

6. **Cognitive bias**: There is also a misperception and underestimation of the risks related to Internet of Things deployments. Internet of Things devices are too often perceived as simple and dumb and not containing strategic information. It is a serious misinterpretation if you consider that Internet of Things devices are connected to the network of the company and constitute new access points that are often physically accessible to outsiders with a lower level of security in terms of authentication and encryption.

As a consequence, Internet of Things deployments are becoming very attractive targets as new entry points and resources for hackers and new attack patterns have emerged. We can highlight two new families of threat that are enabled by the Internet of Things, as follows.

1.3.1 Internet of Things Proxy Attacks

Internet of Things proxy attacks use Internet of Things deployments as either entry points or as resources with which to perform attacks on other targets. We will focus on two major patterns:

1. **IoT-based DDoS:** Internet of Things deployments can be used as resources to launch DDoS attacks by following a WPC pattern. Hackers find ways to access Internet-connected devices to compromise them and use them as proxy to launch massive attacks against public servers or other online services. The objective is usually to disrupt the targeted online service (B level).
2. **IoT entry points:** The other Internet of Things proxy attack that should be carefully considered is the use of Internet of Things devices to access the private network and information of a company. Such attacks follow a PL pattern and can support the whole range of possible impacts, from access (A level) to temporarily disruption (B level), to code and file modification (C level), to destruction (D level). In such a context, a proper network plan with adequate security configuration should be considered and will be discussed further in the chapter on IPv6 IoT security.

1.3.2 Internet of Things Target Attacks

Considering the growing importance of the Internet of Things in monitoring and managing our environment, it is now a meaningful target for hackers. It can be driven by the intention to disrupt the IoT system itself, for instance, when a hacker tries to compromise traffic lights, smart grids or sirens in a city. It can also be a means to neutralise the security system of private premises.

We can categorise such attacks into three main groups:

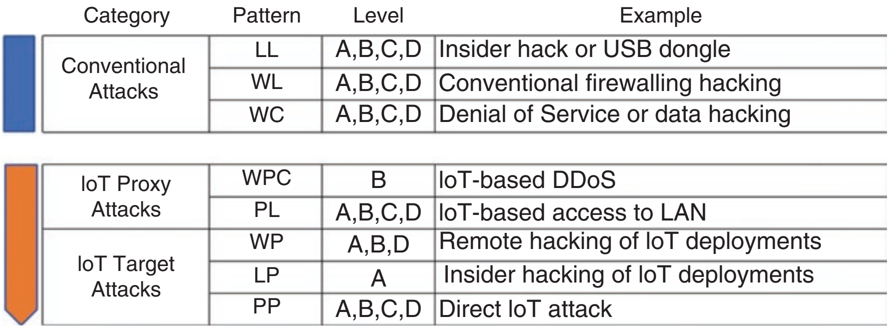
1. **Remote Attack on Internet of Things:** Such attacks follow a WP pattern of attack that may intend to access data from the deployed Internet of Things (A level), temporarily disrupt the Internet of Things network (B level) or destroy such a network (D level).
2. **LAN-Based Attack on Internet of Things:** Similarly, attacks may follow a LP pattern that may intend to access data from the deployed Internet of Things (A level), temporarily disrupt the Internet of Things network (B level) or destroy such a network (D level).
3. **Direct PAN Attack on Internet of Things:** Attacks may follow a PP pattern by directly accessing an Internet of Things device in order to compromise the whole set of interconnected devices. Such attacks may be openly hostile and can cover a wide range of objectives, from accessing data from the deployed Internet of Things (A level) to temporarily disrupting the Internet of Things network (B level), changing the code of the device (C level), up to destroying the Internet of Things network (D level).

The previously mentioned emerging patterns of attack can be summarised in the following Table 1.2.

1.4 New Cybersecurity Threat Matrix

The emergence of these new patterns significantly impacts our matrix of cybersecurity threats. The following diagram highlights the extension of the threats domain with the yellow cells highlighting the change and impact of Internet of Things-related threats on the cybersecurity environment (Fig. 1.3).

Table 1.2 Emerging attack patterns



Category	Pattern	Level	Example
Conventional Attacks	LL	A,B,C,D	Insider hack or USB dongle
	WL	A,B,C,D	Conventional firewalling hacking
	WC	A,B,C,D	Denial of Service or data hacking
IoT Proxy Attacks	WPC	B	IoT-based DDoS
	PL	A,B,C,D	IoT-based access to LAN
IoT Target Attacks	WP	A,B,D	Remote hacking of IoT deployments
	LP	A	Insider hacking of IoT deployments
	PP	A,B,C,D	Direct IoT attack

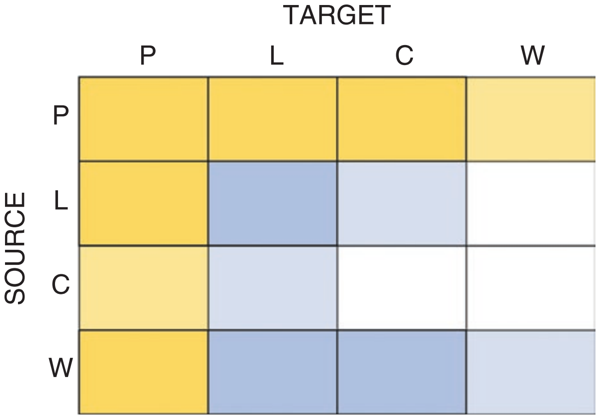


Fig. 1.3 Cybersecurity threat matrix: evolution with the Internet of Things

1.5 Conclusion

The above described taxonomy intends to highlight the main changes regarding cybersecurity threats with the emergence of the Internet of Things. Such an evolution requires the revision of existing cybersecurity models, increased awareness and improved understanding and construction of measures for these new risks. A cornerstone lies in our ability to better organise, segment and monitor a company network with internal firewall strategies. The concomitant transition from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6) constitutes a strong and strategic enabler, not only to address network scalability and get rid of Network Address Translation (NAT) but also as a powerful enabler for simplifying and homogenising network plans and management with stronger security policies.

Chapter 2
Privacy and Security Threats on the Internet of Things

Sébastien Ziegler, Cédric Crettaz, Eunah Kim, Antonio Skarmeta, Jorge Bernal Bernabe, Ruben Trapero, and Stefano Bianchi

2.1 New Perspective on Protection of IoT Systems

The heterogeneous, distributed and dynamically evolving nature of cyber-physical systems (CPS) based on the Internet of Things (IoT) and on virtualised architectures introduces new and unexpected risks that cannot always be solved by current state-of-the-art security solutions. New methodological and technical approaches are thus required to:

1. Incorporate security and privacy into the ICT system at the outset.
2. Adapt to the changing security and privacy conditions.
3. Reduce the need to fix flaws after the deployment of the ICT system.
4. Provide the assurance that the ICT system is secure and trustworthy at all times.

Currently, trustworthiness of complex CPS is substantially based onto two (complementary) pillars: cybersecurity on one side and privacy on the other side (as illustrated in Fig. 2.1).

Since the pervasiveness of interconnected devices is rapidly growing, both solution providers/developers and end users must in fact be ensured that ICT systems

S. Ziegler (✉) · C. Crettaz
Mandat International, Geneva, Switzerland
e-mail: sziegler@mandint.org

E. Kim
Device Gateway, Lausanne, Switzerland

A. Skarmeta · J. B. Bernabe
University of Murcia, Murcia, Spain

R. Trapero
ATOS Research, Madrid, Spain

S. Bianchi
Softeco Sismat, Genova, Italy

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_2

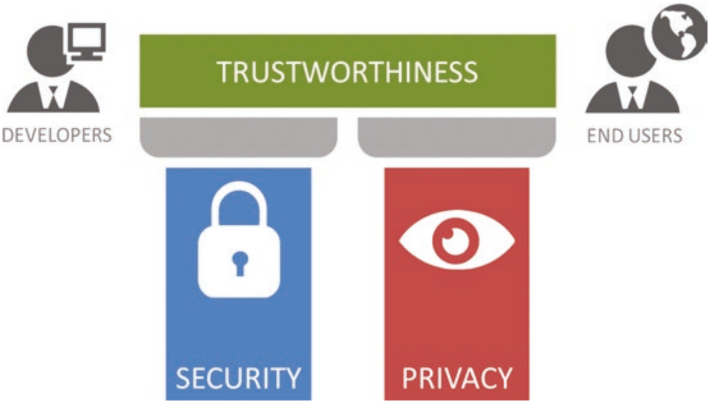


Fig. 2.1 Trustworthiness, security and privacy

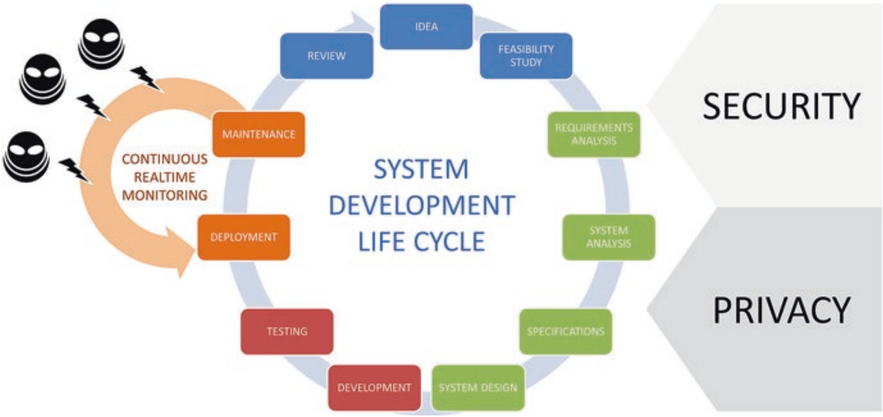


Fig. 2.2 Pervasiveness of security and privacy within the system development life cycle

are secure and compliant with the legislation in force, throughout all the phases of the ICT system development life cycle (SDL), i.e. from design phase up to the deployment and maintenance (Fig. 2.2).

On the practical side, the complexity of the CPS requires a holistic approach that takes into consideration needs, perspectives and constraints at different levels. The application of modern technologies to IoT domain (such as networking ones—software defined networking (SDN) and network function virtualisation (NFV), to name a few) to improve cybersecurity might in fact take into consideration not only the effective enforcement of security policies but also a rigid compliancy with, e.g. privacy constraints (in the light of the new EU General Data Protection Regulation).

Securing CPS based on IoT is not only a priority for the sake of end users and stakeholders but is also an interesting business prospect. In this regard, it was noted that the panel of over 5500 experts interviewed by the authors of the Global

Opportunity Report 2017 [1] ranked “intelligent cybersecurity” as the third major market opportunity in 2017, in relation to global risk “cyberthreats”.

Global risks
(a) Unstable regions
(b) Soil depletion
(c) Rising inequality
(d) Cities disrupted by climate change
(e) Cyberthreats
Market opportunities
(f) Smart water tech
(g) Knowledge for peace
(h) Intelligent cybersecurity
(i) Business of power
(j) Keeping our soils alive
(k) Moisture tech
(l) Behavioural biometrics
(m) Internet of people
(n) Living on air
(o) Gender equality
(p) Cybersecurity game
(q) Instant refuge
(r) Upgrading informal housing
(s) Conflict-free natural resources
(t) Clever codes disrupt inequality

Supporting the holistic approach introduced above, also Gartner [2] points out that “the evolution of the intelligent digital mesh and digital technology platforms and application architectures means that security has to become fluid and adaptive”. Security by design and privacy by design must definitively become a mantra in the ICT domain, with “security teams working with application, solution and enterprise architects to consider all relevant aspects early in the design of applications or IoT solutions”. In any case, multilayered security and privacy approaches, possibly supported by a focused use of behaviour analytics, will foster the take-up of security-oriented solutions in almost any application domain. Forrester [3] predicts that hackers will continue using IoT devices to promulgate large DDoS attacks and that the scale of IoT breaches will definitively increase in size and impact: “When smart thermostats alone exceed one million devices, it’s not hard to imagine a vulnerability that can easily exceed the scale of other common web vulnerabilities […] especially if multiple IoT solutions include the same open source component”.

Forrester includes fleet management in transportation, security and surveillance applications in government, inventory and warehouse management apps in retail and industrial asset management in primary manufacturing among the biggest potential targets. This assessment also accounts for how threats are not actually limited in scope. Along with the notification of large DDoS attacks and severe IoT breaches, the overall demand of expertise in cybersecurity is also steadily increasing, as demonstrated by recent market surveys:

- The overall cybersecurity market is expected to grow from $75 billion in 2015 to $170 billion by 2020 (+125%).
- Millions of cybersecurity jobs are unfilled, with related job postings up ~75% over the past 5 years:
  - Cisco puts the global figure at 1,000,000 cybersecurity job openings.
  - According to Symantec, demand is expected to rise to 6,000,000 globally by 2019, with a shortfall of 1,500,000.

As demonstrated by several initiatives at EU level—e.g. the recent proposal for setting up a EU Cybersecurity Agency and a communitarian certification framework—cybersecurity is a fresh and urgent topic in the digital agenda. Any activity—including edge research projects—that promotes proper behaviour, develops innovative holistic approaches in security (and concurringly privacy) management and delivers innovative technology that improves the way threats are detected and mitigation actions are implemented is obviously of pivotal relevance, with potential large social impact on everyday life (considering the pervasiveness of IoT and of connectivity).

Among many technical goals for securing IoT and promoting its compliance with the upcoming GDPR, it is worth mentioning that to generally improve the level of cyber resilience in distributed architectures such as those of CPS, it is necessary:

- To provide end users with intuitive and user-friendly tools and solutions to model, configure, enforce and monitor policies governing both security and privacy in decentralised and virtualised architectures.
- To leverage complementary (e.g. networking and smart object communications) technologies and advanced functionalities to allow easy deployment of security solutions for highly connected CPS that include IoT.
- To design, implement and maintain virtuous plan-do-check-act (PDCA) processes supporting the whole system development life cycle (SDLC) through the definition of security and privacy policies, their enforcement, the monitoring of the CPS architecture and the definition and deployment of proper mitigation plans against detected attacks.
- To develop technologies able to support security/privacy labelling and certification frameworks.[1]

To reach the aforementioned goals, several technologies can be leveraged to secure IoT: IoT network security, IoT authentication, IoT encryption, IoT PKI, IoT

[1] As suggested by analysts, most vendors will soon start applying for certifications for their product portfolios.

security analytics, IoT API security, etc. Among the main challenges to be faced using these technologies, it is important to highlight that:

1. As demonstrated by recent successful cyberattacks, many IoT devices lack basic security requirements. This highlights that IoT security necessarily requires an **end-to-end holistic approach**.
2. The large number of IoT de facto standards and protocols—which depict a largely immature domain—potentially creates **security blind spots**. This highlights that standardisation at the relevant level should be effectively pursued.
3. The scale and scope of IoT deployments hinder **visibility into security incidents**.
4. Notwithstanding the legislative frameworks and the labelling/certification initiatives, there is still a lack of clarity on the **responsibility and roles pertaining to privacy and security**.
5. Dealing with the deployment explosion of IoT devices, any cybersecurity-focused approach must primarily address **scalability** and largely leverage security analytics to succeed.

As highly connected CPS introduce high dynamism in the architectures to design, develop and secure the system from external attacks, holistic approaches that enable the collection of data and information from all the distributed CPS components (HW and SW), supporting scalability and adaptability by means of a continuous monitoring-analysing-planning-executing process, are necessarily and urgently required.

As security is deeply intertwined with (and often a prerequisite for) other trustworthiness aspects such as safety and privacy, cybersecurity is not only an ICT issue anymore but spreads all over all interconnected critical infrastructures, following the pervasiveness of IoT and of virtualised architectures.

Security in decentralised and virtualised architectures necessarily copes with both virtual and physical infrastructures. Additionally, frameworks, methodologies and solutions that secure IoT by leveraging networking technologies (see, e.g. ANASTACIA project) represent a valuable resource to counteract the most recent threats in a scalable manner.

All the phases of the system development life cycle (SDLC) must be covered by security-by-design and privacy-by-design approaches, possibly with the adoption of guidelines and procedures for design steps, as well as development and verification tools for development steps, and finally monitoring and mitigation components for the deployment and maintenance steps, with attention paid also to reducing cost and complexity of assurance in large-scale systems.

New methods for reliability and quality development and validation of highly dynamic systems in terms of both security and privacy are needed, possibly converging to the definition of recognised rules and the wide adoption of certification frameworks.

The changing threat landscape must be taken into account, with anomaly detection systems facing 0-day/unknown cyberthreats and mitigation plans that must adapt and evolve accordingly, keeping all stakeholders properly informed of the security and privacy positioning of the observed CPS.

Within the Horizon 2020 projects, ANASTACIA[2] aims at developing a security and privacy framework with a systemic approach that provides self-protection, self-healing and self-repair capabilities through novel enablers and components. The researched framework dynamically orchestrates and deploys security policies and actions that can be instantiated on local agents, enforcing security in different kinds of devices and heterogeneous networks, e.g. IoT- or SDN/NFV-based networks. The framework includes:

- Security Development Paradigm: a security development paradigm based on the compliance with security best practices and the use of the security components and enablers (to provide assisted security design, development and deployment cycles to assure security by design).
- Distributed Trust and Security Enablers: a suite of distributed trust and security components and enablers able to dynamically orchestrate and deploy user security policies and risk-assessed resilient actions within complex and dynamic CPS and IoT architectures (online monitoring and testing techniques will allow more automated adaptation to mitigate new and unexpected security vulnerabilities).
- Dynamic Security and Privacy Seal: a seal combining security and privacy standards and real-time monitoring and online testing (to provide quantitative and qualitative run-time evaluation of privacy risks and security levels, which can be easily understood and controlled by the final users).

This chapter has been structured according to the main topics in the addressed domain:

- "Related work" includes an overview of latest research activities in the field of IoT security and privacy.
- "New security and privacy threats in IoT" illustrates main trends in the cybersecurity domain related to IoT devices, including privacy issues.
- "Main privacy threats in IoT" focuses on the urgent (and often neglected) topic of privacy within the IoT arena, considering the new General Data Protection Regulation recently come into force.
- "Related security frameworks" provides an extensive overview of the main tools, guidelines and frameworks available for IoT developers to secure their architectures, including the main results from reference initiatives and research projects.
- "Conclusions" briefly summarises the main highlighted trends and the most important findings, providing also some insights on future evolution and hot topic to monitor in the near future.

[2] www.anastacia-h2020.eu.

2.2 Related Work

On adaptation and utilisation of IoT in diverse industry sectors, multiple reports and papers stress the importance of inclusion of security and privacy in IoT. For example, "Internet of Things—New security and privacy challenges" [4] emphasises on ensuring the architecture's resilience to attacks, data authentication, access control and client privacy in IoT system and states the importance of the legal framework of IoT data security and privacy, and [5] reviews privacy and security problems on device-to-device (D2D) communication, summarises overall challenges and requirements of different solutions on privacy and security on D2D communication for finding best practice and identifies open problems for guiding the further design and implementation of D2D security and privacy solutions.

According to Thales Data Threat Report [6] issued in conjunction with "451 Research", an analyst firm, 93% of organisations are using sensitive data in an advanced technology environment such as SaaS, IaaS, PaaS, Mobile, big data and IoT. A majority of those respondents (69%) also believe their organisations are deploying these technologies ahead of having appropriate data security solutions in place, and 88% respondents admitted to feeling vulnerable to threats and believe network security very/extremely effective at protecting data. Moreover, security attacks as DDoS become a major issue in terms of costs to the digital economy actors.

A white paper from Cisco [7] states that IoT networks are challenging to secure and analyses IoT threat environment and actors. To overcome the challenges, it recommends risk-based security program with its recommendation of three steps to implement security enforcement program: access, implementation and formalising.

EU estimates that the IoT market in the region will be higher than one trillion euros by 2020 [8]. Accordingly, it has set up IoT action plan with three pillars:

- Single market for IoT.
- Thriving IoT ecosystem.
- Human-centred IoT.

The third pillar, "human-centred IoT", has been established with respect to European values, empowering people along with machines and businesses, and high standards for protection of personal data and security, notably through a "Trusted IoT label". In [9], it gives more details on Trusted IoT label explaining "Trusted IoT label could be developed for consumer products, providing transparency about different levels of privacy and security", and states that "such a labelling system has been implemented as regards energy-efficiency across the EU". It explains that "the Commission services consider important to reflect upon possibilities for certification of networked devices that would provide a minimum level of secure authentication, from the hardware level to network integrity. This would entail some analysis of the functions with which each device is equipped, secure data processing and secure connectivity for the devices to which data are transmitted". It indicates five steps to facilitate data flow and transfer for IoT single market such as:

1. Generation of data
2. Transfer of data
3. Storage of data
4. Processing of data
5. Provision of data services

These steps emphasise the importance of trusted IoT data and at each step combine quality, reliable and security services, together with available, accessible and easily aggregated, processed data.

Many European projects have been or are working on IoT security and privacy, data protection and certification to facilitate the uptake of IoT in Europe following the "Trusted IoT label" policy aligned with EU data protection policy (GDPR) that activates in May 2018.[3] A few examples include:

1. ANASTACIA (Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures, Jan 2017–Dec 2019) aims at developing a security and privacy framework with a systemic approach that provides self-protection, self-healing and self-repair capabilities through novel enablers and components. The more information on this project is included in the following sections.
2. ARMOUR[4] (Large-scale experiments of IoT security and trust, Feb 2016–Jan 2018) project aims to provide duly tested, benchmarked and certified security and trust solutions for large-scale IoT using upgraded FIRE large-scale IoT/cloud testbeds. ARMOUR is working on enhancing two FIRE testbeds for large-scale IoT security and trust experiments, providing benchmark methods on IoT security and trust in large-scale experiments and defining a certification scheme for setting confidence on security and trust IoT solutions.
3. SMARTIE[5] (Secure and smarter cities data management, Jan 2013–Aug 2016) aimed to create a distributed framework to share large volumes of heterogeneous information for use in smart-city applications, enabling end-to-end security and trust in information delivery for decision-making purposes following data owner's privacy requirements.
4. Privacy Flag[6] (May 2015–April 2018) project aims to develop high scalable privacy monitoring and protection solutions by combining crowdsourcing, ICT technology and legal expertise to protect citizen's privacy when visiting websites, using smartphone applications or living in a smart city. It will enable citizens to monitor and control their privacy with a user-friendly solution provided as a smartphone application, a web browser add-on and a public website.

[3] European Commission provides infographic on the data protection rule in http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm.

[4] http://www.armour-project.eu.

[5] http://www.smartie-project.eu.

[6] http://privacyflag.eu.

5. The SECURED[7] (SECURity at the network EDge, Oct 2013–Sep 2016) project has developed open specifications and sample open-source implementations for trusted network security applications providing secure solutions on the network edge such as a home gateway or an enterprise router. High-level Security Policy Language (HSPL) and Medium-level Security Policy Language (MSPL) are two policy languages defined within the European SECURED project in order to specify security policies.

While there have been several projects and studies on security in technical approaches, IoT privacy issues are tightly connected to the data privacy policies and regulations. The EU projects such as Privacy Flag and ANASTACIA try to map such policy requirements (e.g. EU GDPR) into trusted system development providing the user with information on the level of data protection.

Alliance for Internet of Things Innovation (AIOTI) also put its efforts on IoT security and runs Privacy and AIOTI WG4 (policy) and AIOTI WG3 (privacy by design). AIOTI hold a Workshop on Security and Privacy, hosted by ETSI and co-organised by the European Commission, NXP and Arthur's Legal. It was explored and debated whether and to what extent a minimum level of basic requirements can be identified and formulated for security and privacy in IoT that can be taken into account while thinking about a certain evidence-based trust label linked to IoT products and services (European Commission's initiative "Trusted IoT Label") while remaining open to innovation and competitiveness.

As the IoT applications and services are tightly connected to user acceptance more than traditional ICT systems, there are ongoing studies on adapting IoT security and/or privacy certification mechanism on IoT as well. Due to the character of the diverse IoT products, networks and services, it cannot be simply a question of adapting the traditional certification concept into IoT, and ongoing projects of ARMOUR and ANASTACIA are working on this issue as briefly described in the above. Also, there are a few examples of the related papers as the following.

In order to be aligned with the European Union data protection legislation, [10] proposes a solution by enforcing security policy rules. It presents security and privacy challenges and describes a Model-based Security Toolkit named SecKit that integrated into the MQ Telemetry Transport (MQTT) to support IoT security and privacy requirements.

Security certification and labelling in Internet of Things [11] proposes IoT security certification addressing the identified limitations and links formal models to testing and certification. In [12, 13] authors describe the challenges for IoT security testing and present a model-based testing approach solution, which can be used to support an EU security certification framework at European level for IoT products.

International standards bodies are also working on IoT security enhancement. In the IETF, Authentication and Authorisation for Constrained Environments (ace) working group is particularly handling security issues on the constrained networks which applies to IoT systems and networks, while there are other WGs handling network security issues. ITU-T SG17 also has several works related IoT security.

[7] http://www.secured-fp7.eu.

2.3 New Security and Privacy Threats in IoT

With the number of IoT devices increasing, customers accessing to this technology are also increasing, leveraged by the reduction of prices and the increase on the number of functionalities. Furthermore, IoT devices are becoming a critical part of cyber-physical systems which are the core of many critical infrastructures.

This section analyses the current context regarding the security and privacy threats currently appearing in IoT/CPS. It is worth noticing that there are important differences between the traditional IT domain and the current IoT/CPS context. These differences really impact on the type of events threatening these platforms and how they are managed.

The main differences derive from the dynamic and changing character of IoT/CPS platforms, with a large number of devices connecting and disconnecting, installed and uninstalled in a short period of time. This is especially critical for activities such as patching and updating, which are difficult (and costly) to address in such changing environments. Not to mention compliance requirements that new updates might need to fulfil, in order to avoid violations of certifications procedures that these systems, if running on a critical environment, need to comply.

Closely related to the dynamicity of IoT/CPS platforms is the large amount of legacy systems running in these platforms. It is common that many devices from different vendors use different protocols and have different capabilities. Sometimes they are providing just analogue signals that have to be transformed into digital information in order to be used within the platform. This is an issue that has a high impact on the security of an IoT/CPS platform, as many legacy systems require tailored implementations of certain security mechanisms. For other devices, due to resource limitations, those security mechanisms are not even possible.

Another aspect that is inherent to IoT/CPS is the real-time capabilities that, very often, these systems require. This impacts on the way that security events and potential threats are managed, as availability might become a paramount aspect to consider, especially for very critical domains.

The aforementioned distinctive features are exploited by malicious parties to design attacks, but who are these malicious parties and what are their motivations? Authors in [14] classify potential attackers into four main groups:

1. Cybercriminals, whose aim is to target any unprotected system, with no specific purpose, but whose attacks might cause negative side effects.
2. Disgruntled employees, or simply careless ones, installing malware from the inside of the system. These insiders' attacks are very difficult to manage, as the attacker has direct access to the computer and networks, even if the network is physically disconnected from the public Internet.
3. Terrorists, activists and organised criminal groups, who have deep knowledge of systems and are able to exploit even unknown vulnerabilities. Very often these attackers are motivated by economic interests, using them for extortions or simply for public discredit.
4. Nation states, mainly focused on cyber espionage.

The following subsections analyse the context of threats in IoT/CPS from three perspectives:

Analysis of threats: what are threats and the dimensions that need to be considered when analysing them.

Analysis of cyberattacks: what is the life cycle of an attack, that is, the identification of the phases that any attack follows when breaking into a system.

Security objectives: what are the objectives that any security protection policy has to consider when dealing with the protection against potential threats and their corresponding attacks.

The current analysis of threats management in IoT/CPS concludes with the identification of the most paramount attacks and threats and a classification of countermeasures.

2.4 Cyberthreat Analysis

According to the InfoSec Institute [15], a threat could be *anything that leads to interruption, meddling or destruction of any valuable service or item existing in the firm's repertoire*. Threat analysis is essential to combat cyberattacks. The analysis of the information, internal and external, associated to a potential threat represents the difference between reacting to attacks and preventing attacks, thus reducing its impact within a system.

Threat analysis evaluates four dimensions associated to potential threats:

1. Scope, which is the collection of items (devices, information, premises and services) that a threat can target and, thus, can be potentially compromised.
2. Data collection, which is the ability to gather cyberthreat information used by threats, such as vulnerabilities, list of open ports, list of emails or IP addresses of a system.
3. Risk analysis, in order to determine the level of exposure to a threat. This is done by evaluating the current mechanisms that an IoT/CPS platform has to neutralise threats in terms of availability, confidentiality and integrity.
4. Mitigation and anticipation, derived from the outcomes of phases (1), (2) and (3). This phase would be capable of designing mitigation measures and prevent similar attacks in the future.

It is worth noticing that despite the fact that any IoT/CPS platform might be the subject to be attacked in many ways, the risk of suffering a successful cyberattack is higher when three aspects converge (see Fig. 2.3):

- System susceptibility. Not all systems are vulnerable to be attacked. In general, updated systems are less vulnerable that systems with outdated software installed in their devices. As mentioned before, this is a problem in IoT/CPS platforms, with a large number of many different devices running different operating systems or built with different technologies. Additionally, not all systems are

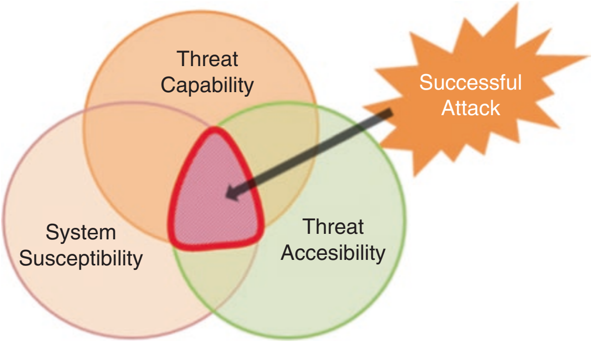


Fig. 2.3 Dimensions of a successful attack

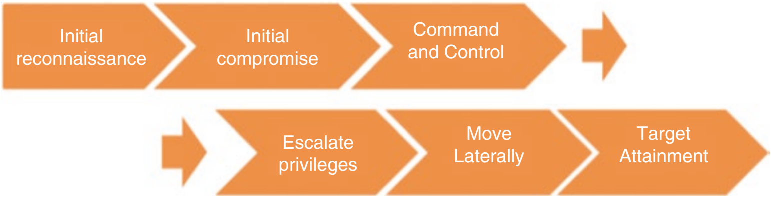


Fig. 2.4 Cyberattack life cycle

interesting for attackers. Only those targets that might return the attacker any type of value are worth the effort of exploiting known vulnerabilities (even more for the effort of discovering and exploiting 0-day vulnerabilities).

- Threat accessibility. Not all systems are accessible to be attacked. Devices physically disconnected from the public Internet are less vulnerable to cyberattacks, while devices physically protected are less vulnerable to tampering attacks.
- Threat capability. The existence of known techniques or tools to exploit vulnerabilities makes it easier for attackers to succeed.

Therefore, when these three dimensions converge at the same time, the likelihood of being attacked is high, and therefore the system/platform is clearly compromised.

2.4.1 Life Cycle of Cyberattacks

The previous threat analysis can be detailed in a set of stages (see Fig. 2.4) that typically characterise the life cycle of a cyberattack [16]:

- Initial reconnaissance: an attacker will study the scope of his/her attack by evaluating the available defences of a system and its potential vulnerabilities, either logical (i.e. software 0-day vulnerabilities), physical (i.e. direct access to a temperature sensor) or human (i.e. unsatisfied employee).

- Initial compromise: an attacker is able to gain entry in some system/platform network by exploiting any of the vulnerabilities identified in the reconnaissance stage.
- Command and control: once inside the platform, the attacker typically would install any malicious software, such as remote access tools, in order to quickly access again to the system with very few resources.
- Escalate privileges: attackers typically try to escalate their privileges once inside the system, for example, by obtaining PKI certificates or with the installation of key loggers to obtain passwords.
- Move laterally: attackers scan the network internally in order to find additional targets, for example, to access to other devices and performing internal vulnerability scans.
- Target attainment: attackers finally get access to the pursued resources, either retrieval or deletion of files or info from databases or simply resetting configurations or shutting down devices.

2.4.2 Security Objectives for IoT/CPS

The third pillar to analyse is related to the security objective that has to be reached for the protection of an IoT/CPS against threats and attacks. According to [17], four objectives typically targeted are:

- Confidentiality, to prevent the disclosure of sensible information (including the maintenance of user's privacy) to unauthorised individuals or systems.
- Integrity, to ensure that the data managed in the system have not been altered by unauthorised parties.
- Availability, to assure that the services provided in IoT/CPS platforms or the resources offered by devices are working properly without interruptions.
- Authenticity, to verify that all the processes (data management, transactions and communications) are genuine and produced/consumed by trusted parties.

2.4.3 Threat Actors

According to the IoT Threat Environment published by CISCO in 2015 [7], several threat patterns can be identified based on the actors involved. More specifically, the report identifies two actors:

Sophisticated actors, with technical skills and following an economic motivation. These actors are typically organised in groups and targets critical infrastructures, such as energy or public-sector infrastructures.

Insider actors which are typically represented by employees, contractors or vendors. Threats associated to these actors can be either malicious or unintentional. The unintentional threats are related to the access to sensitive resources and to the propagation of attack vectors, such as malware infections due to infected computers from contractors, infected USB devices, untrusted software installations or phishing attacks. Malicious attacks from insider actors are commonly similar to unintentional attacks, but their impacts are bigger as their target is more clear, trying to achieve a more tangible impact making use of the knowledge of the system.

2.4.4 Attack Patterns

From the above evaluation of attacks and controls, we can identify different attack patterns that differ on the purpose of the attack, the way it is performed and its effects. According to [7], four patterns can be identified:

- **Targeted attacks**: In this type of attacks, attackers know in advance the objective they want to target, which is commonly based on the impact of it, or the benefits they would obtain. Very often, attack vectors move laterally from one objective to another, looking for the highest impact. To this end, network managers would minimise the risk of the attack moving from one objective to another by keeping devices updated and vulnerabilities controlled.
- **Collateral damage risk**: This pattern is related to the targeted attack. It happens when attackers, when looking for the main target of their attack, also compromise and infect related nodes, exploiting vulnerabilities of these secondary nodes and compromising also the information managed by them.
- **Social engineering and phishing**: Insider actors, being one of the weakest links in the security chain, are the objective of attackers, trying to cheat them to click on malicious links, open infected emails or install malware.
- **Remote access**: Taking advantage of poorly designed security mechanisms, attackers can take control of devices and use them to trigger attacks remotely. Most of DDoS attacks towards some famous service providers followed this pattern.

2.4.5 Major Security Vulnerabilities

The following table gives an overview of major security vulnerabilities, according to ETSI M2M [18] (Table 2.1).

Table 2.1 Major security vulnerabilities

Id	Title
V1	Discovery of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways
V2	Deletion of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways
V3	Replacement of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways
V4	Discovery of Long-Term Service-Layer Keys stored in M2M Infrastructure
V5	Deletion of Long-Term Service-Layer Keys Stored in M2M Infrastructure Equipment
V6	Discovery of Sensitive Data in M2M Devices or M2M Gateways
V7	General Eavesdropping on M2M Service-Layer Messaging Between Entities
V8	Alteration of M2M Service-Layer Messaging Between Entities
V9	Replay of M2M Service-Layer Messaging Between Entities
V10	Unauthorised or Corrupted Applications or Software in M2M Devices/Gateways
V11	M2M System Interdependencies Threats and Cascading Impacts
V12	M2M Security Context Awareness
V13	Eavesdropping/Man-in-the-Middle Attack
V14	Transfer of Keys via Independent Security Element
V15	Buffer Overflow
V16	Injection
V17	Session Management and Broken Authentication
V18	Security Misconfiguration
V19	Insecure Cryptographic Storage
V20	Invalid Input Data
V21	Cross Scripting

2.4.6 Main Threats in IoT/CPS

A myriad of cyberattacks are threatening IoT/CPS infrastructures. Almost every week some relevant new incident involving cyberattacks and IoT appears in the mass media. One of the first proven massive cyberattacks in IoT happened in 2014, when 750.000 malicious emails were sent from 100.000 devices such as TVs or refrigerators. In October 2015 a massive DDoS attack, triggered from smart light bulbs, webcams or smart thermostats, affected important DNS servers in the USA. Many cyberattacks have also targeted IoT infrastructures built over critical infrastructures. The most salient one occurred already in 2010 when the so-called Stuxnet ruined several nuclear centrifuges of nuclear power plants by exploiting several vulnerabilities present in access control devices. More recently, in the winter of 2015, a Ukrainian power grid suffered the so-called Blacknet attack. The attack managed to install malware in many devices within the power grid premises. The result was the complete blackout of an entire city. Another massive DDoS attack triggered from many different devices took down for a week in November 2016 the central heating system of a Finnish city.

Authors in [19] have organised potential attacks to IoT systems according to the layer that is targeted, distinguishing between threats at the physical, network and application layers. The following table shows the attacks identified by [19]. We have completed the listing by adding the potential controls needed to mitigate such threats. These controls have been identified by the Cloud Security Alliance [20].

Seven controls, as identified by the CSA for risk mitigation, are:

Control 1. Analyse privacy impacts to stakeholders and adopt a privacy-by-design approach to IoT development and deployment.

IoT systems collect huge amount of data which very likely contains sensitive information about individuals or infrastructures. Users should know what data is collected from and about them and decide what information to exclude from the set of collected data.

Control 2. Apply a secure systems engineering approach to architecting and deploying a new IoT system.

This control is based on the implementation of security requirements at design time, thus ensuring that the deployment is secure enough against potential threats. The security mechanisms to incorporate in the design would depend on threat models that would identify which are the security requirements to cover.

Control 3. Implement layered security protections to defend IoT assets.

This control is related to the separation of the elements to protect, for example, distinguishing between the IT and the OT or to focus on the mechanisms covering the threat targeting, for example, the transport layer.

Control 4. Implement data protection best practices to protect sensitive information.

Including mechanisms for encryption, identification of data or its classification.

Control 5. Define life cycle controls for IoT devices.

This control includes the monitoring and management of assets during the operation time and a clear specification of actions to carry out for securely disposing IoT assets at the end of the life cycle.

Control 6. Define and implement an authentication/authorisation framework for the organisation's IoT deployments.

This control stresses the need of mechanisms for identifying the entities/users accessing devices or certain capabilities within a device (e.g. using authentication based on the exchange of certificates).

Control 7. Define and implement a logging/audit framework for the organisation's IoT ecosystem.

This control relies on the correlation of information retrieved from devices, for example, through monitoring agents, with the possibility to use logs from devices running outside the organisation.

2.4.7 Security Threats on Physical Layer

The following table provides an overview of major security threats on the physical layer.

Security threats	Description	Related controls	Actor
Physical attack	Physical attack mainly refers to the physical damage for the nodes	3: A separation of the assets to protect would allow to focus on the physical protection of devices, for example, with anti-tampering objects	Insider actor with physical access to devices
Equipment failure	Equipment reduces or loses performance due to external forces, environment or ageing	2: Potential damages (i.e. loss of information) can be mitigated with specific security mechanisms implemented at design time (i.e. with data backups when the equipment performance decreases) 5: Active monitoring performed at operation time would allow to detect potential degradations of the service offered by a device	Not linkable to any actor (except in cases of sabotage performed by insider actors)
Line fault	Line failure is the failure of power lines on the nodes	2: Specific security measures designed in case of power lines would allow to prevent the reception of incorrect data. For example, temporally isolating parts of the infrastructure in case of line failures 5: Active monitoring performed at operation time would allow to detect potential degradations of the service offered by a device	Sophisticated actor interceding with external power infrastructures Insider actor with access to the internal power infrastructures (e.g. disabling SAIs)
Electromagnetic leakage	By processing electromagnetic signal equipments at work radiated out, attackers can restore the original data	2: Specific security mechanisms must be designed to prevent the correlation of information obtained from electromagnetic signals (e.g. obfuscating the information display)	Sophisticated actors with technically advanced mechanisms for extracting information from electromagnetic signals

Security threats	Description	Related controls	Actor
Electromagnetic interference	Unwanted electromagnetic signals or commotions make negative impacts on useful signals, resulting in system performance degradation	2: Specific security mechanisms must be designed to prevent this threat, for example, buffering data to send, while the quality of the wireless link is not good or looking for an alternative frequency where to send the data 5: Active monitoring performed at operation time would allow to detect degradation of the service due to signal interferences	Sophisticated actors capable of interfering electromagnetic signals
Denial of service (DoS)	Attacker makes the target system stop providing services through network bandwidth consumption	2: Mechanisms implemented by design can be implemented to prevent denial-of-service attacks, such as dynamic load balance or isolation of requests	Sophisticated actors capable of accessing to a large amount of devices and trigger the attack from there
Channel blocking	Data cannot be transmitted for communication channel has been occupied for a long time	3: Specific mechanisms at transport layer can be designed to stop and resume the communication. At the physical layer, it can be mitigated by changing the communication channel (e.g. negotiate a different frequency by using ultrasounds)	Sophisticated actors performing an active attack on communication channels Insider actor using, on purpose or not, too much bandwidth
Sybil attack	Single malicious node has multiple identities, to attack the system by controlling most of the nodes	6: Authorisation mechanisms need to be designed in order to prevent not allowed parties to access to devices	Sophisticated actors
Replay attack	Attacker resends the legitimate data obtained before, to get the trust of the system	2: Mechanisms implemented by design can be implemented to prevent intermissions of untrusted parties 4: Encryption mechanisms can be used to guarantee non-repudiation of data	Sophisticated actors and insider actor either from the outside of the infrastructure or from the inside, respectively
Perception data destruction	The unauthorised addition, deletion, modification and destruction of perception data	4: Mechanisms for the protection of sensitive information are needed to prevent the disclosure of sensitive information 6: Mechanisms for authentication and authorisation are required to prevent attackers to access to data	Sophisticated actors and insider actor, either malicious or not

Security threats	Description	Related controls	Actor
Data intercept	Illegal access to the data resources through intercepting the communication channel	3: Mechanisms can be implemented at the transport or physical layer to prevent untrusted parties to access the communication channel 4: Data encryption can be implemented to prevent untrusted parties to access to data intercepted 6: Authentication and authorisation mechanisms would prevent untrusted parties to access to communication channels	Sophisticated actors and insider actors
Data tampering	Attacker intercepts and modifies the data and then sends modified data to the recipient	3: Mechanisms can be implemented at the transport or physical layer to prevent untrusted parties to access to the communication channel 4: Data encryption can be implemented to prevent untrusted parties to access to data intercepted 6: Authentication and authorisation mechanisms would prevent untrusted parties to access to communication channels	Sophisticated actors Malicious insider actors
Unauthorised access	Resources are accessed by unauthorised users	6: Authentication and authorisation mechanisms would prevent untrusted parties to access to resources	Sophisticated actors Malicious insider actors
Passive attack	Attacker passively collects data by sniffing and information collection	3: Mechanisms can be implemented at the transport or physical layer to prevent untrusted parties to access the communication channel 4: Data encryption can be implemented to prevent untrusted parties to access to data intercepted 6: Authentication and authorisation mechanisms would prevent untrusted parties to access to communication channels	Sophisticated actors
Node capture	Gateway node or ordinary node is controlled by attackers	6: Authentication mechanisms would allow to prevent attackers to get control of the gateway	

2.4.8 Security Threats of Network Layer

The following table provides an overview of major security threats on the network layer.

Security threats	Description	Related controls	
DDoS	Plenty of malicious nodes attack target server as the sources of DoS at the same time	2: Mechanisms implemented by design can be implemented to prevent denial-of-service attacks, such as dynamic load balance, or rules to block requests	Sophisticated actors
Routing attack	Attacker interferes with the normal routing process by sending forged routing information	3: Specific mechanisms at transport layer can be designed to prevent attackers to forge routing activities	Sophisticated actors
Sink node attack	Interrupting data transmission between physical layer and network layer by attacking the sink node	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7: Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
Direction misleading attack	Malicious node modifies the source and destination addresses of data packets and then sends it to a wrong path, resulting in network routing confusion	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7: Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
Blackhole attack	Malicious node cheats other nodes to establish routing connections with it and then discard the packet that should be forwarded, causing packet loss	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7 Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
Flooding attack	Exhausting the resources of the network servers on network layer by Smurf and DDoS	2: Software developed with security-by-design mechanisms can be implemented to prevent flooding attacks	Sophisticated actors
Trapdoor	Allow the exception of security policy when specific data transporting	2: Ensure security-by-design mechanisms to guarantee the policy enforcement, warning about potential violations of it	Sophisticated actors
Sybil attack	Malicious node illegally has multiple identities, to obstruct data transmission by controlling most of the nodes	6: Authentication mechanisms would prevent untrusted parties to control IoT nodes	Sophisticated actors

Security threats	Description	Related controls	
Sinkhole attack	Malicious node attracts normal nodes around as a point in the routing path, so that all data will flow through it	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7: Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
Wormhole attack	Malicious nodes attack together to get the routing right by the less routing hops between the malicious nodes	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7: Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
Routing loop attack	Malicious node modifies the data path to cause an infinite routing loop	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7: Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
Hello flooding attack	Malicious node makes nodes in the network aware that it is their direct neighbours by using strong signal to broadcast routing information	3: Specific mechanisms at network and transport layer, for example, to reroute traffic 7: Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
Spoofing attack	Malicious node spoofs normal nodes to send data through an inefficient path or to a failure node	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7 Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
Selective forwarding	Malicious node deliberately loses some or all of the key information in the forwarding	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7: Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
Tunnel attack	Malicious nodes hide the real link distance between them to lure the other nodes to establish routing path through them	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7: Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors
False routing information	Malicious node attacks network layer network by tampering with the routing information	3: Specific mechanisms at network and transport the layer, for example, to reroute traffic 7: Log network activities to detect the attack and trigger the appropriate rerouting	Sophisticated actors

2.4.9 Security Threats of Application Layer

The following table provides an overview of major security threats on the application layer.

Security threats	Description	Related controls	
Privacy data leaking	Leaking of privacy data of users due to the insecurity of data transmission, storage and presentation	1: Privacy by design mechanisms allow to keep control of sensitive data, minimising the impact in case of leakage of information 4: Data protection mechanisms can be implemented to prevent sensitive data disclosure to untrusted parties	Sophisticated actors Malicious insider actors
Unauthorised access	Illegal access to the network and system data	6: Authentication mechanisms would prevent untrusted parties to control or access to protected resources 7 Log access activities to detect the attack and prevent unauthorised access	Sophisticated actors
Malicious code	Code in the system with no effect but may have security risks	2: Security by design and testing activities will allow to minimise the insertion of malicious code in the system	Insider actors, inserting bugs in code either voluntarily or involuntarily
Forged control commands	Attackers maliciously use the system or damage the system by forging control commands	6: Authentication mechanisms would prevent untrusted parties to control or access to protected resources	Sophisticated actors Malicious insider actors
Loophole	Attacking the system by using the loopholes in the applications on application layer	2: Security by design and testing activities will allow to minimise the insertion of malicious code in the system	Insider actors, inserting bugs in code either voluntarily or involuntarily
Viruses and Trojan horses	Viruses and Trojan horses are the generally security threats of applications on application layer	2: Security by design and testing activities will allow to minimise the insertion of virus and Trojans in the system 7: Log antivirus and malware detectors will allow to detect, clean and prevent this threat	Insider actors that involuntarily execute malicious software
SQL injection attack	SQL injection is a common mean of attack on database of the system	2: Security by design and testing activities will allow to minimise the insertion of incorrect data to databases	Sophisticated actors

2.5 Common Countermeasures to Mitigate Threats in IoT/ CPS

A countermeasure is defined as an action taken to weaken the effect of another action or a situation or to make it harmless. In general, threats are unavoidable, and every system has to be designed with the assumption that it will often suffer from many different types of attacks. According to [14], the growing concern for protection IoT/CPS against malicious cyberattacks is based upon the premises of prevention, detection, recovery, resilience and deterrence.

Prevention is the first defence against cyberattacks and becomes a challenge mostly targeted by the standardisation community from many different domains. Some examples are the cybersecurity standard for controls systems in the electric sector created by the North American Electric Reliability Corporation (NERC). The NIST has also published a set of best practices in the NIST SP 800-53, with a set of recommendations that can provide guidance for analysing the security of most companies. The ISA (International Society of Automation) is developing the ISA99, which includes a set of standards, recommended practices, technical reports and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance, with the objectives of improving confidentiality, integrity and availability of control systems.

The detection and recovery against attacks are the main reaction countermeasure to address when an attack has succeeded. The usage of monitoring tools becomes the first mechanism to detect attacks. To this end, a key aspect for detecting attacks is the deep knowledge of the system. Very often this is done through human intervention, although the need of automatic recovery becomes one of the paramount challenges being currently targeted by industry.

System resilience, together with security-by-design principles, becomes another important aspect used to react or prevent attacks. Some specific actions related to this aspect are the redundancy (to prevent singles point of failure), diversity (having the same service running on different SOs) or the limitation of privileges (separating privileges among different users to limit the access that a corrupted entity can have to the system and its resources).

Not being the most successful measure to prevent or react to attacks, deterrence becomes the basic aspect that any domain should have. However, very often this aspect depends on successful legislation, law enforcement and international collaboration, which have been proved not to be effective enough to prevent cyberattacks.

2.6 Major Privacy Threats in IoT

The continuous development of the Internet of things (IoT) brings considerable innovations and new use cases for all the people buying connected devices. But at the same time, privacy is more and more put in danger. The revelations about privacy breaches, which are voluntarily done or not, are weekly or almost daily published in the different media. To prevent the privacy leaks, the main threats for the privacy should be analysed in the context of IoT.

Firstly, the privacy policies should be more transparent and clearer. The legal texts accompanying the services provided with the IoT devices (e.g. the legal notice about the privacy introduced in the terms and conditions of a server collecting data of IoT sensors) are lengthy and not very understandable for the majority of the IoT devices buyers. Scarcely anyone reads all the legal texts, and hence, the awareness of the users is not adequate in comparison of the privacy risks. The user accepting a privacy policy without fully reading it can authorise the collection of personal data through IoT sensors. Therefore, the first threat is the opacity of the privacy policies but also the opacity of the different companies engaging in business related to IoT. Several companies claim to take care of the privacy when collecting personal data through their sensors, but often, these companies share these data through their different services or to third parties like mentioned in this article [21]. At the end, the users don't know if the privacy is fully respected across all the entities or organisations using their data.

To solve this threat, the representation of the privacy policies should be made more attractive to the final IoT users. For example, an adequate iconography or a short video could replace in a better way the actual textual representation of the privacy policies.

A second important threat concerning the privacy is the identification of the data subject. New technologies or improvements of existing technologies make the life easier for the users but can severely compromise their privacy. For example, fingerprinting and facial recognition are becoming more and more usual on the smartphones and on the laptops, facilitating the authentication of the users when accessing these mobile devices. Regardless of how appealing these features may be, vulnerabilities are increasingly reported [22], a good indicator of lacking maturity which in turn raises privacy considerations. Among the devices and features primarily concerned by this threat are the video cameras, the fingerprinting and the speech recognition. Of course, the users should acquire the awareness about the privacy risks linked to their identification.

The IoT devices are a good source of data for profiling. The method to achieve the profiling is the automated processing of personal data followed by the evaluation of certain personal aspects of a natural person. The profiling can lead to an inequity of treatment for a person and, finally, to a discrimination against this person. The profiling can be realised through simple IoT sensors and some aggregations of data provided by these remote sensors. For example, a system composed by a remote sensor network monitoring the apartment of an elderly or a disabled person and launching alerts when something happens wrong can be diverted from its original goal to determine the behaviour of this person. The profiling is very spread in the online market places selling different kinds of product. This practice enables the creation of personalised advertising to encourage the profiled user to buy new products compatible with his preferences.

Another privacy threat in IoT is the linkage. The objective of the linkage is the re-identification of anonymised data. After the linkage, a profiling is possible without any difficulty. Of course, several sources of data are used, in particular these provided by the IoT devices. The dilemma with the linkage is that if there are two or more sources of data, which are all privacy friendly, the combination of these different sources after linkage can bring a breach in terms of privacy. The parameter to achieve the linkage in the two different datasets which are provided by two different data sources must be common to both datasets: for instance, the location or the timestamp (the date and the time) are good candidates facilitating the linkage of data. The linkage becomes more and more efficient as the data mining and the artificial intelligence are more sophisticated than several years ago.

The localisation is the next threat touching the privacy. Not only is the famous GPS a source of localisation for smartphones, but there are a lot of technical solutions to obtain a more or less precise location of an IoT device. For instance, several companies working with the LoRa protocol are able to geolocalise their wireless low-powered IoT devices without using a GPS consuming a lot of power; this technology is named localisation-based services (LBS) over LoRa. So, the wireless sensor networks offer by themselves some solutions for the localisation, depending of the communication protocol and its lowest layers (physical, data link and network layers of the OSI model) used within each of them. But a second kind of localisation can be made easily using the IP address of the connected device, and next, a WHOIS request can be done to get personal data linked to the organisation or person associated to the IP address of the IoT device. By the way, WHOIS is itself not compatible [23] with the GDPR. So turning off the GPS localisation on a smartphone or on an IoT device doesn't mean that the current localisation is not retrieved and sent; this is particularly true for smartphones which require to turn them off completely to ensure that the location is not sent in any case.

The personal data can be stored inside IoT devices or IoT gateways and also represents a threat for the privacy. By the principle of the privacy by design, the personal data created and stored inside an IoT device should be reduced to a minimum. If it is really needed, the storage of the personal data and their transmission from the IoT device to IoT gateways must be encrypted by the relevant methods and standards. As the IoT device and also the IoT gateways are often constrained nodes with low power, the possibilities offered to them to protect against attacks are reduced, but there are more and more microchips with hardware encryption available on the market. To protect the communication between the IoT device and its gateway, some protocols were designed for constrained nodes taking into account the security: for instance, CoAP (Constrained Application Protocol) is used with DTLS (Datagram Transport Layer Security) to ensure a good security during the transmission of data.

2.7 Related Security Frameworks

Previous sections have identified the main security and privacy threats, vulnerabilities and attacks in the Internet of Things. This section provides an overview of the main efforts being carried out to cope with the aforementioned issues. Namely, the section reviews the main security and privacy frameworks defined in the scope of different initiatives, such as OWASP, oneM2M, GSMA as well as European H2020 projects like ANASTACIA and ARMOUR.

2.7.1 OWASP IoT

The OWASP [24] IoT project defines a security framework that gathers information on security issues associated to the IoT development, deployment or technology assessment. It aims to help manufacturers and developers as well as consumers to increase their confidence into this rapidly evolving domain.

More specifically, the OWASP IoT security framework defines the following 17 surface areas that may undergo attacks going from device memory to vendor back-end APIs through the ecosystem access control and communication, as depicted in Fig. 2.5.

Furthermore, they provide ten high-level vulnerabilities, depicted in Table 2.2, which can be identified among the IoT surface areas.

OWASP main top vulnerabilities. Source: [24].

For each vulnerability, among other elements, a short description is given, linking it to the problem that creates the vulnerability, the threats, attack vectors and their impact (technical or business). A risk analysis based on the OWASP Threat

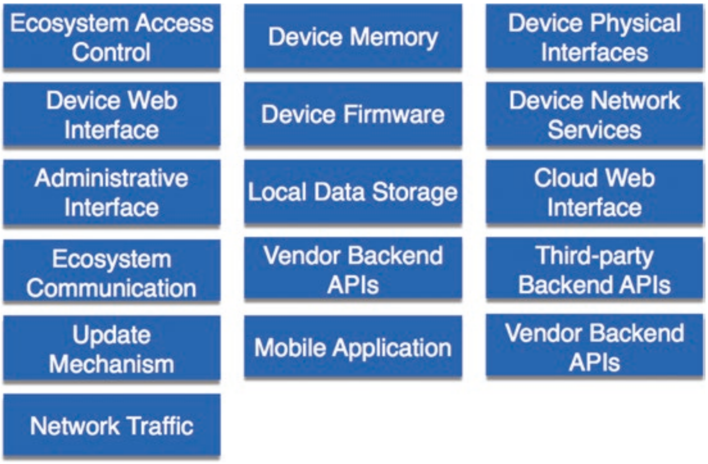


Fig. 2.5 OWASP IoT surface areas

Table 2.2 OWASP top ten vulnerabilities

ID	Name	Description
I1	Insecure web interface	Anyone having access to the web interface if the system is not secured enough could perform attacks such as SQL injection or XSS (for more details see OWASP TOP 10)
I2	Insufficient authentication/ authorisation	When weak passwords are used or poorly protected. It is prevalent if it is assumed that the interfaces web connections from external networks are not taken into account
I3	Insecure network services	They might be susceptible to buffer overflows or attacks that create denial of service
I4	Lack of transport encryption/integrity verification	Allows data to be viewed as it travels over local networks or the Internet. Often local network is under such risk as it is assumed that it will not be widely visible
I5	Privacy concerns	Lack of proper protection of collected personal data
I6	Insecure cloud interface	Lack of credentials and reset mechanisms or not using SSL for connection on the cloud interface
I7	Insecure mobile interface	Lack of credentials and reset mechanisms or not using SSL for connection to the mobile wireless network
I8	Insufficient security configurability	Lack of granularity in configuration options, especially for user permissions
I9	Insecure software/ firmware	They contain hard-coded sensitive data or unprotected network connection for updates of the software/firmware
I10	Poor physical security	USB or other ports can be easily accessed on the device, for instance, to bypass configurations or permissions

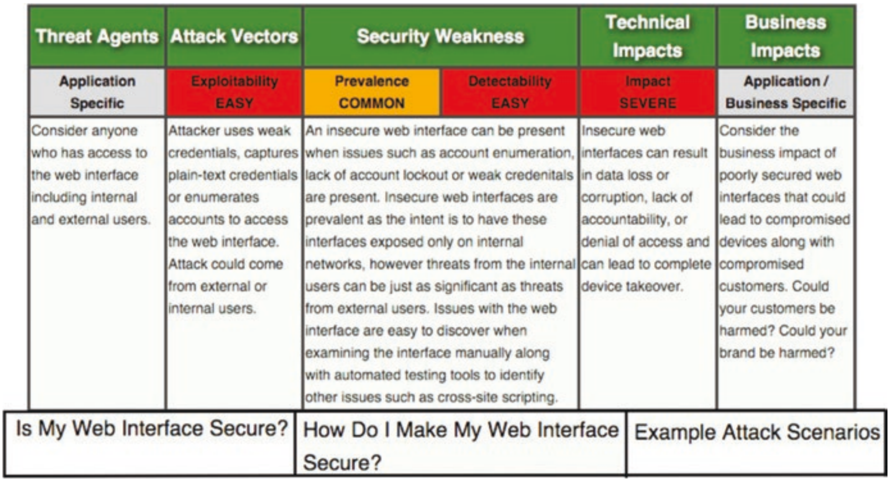
Risk Modelling [24] and Risk Rating Methodology is also performed for each of the vulnerability categories. In the following, we present an example of OWASP IoT vulnerability.

In addition, in order to verify the application resilience to such attacks, the framework provides countermeasures, as well as attack scenarios for each of the ten vulnerabilities, as depicted on the bottom of Fig. 2.6. The framework makes reference to existing vulnerabilities in the worldwide known vulnerabilities databases, such as CWE.

To resume, the OWASP IoT security framework indeed offers guidance for security awareness and testing. Hence, it often remains too high level and lacks specific methodology that could be used in a systemic way—for instance, in security audits. Moreover, the attack surface areas need more structured view—for instance, based on the four segments of IoT: devices and data, (wireless) connectivity, platforms and applications and services.

2.7.2 oneM2M

oneM2M was established to develop a single horizontal platform for the exchange and sharing of M2M/IoT data among all applications, thus creating a distributed software layer which provides a framework for interworking with different



Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the web interface including internal and external users.	Attacker uses weak credentials, captures plain-text credentials or enumerates accounts to access the web interface. Attack could come from external or internal users.	An insecure web interface can be present when issues such as account enumeration, lack of account lockout or weak credenitals are present. Insecure web interfaces are prevalent as the intent is to have these interfaces exposed only on internal networks, however threats from the internal users can be just as significant as threats from external users. Issues with the web interface are easy to discover when examining the interface manually along with automated testing tools to identify other issues such as cross-site scripting.		Insecure web interfaces can result in data loss or corruption, lack of accountability, or denial of access and can lead to complete device takeover.	Consider the business impact of poorly secured web interfaces that could lead to compromised devices along with compromised customers. Could your customers be harmed? Could your brand be harmed?

Is My Web Interface Secure?	How Do I Make My Web Interface Secure?	Example Attack Scenarios

Fig. 2.6 OWASP IoTI1: Insecure web interface. Source: [24]

technologies [25]. oneM2M defines a security framework from its own *architecture model* which supports end-to-end M2M services. A high-level functional view of this architecture model is shown in Fig. 2.7. Starting from this, oneM2M identifies four security domains which in turn provide a set of security measures to address certain threats that may appear on it.

Applications domain security: A set of security measures that enable the Applications entity and the Common Services entity to securely exchange messages and protect against attacks on **(1)**.

Intra-common Services domain security: A set of security measures that enable Common Services Functions in the Common Services entity to securely exchange messages and protect against attacks on **(2)**.

Inter-common Services domain security: A set of security measures that enable messages a secure exchange between different Common Services entities and protect against attacks on **(3)**.

Underlying Networks security: A set of security measures that enable the Common Services entity and the Underlying Networks Services entity to securely exchange messages and protect against attacks on **(4)**.

In addition, the oneM2M security architecture consists of the following layers:

- **Security functions layer**: this layer contains a set of security functions which can be classified into six categories: they are identification, authentication, authorisation, security association, sensitive data handling and security administration.
- **Security environment abstraction layer**: this layer implements various security capabilities such as key derivation, data encryption/decryption, signature generation/verification, security credential read/write from/to the secure environments and so on. The security functions in the security functions layer invoke these functions in order to do the operations related to the secure environments.

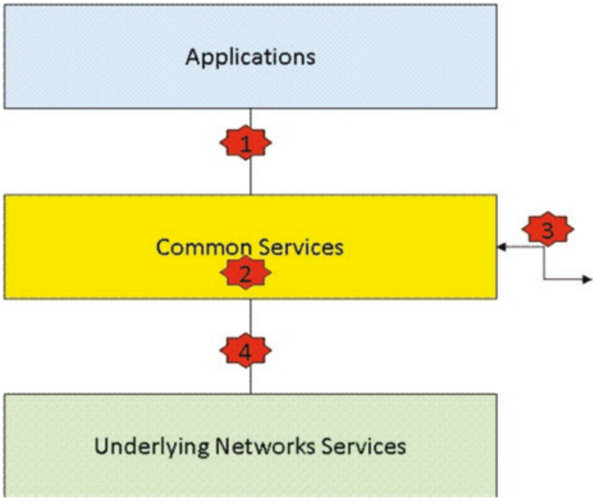


Fig. 2.7 oneM2M context and security domains

In addition, this layer also provides physical access to the secure environments. This layer is not specified in the oneM2M release 1.

- **Secure environment layer**: this layer contains one or multiple secure environments that provide various security services related to sensitive data storage and sensitive function execution. The sensitive data includes SE capability, security keys, local credentials, security policies, identity information, subscription information and so on. The sensitive functions include data encryption, data decryption and so on.

The definition of threats that can appear in each domain, as well as the implementation of security measures to solve them or palliate them, is based on the following aspects: secure storage of sensitive data, sensitive functions executing operations on sensitive data and secure connections allowing the secure transmission of sensitive data. Based on them, oneM2M describes a set of vulnerabilities relevant to the security domains explained above. To do this, a predefined template is used that includes the following information: the issue caused by the threat, a description of the vulnerability, the affected security domains and the list of M2M stakeholders and M2M architecture components which are impacted by the threat.

2.7.3 GSMA IoT Security Guidelines

GSMA (GSM Association) provides a set of security guideline documents that acts as a baseline for IoT security issues for all IoT involved entities (service providers, device manufacturers, developers, network operators, etc.). These guidelines provide recommendations at three levels: service ecosystem, endpoint ecosystem and network operators, providing also a link to the mobile solution, as one of the most promising connectivity solutions for the IoT. Figure 2.8 shows the GSMA example of an IoT model.

The GSMA Security Framework does not provide new IoT standards, as oneM2M, for instance, but points to currently available solutions, standards and best practices in order to respond to the following IoT security challenges [26].

To ensure **IoT availability**, for instance, for cellular communication low-power wide area (LPWA), wireless technology and protocols should be integrated to provide services and solutions for IoT needs, i.e. low-power consumption and effective communication.

Ensuring **identity of IoT** ecosystem means preventing from attacks such as glitching, side-channel analysis, passive data interception, physical tampering and identify theft. To this end, GSMA proposes to integrate security specifications, for instance, oneM2M. These specifications provide solutions for securing over-the-air firmware updates and management of devices capabilities and identities.

To address the challenge of **privacy and security**, technologies such as 3G and 4G use mutual authentication to verify the identity of an endpoint and a network. In addition, as the devices are dealing with individual's personal information, privacy and security need to be ensured also of this individual information. However, what elements need to be protected are also a key challenge for IoT service providers as they are often country-dependent (different laws differently even inconsistently implemented in the countries).

In addition, as well as oneM2M, GSMA suggests to follow a concept of information technology **risk assessment process**. For instance, they refer to the existing process by the National Institute of Standards and Technology (NIST) Risk Management Framework and the Computer Emergency Response Team's (CERT) OCTAVE model.

Although this framework provides guidelines on how to prevent and countermeasures on three levels (i.e. service, endpoint and network), it is more focused on mobile technology, as one of the most promising technology for working within the "things".

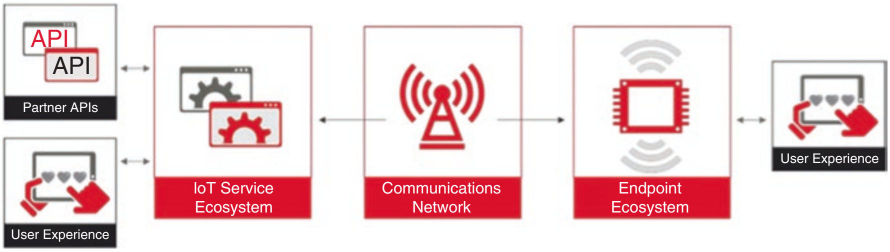


Fig. 2.8 GSMA IoT example model

2.7.4 ANASTACIA Project Security Framework

ANASTACIA [27] will develop a trustworthy-by-design autonomic security framework that allows testing, validating and optimising security, from design to deployment and maintenance. The framework relies on diverse enablers to dynamically orchestrate and deploy user security preferences, facilitate the deployment of local agents and enforce security in heterogeneous scenarios including those based on SDN/NFV and IoT networks. ANASTACIA will ultimately facilitate the testing and vulnerability analysis of the deployed components with simple and user-friendly security policy tools. The ANASTACIA framework includes:

- A security development paradigm based on the compliance to best practices and the use of the security components and enablers (to provide assisted security design, development and deployment cycles and thus assure security by design).
- A suite of distributed trust and security components and enablers that are able to dynamically orchestrate and deploy user security policies and risk-assessed resilient actions within complex and dynamic CPS and IoT architectures (online monitoring and testing techniques will allow more automated adaptation of the system to mitigate new and unexpected security vulnerabilities).
- A holistic Dynamic Security and Privacy Seal, combining security and privacy standards and real-time monitoring and online testing (to provide quantitative and qualitative run-time evaluation of privacy risks and security levels, which can be easily understood and controlled by the final users).

The ANASTACIA architecture includes a set of planes shown in Fig. 2.9. The data plane establishes network communication between ANASTACIA components, and the control plane manages the resource usage and real-time operation of the services. The autonomic plane enforces security mechanisms and real-time reconfiguration and adaptation of the services, while the user plane provides interfaces and tools to end users for policy definition, service monitoring and management. The seal management plane combines security and privacy standards with real-time monitoring.

To cope with the IoT vulnerabilities above identified, ANASTACIA is addressing the development of different innovative cyberthreat solutions to counter cyberthreats. Anomaly detection and prevention systems facing 0-day/unknown cyberthreats are being devised to enhance the cyberthreat protection capacity. ANASTACIA is working on the impact of self-adaptive attack and defence approaches in response to a priori information available to each other. A cyclic policy-based [28] refinement process is being adopted, following a loop of interactions between security policy definition, enforcement, time-varying attack and defence mechanisms, which will allow to come up with more reliable detection and prevention tools.

Additionally, innovative protection algorithms are being designed in ANASTACIA to identify cyberthreats, through anomaly-based intrusion detection approaches inferring certain features from live network traffic and applying techniques belonging to different fields to identify running unknown attacks (0-day)

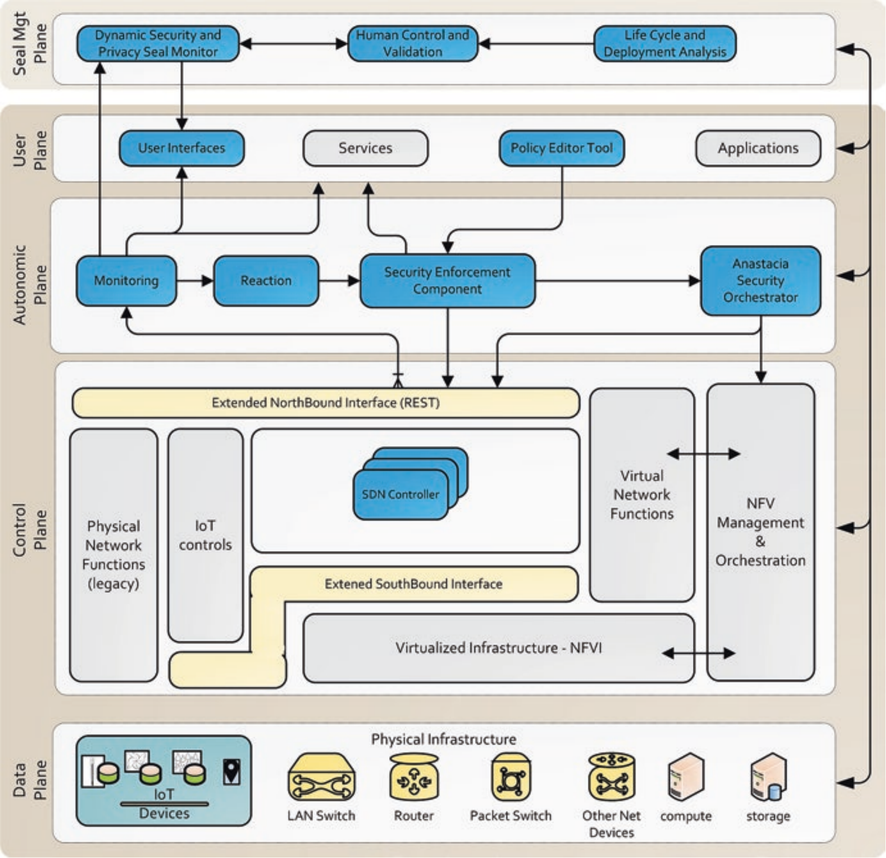

Seal Mgt Plane
Dynamic Security and Privacy Seal Monitor
Human Control and Validation
Life Cycle and Deployment Analysis
User Plane
User Interfaces
Services
Policy Editor Tool
Applications
Autonomic Plane
Monitoring
Reaction
Security Enforcement Component
Anastacia Security Orchestrator
Control Plane
Extended NorthBound Interface (REST)
Physical Network Functions (legacy)
IoT controls
SDN Controller
Virtual Network Functions
NFV Management & Orchestration
Extened SouthBound Interface
Virtualized Infrastructure - NFVI
Data Plane
Physical Infrastructure
IoT Devices
LAN Switch
Router
Packet Switch
Other Net Devices
compute
storage

Fig. 2.9 ANASTACIA framework overview

performed against specific services. These algorithms are complemented through the implementation of automated reaction components able to autonomously protect the system [29, 30], by integrating with the monitoring systems developed in ANASTACIA as well as developing appropriate mitigation plans able to counter identified threats.

2.7.5 ARMOUR Project Framework

The security framework proposed in ARMOUR [31] is supposed to serve as a security guide covering the IoT deployment segments. It is supposed to change as far as necessary to respond to the constant evolution in this domain.

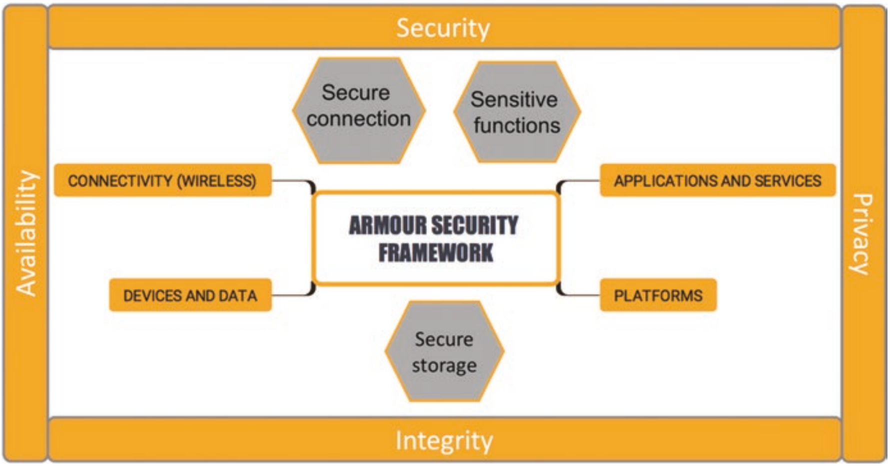


Fig. 2.10 ARMOUR framework overview

Based on the analysis of the proposed security experiments, ARMOUR defines four IoT segments of an IoT deployment:

- Devices and data.
- (Wireless) connectivity
- Platforms.
- Applications and services.

ARMOUR proposes to map OWASP IoT, oneM2M and GSMA to the ARMOUR security framework as depicted in the Fig. 2.10. The ARMOUR security framework defines the security in terms of availability, integrity and confidentiality/privacy. It defines guidelines for each of the four segments described above and identifies elements to be secured.

The ARMOUR security framework takes as its main entry the oneM2M vulnerabilities, threats and risk assessment methodology and identifies eventually missing vulnerabilities and threats based on the seven experiments to be conducted within the project.

2.8 Conclusion

The IoT ecosystem needs to face new security and privacy challenges due to its pervasive nature, the constrained environments (devices and networks), the huge scale of deployments as well as its heterogeneity. Thus, the main challenges and open aspects regarding security and privacy encompass the implementation of an end-to-end holistic approach, protection of collected personal data and identity theft, strengthening of the diverse interfaces and software/firmware, standardisation of the immature domain, assignations of responsibilities regarding privacy and security, scalability issues and largely leverage security analytics.

In this regard, this book chapter has described the main security and privacy threats, vulnerabilities in the Internet of Things as well as diverse ongoing initiatives and projects that are devising new enablers, solutions, frameworks and guidelines to cope with those emerging and evolving security and privacy issues. The security frameworks are starting to provide holistic IoT solutions supporting scalability and adaptability by means of a continuous monitoring-analysing-planning-executing process, including anomaly detection systems facing 0-day/unknown cyberthreats and mitigation plans that adapt and evolve accordingly, keeping all stakeholders properly informed of the security and privacy positioning of the observed cyber-physical system.

Acknowledgments This chapter includes results shared by the European research project Anastacia (Grant Agreement N° 731558), which has received funding from the European Union’s Horizon 2020 Research and Innovation Programme and the Swiss State Secretariat for Education, Research and Innovation.

References

1. Global Opportunity Report 2017, First Edition is published by DNV GL AS. DNV GL AS, Høvik, Oslo Copyright © 2017 By DNV GL AS. This report is available at www.globalopportunitynetwork.org
2. Top ten strategic technology trends 2017, Gartner, October 2016
3. Predictions 2017: security and skills will temper growth of IoT, Forrester, 2016
4. R.H. Weber, Internet of things—new security and privacy challenges. Comput. Law Secur. Rev. **26**(1), 23–30 (2010)
5. M. Haus, M. Waqas, A. Ding, Y. Li, S. Tarkoma, J. Ott, Security and privacy in device to device (D2D) communication: a review. IEEE Commun. Surv. Tutor. **19**(2), 1054–1079 (2017)
6. Thales data Threat Report (2017). https://dtr-fin.thalesesecurity.com/
7. Cisco. IoT threat environment—an overview of the IoT threat landscape with risk-based security program recommendations. White paper (2015)
8. IDC and TXT Solutions, SMART 2013/0037 Cloud and IoT combination, study for the European Commission. http://www.telit2market.com/wp-content/uploads/2015/02/TEL_14016_P_112-114.pdf; 26 Billion “things” may be connected globally by 2020 (2014)
9. Commission staff working document—advancing the Internet of things in Europe, EC, Apr 2016
10. R. Neisse, G. Steri, G. Baldini, Enforcement of security policy rules for the Internet of things, 3rd International workshop on Internet of things communications and technologies (IoT-CT), in conjunction with The 10th IEEE WiMob, Oct 2014
11. G. Baldini, A. Skarmeta, et al. Security certification and labelling in Internet of things, 2016 IEEE 3rd WF-IoT, 12–14 Dec 2016
12. A. Ahmad, G. Baldini, P. Cousin, S.N. Matheu, A. Skarmeta, E. Fourneret, B. Legeard, Large scale IoT security testing, benchmarking and certification, cognitive hyperconnected digital transformation, Chap. 7, pp. 189–220
13. A. Ahmad, G. Baldini, P. Cousin, S.N. Matheu, A. Skarmeta, E. Fourneret, B. Legeard,O. Vermesan, J. Bacquet (Eds), *Large scale IoT security testing, benchmarking and certification, Cognitive Hyperconnected Digital Transformation* (River Publishers, Gistrup)
14. A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, Challenges for securing cyber physical systems. Proceedings of the Workshop on future directions in cyber-physical systems security (2009), p. 5

15. Dimitar Kostadinov, Cyber threat analysis. InfoSec Institute, July 2014. https://resources.infosecinstitute.com/cyber-threat-analysis
16. Threat lifecycle management: overview and solutions. The Sage Group. 2017. http://thesagegrpmentoring.com/wp-content/uploads/sites/524/2017/03/Sage-Group-LE-Solutions-Threat-Lifecycle-Management.pdf. Accessed May 2017
17. E.K. Wang, Y. Ye, X. Xu, S.M. Yiu, L.C.K. Hui, K. P. Chow, Security issues and challenges for cyber physical system. Proceedings of the 2010 IEEE/ACM Int'l conference on green computing and communications & Int'l conference on cyber, physical and social computing. IEEE Computer Society (2010), pp. 733–738
18. Machine to Machine Communications (M2M), Threat analysis and counter-measures to M2M service layer, ETSI TR 103 167 V0.2.1 (2011-01)
19. Y. Gao, Y. Peng, F. Xie, W. Zhao, D. Wang, X. Han et al. Analysis of security threats and vulnerability for cyber-physical systems. In Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference (IEEE, 2013), pp. 50–55
20. Mobile Working Group. *Security Guidance for Early Adopters of the Internet of Things*. (CSA, 2015)
21. Paul Bischoff, Comparing the privacy policy of Internet giants side-by-side, Published 20 Mar 2017. https://www.comparitech.com/blog/vpn-privacy/we-compared-the-privacy-policies-of-internet-giants-side-by-side/
22. J. Tully, Cyber security expert: iPhone X facial recognition is vulnerable, Published 20 Nov 2017. http://www.abcactionnews.com/money/consumer/cyber-security-expert-iphone-x-facial-recognition-is-vulnerable
23. K. McCarthy, Whois? No, Whowas: Incoming Euro privacy rules torpedo domain registration system. Published 26 Oct 2017. https://www.theregister.co.uk/2017/10/26/whois_gdpr_europe/
24. https://www.owasp.org/index.php/Perform_security_analysis_of_system_requirements_and_design_(threat_modeling)
25. oneM2M white paper, January 2015, http://www.onem2m.org/images/files/oneM2M-white-paper-January-2015.pdf
26. GSMA Security Framework CLP11, February, 2016
27. S. Ziegler, A. Skarmeta, J. Bernal, E.E. Kim, S. Bianchi, ANASTACIA: Advanced networked agents for security and trust assessment in CPS IoT architectures. 2017 Global Internet of Things Summit (GIoTS), Geneva (2017), pp. 1–6. doi: https://doi.org/10.1109/GIOTS.2017.8016285
28. A.M. Zarca, J.B. Bernabe, I. Farris, Y. Khettab, T. Taleb, A. Skarmeta, Enhancing IoT security through network softwarisation and virtual security appliances. Int. J. Netw. Manag. **28**(5), e2038 (2018)
29. I. Fzarris, J. B. Bernabe, N. Toumi, D. Garcia-Carrillo, T. Taleb, A. Skarmeta, B. Sahlin, Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems. 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki (2017), pp. 169–174. doi: https://doi.org/10.1109/CSCN.2017.8088617
30. A. Molina Zarca, J.B. Bernabe, I. Farris, Y. Khettab, T. Taleb, A. Skarmeta, Enhancing IoT security through network softwarization and virtual security appliances. Int. J. Netw. Manag. **28**(5), e2038 (2018)
31. ARMOUR—large-scale experiments of IoT security trust. European Union's H2020 project http://www.armour-project.eu/

Chapter 3
End-Node Security

Antonio Skarmeta, Dan Garcia Carrillo, and Alexis Olivereau

3.1 Introduction

Security in IoT is a multidisciplinary area that influences virtually all aspects of a network deployment. From the physical placement of the devices, the process of joining the network, which entails authenticating the devices and authorising their activity in the network to avoid the misuse of the network resources, securing the communications between authenticated parties within the network and preventing and detecting intrusions within the network are some of the aspects that need to be considered regarding the security on the IoT end nodes.

This chapter will cover several aspects, starting from the deployment of IoT devices, how they are securely integrated into the network, to how the end nodes are able to perform their operation securely within the network and how we can prevent and detect intrusions into the network. To achieve this, we consider the state of the art in the area, the work in standardisation organisations such as the IETF and IEEE, as well as innovations that go beyond the state or the art. We see the concept of life cycle of an IoT device and how we can use current standards, such as EAP and PANA for network access authentication of the IoT devices, as well as a lightweight alternative to PANA. We will explore the use of intrusion prevention and detection systems in IoT, analysing the current work done in the area as well as intrusion detection systems (IDS) managed through software-defined networking (SDN).

A. Skarmeta (✉) · D. Garcia Carrillo
University of Murcia, Murcia, Spain
e-mail: skarmeta@um.es

A. Olivereau
CEA, Gif-sur-Yvette, France

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_3

3.2 Security Bootstrapping and Commissioning

3.2.1 What is Bootstrapping

The term bootstrap is defined as "to pull oneself up by one's bootstraps". In computer science it refers to a self-starting process without external input. In the context of the Internet of Things (IoT)—where it is estimated that by 2020, there will be 24 billion devices connected to the Internet [1], most of them operating autonomously with minimal human interaction—bootstrapping brings interesting challenges to achieve a secure and well-managed Internet that is expected to keep growing.

In the area of IoT, bootstrapping is defined as the process of authenticating and authorising a device to enter a security domain [2], gathering the necessary key material to operate in said domain. This process needs to manage a growing number of devices that may belong to different organisations, performing their functions in infrastructures that may not be owned by the organisation operating those devices.

3.2.2 IoT Device Life Cycle

The IoT device life cycle described by Garcia-Morchon et al. [2] (illustrated in Fig. 3.1) is composed of several phases: (*1*) *manufacture*, (*2*) *bootstrapping*, (*3*) *operational*, (*4*) *maintenance and re-bootstrapping and* (*5*) *maintenance*.

Each phase entails one or more actions. The *manufacture phase* refers to the fabrication of the device. The bootstrapping phase entails the physical installation of the device, and its commissioning, where the necessary programming, credentials, etc. are loaded into the device, preparing it to boot up and continue with the necessary process of authentication and authorisation, getting the necessary key

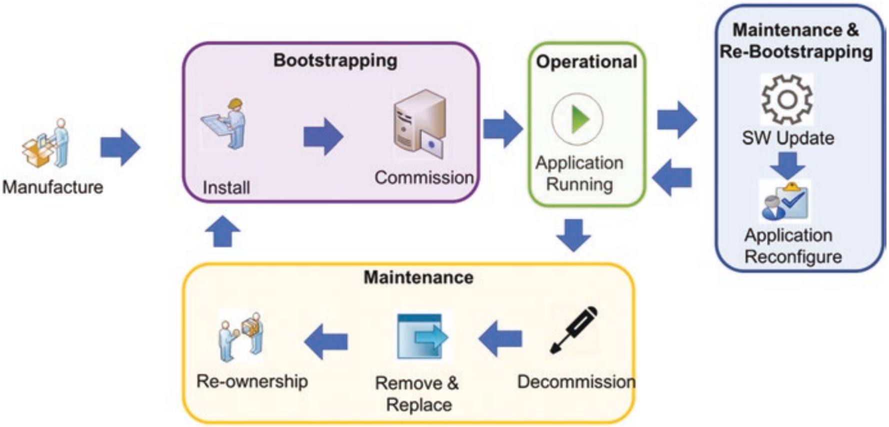


Fig. 3.1 IoT device life cycle (representation of the work of García-Morchon [2])

material for the operational phase. The operational phase refers to the normal operation of the device. In this phase the IoT device uses the key material obtained in the bootstrapping phase.

The *maintenance and re-bootstrapping phase* considers the updates the device may need, after which a new process of bootstrapping is completed again to prepare the device for the operational phase. When the device is no longer usable, it enters in a phase of maintenance where it is decommissioned, removed, replaced or acquired by another party where the life cycle will start again.

We focus here on the *bootstrapping phase*, and we will describe the different steps needed to complete it and propose the protocols to carry it out.

3.2.3 Generic Bootstrapping Framework

Bootstrapping can be seen as a generic framework involving three entities [3]: (1) A bootstrapping client (*BC*), (2) bootstrapping agent (*BA*) and (3) bootstrapping target (*BT*), as depicted in Fig. 3.2.

The bootstrapping client contacts the bootstrapping agent to ask for access to a certain service. This is done using a bootstrapping protocol (A) that can be DTLS, IKEv2, HIP-DEX, 802.1X, EAP, etc. The bootstrapping target provides the service under the guidance of the bootstrapping agent. The bootstrapping target and agent can be co-located. The client and target both communicate using a protocol to access the service. With this basic framework, we propose how we can perform bootstrapping in IoT using current standard protocols and how we can improve the performance in the constrained link.

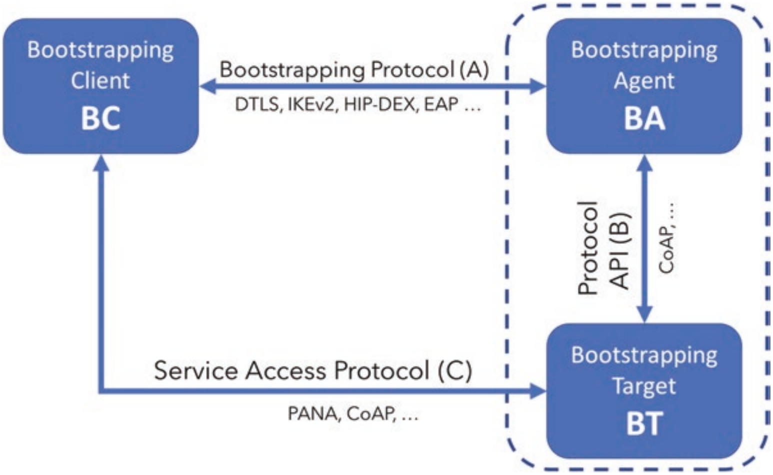


Fig. 3.2 Generic bootstrapping framework

3.3 Setting the Bases for Secure Communications

As we saw in the previous section, to complete the bootstrapping phase, we need to use the credentials that are installed in the device during the commissioning phase. The goal is to integrate the IoT device securely into the network where it is deployed, completing the necessary authentication and authorisation process to join the network, obtaining the necessary key material to interact securely within the security domain. This process needs to support a considerable number of devices, and depending on the deployment, having devices from different organisations operating under the same infrastructure.

To achieve this, we propose the use of Authentication, Authorisation and Accounting (AAA) infrastructures, to manage a great number of devices and provide advanced features such as identity federation. We also propose the use of the Extensible Authentication Protocol (EAP) [4]. EAP is a protocol that allows to run a variety of authentication methods instantiated in what are called EAP methods. EAP methods implement the authentication algorithms, generating and processing the EAP messages to complete the authentication. This gives the necessary flexibility to choose the authentication mechanism that suits the capabilities of the devices or the policy of the organisation where they are deployed. EAP requires a protocol to transport it, known in EAP terminology as an *EAP lower layer*. This protocol can provide more functionality besides transporting EAP. It can manage some aspects of the different IoT devices of the security domain: checking if they are still active, deliberately remove a device from the network, deliver credentials or key material, authorisation information, etc.

A current standard, used by ZigBee IP [5], is the Protocol for Carrying Authentication for Network Access (PANA) [6]. It is an IETF standard to transport EAP and perform network access authentication. As a lightweight alternative to PANA, we propose CoAP-EAP [7]. PANA was not designed with the constraints of IoT in mind, and CoAP-EAP seeks the reduction of resources used to perform the bootstrapping as IoT deployments may have severe restrictions in terms of memory, battery life, limited bandwidth and reduced payloads requirements. CoAP-EAP achieves this using the Constrained Application Protocol (CoAP) [8] to transport EAP with less overhead.

3.3.1 Authentication, Authorisation and Accounting (AAA)

The Authentication, Authorisation and Accounting (AAA) framework supports three security services: authentication, establishes the identity of the user; authorisation, states the conditions in which the user can access the network resources; and accounting, tracks the use of resources. The AAA framework defines a model consisting of an end user (*EU*) who wants to access some network service, an identity provider (*IdP*) that stores the identity of the *EU* and long-term credentials and a service provider (*SP*), who manages the access to the network service. In a scenario that does not uses federation, the IdP and the SP belong to the same organisation (the IdP's organisation). In a federated scenario, the IdP and SP belong to different organisations. The organisations participating in the federation will have independent AAA servers, which will communicate and exchange AAA information among them using an AAA protocol. The most commonly deployed AAA protocols are Diameter [9], widely deployed in 3G networks, and RADIUS [10], used in Wi-Fi and WiMAX. The SP operates the network access server (*NAS*) that communicates with the IoT device and the AAA infrastructure. In the simplest scenario, an AAA infrastructure consists of a NAS, with a direct connection to the AAA server. In more complex scenarios, additional AAA servers (called AAA proxies) can be deployed between the NAS and the AAA server for scalability or to support federated access.

3.3.2 Extensible Authentication Protocol (EAP)

The Extensible Authentication Protocol (EAP) [4] is a standard protocol for authentication. EAP allows the execution of several authentication mechanisms (e.g. based on digital certificates, symmetric keys, etc.), named EAP methods, without the need of changing the protocol. As an example of an EAP method, we can mention EAP-PSK [11], which provides a lightweight authentication mechanism based on pre-shared key (PSK). Other examples of EAP methods, such as EAP-TLS, can be seen in [12].

EAP has been designed with the principle of media independence. That is in this context, the protocol is independent of the wireless technology. By definition EAP is a lock-step protocol, which means it handles a single packet, a request or a response, per flight. Each EAP request is answered with an EAP response. The number of message exchanges depends on the EAP method used. This gives flexibility to choose the authentication that fits best in each case. Every EAP method runs between the EAP peer and the EAP server through the EAP authenticator acting as a forwarder. To start an EAP authentication, the EAP authenticator typically sends an EAP request/identity message to the EAP peer, whom in turn answers with its identity. The identity is sent following the Network Access Identifier (NAI) format [13] (e.g. iot_device@organisation_a.org). The NAI contains the smart object identity, separating the domain name (organisation_a) with an @ sign. Once the EAP server receives the identity of the EAP peer, it is able to select the EAP method to be performed. The EAP method is performed using EAP request/responses between the EAP server and the EAP peer.

There are two models to deploy EAP. On the one hand, we have the EAP standalone model, in which the EAP authenticator and the EAP server are co-located in the same device. This model can be used in small deployments, where no AAA is required. On the other hand, when scalability becomes a must, the EAP pass-through authenticator model can be used. In this case the communication between the EAP pass-through authenticator and the EAP server is done using an AAA protocol.

Common to both cases is the use of an EAP lower layer to carry EAP messages between the EAP peer and the EAP authenticator.

The EAP key management framework (KMF) [14] specifies how EAP methods can generate key material. Two keys are exported after a successful EAP authentication: the Master Session Key (MSK) and the Extended Master Session Key (EMSK). Only the MSK has a defined use for network access authentication in order to run a security association protocol (SAP) to derive Transient Session Keys (TSK). In turn, the TSKs allow to protect the communications between the EAP peer and EAP authenticator. The MSK is sent by the AAA server to the EAP authenticator using the AAA protocol, while the EMSK must not be provided to any other entity, keeping it only between the EAP peer and the EAP server.

Figure 3.3 shows the EAP architecture composed by the EAP peer, authenticator and server. In this figure, we can see the EAP stack of each entity and how EAP is transported with an EAP lower layer between the EAP peer and authenticator and with an AAA protocol between the EAP authenticator and server. There is also important to remark, how the keys are exported, as illustrated, the EAP peer and server export the MSK and EMSK. The EAP authenticator does not export any key but receives the MSK form the EAP server through the AAA protocol, which can be used as shared key material between the EAP peer and authenticator.

3.3.3 Transporting EAP in IoT

Transporting EAP, as commented before, requires an EAP lower layer. A simple alternative would be to transport EAP over the link layer, but it would entail modifying the link layer to support it. For IEEE 802.15.4 [15] there is a standard called IEEE 802.15.9 [16] to transport key management protocol (KMP) datagrams within IEEE 802.15.4. The problem here is that IEEE 802.15.4 is not the only technology used in IoT. For instance, there are several radio technologies conforming what is known as *Low-Power Wide Area Networks* (LPWAN), with a more demanding set of requirements, such as very low bandwidth and smaller payload. Having this in mind, we look for a good performance in the bootstrapping, but we also seek interoperability as a trade-off for not having an optimised solution for each case.

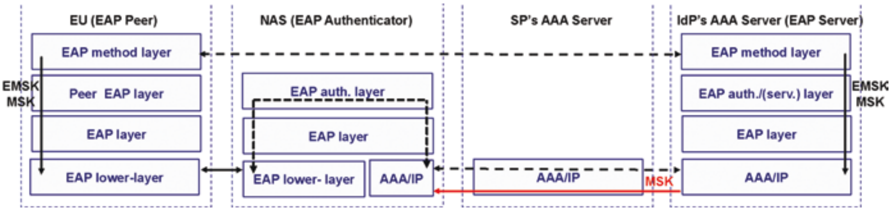


Fig. 3.3 EAP mode pass-through

In this sense, we look for an EAP lower layer to transport EAP in IoT, and we propose two alternatives: (1) Protocol for Carrying Authentication for Network Access (PANA) and (2) CoAP-EAP.

PANA can be used when the restrictions in the link are not as important as to have an interoperable standard with the possibility of adding new functionality. CoAP-EAP is the alternative when interoperability is still needed, but we also seek to reduce the number of bytes sent over the network, due to hard restrictions in the link.

Protocol for Carrying Authentication for Network Access (PANA)

The PANA protocol in IoT is adapted to run in Contiki OS, called PANATIKI [17]. It provides an implementation of the EAP state machine and the PANA protocol adapted for IoT. PANA runs on top of UDP and IP, making it link-layer agnostic. When the EAP authentication is successful, the PANA protocol establishes a PANA session and security association (PANA SA) between the entity that is being authenticated called PANA client (*PaC*) and the authenticator called PANA agent (*PAA*). During the PANA session, the PaC and PAA can exchange messages to reauthenticate and perform liveness tests. This provides to PANA certain flexibility, in the sense that new Attribute-Value Pairs (AVPs) can be defined to extend the functionality of PANA.

Figure 3.4 shows the flow of operation of PANA. As we can see, the exchange is divided in an initial message that starts the process (*step 1*), indicating the PANA agent (PAA), as EAP authenticator, to start the EAP authentication. The next exchange involves nonces (*steps 2 and 3*), and after that the PAA sends the EAP identity request to the PaC (*step 4*). Then the response identity arrives to the PAA (*step 5*); it sends this message to the EAP server (*step 6*), which chooses the EAP method to be used. At this point the EAP method is exchanged between the EAP server and the EAP peer (*steps 7–14*), being transported on top of AAA between the PAA and the EAP server and with PANA between the PAA and the PaC. When the EAP method finishes successfully, the EAP success message arrives to the PaC (*step 16*), which indicates the end of a successful authentication, and the PaC and PAA share key material from EAP, the MSK. With this information the PaC and PAA establish a PANA security association (PANA SA), using the MSK to generate authenticated tag in an AVP called AUTH AVP (*steps 16 and 17*). This provides mutual authentication between the PAA and PaC and gives way to the OPEN phase of the PANA session and as a consequence access to the network for the PAA.

CoAP-EAP

CoAP-EAP is designed as a lightweight alternative to transport EAP in IoT [7]. It integrates the bootstrapping service as an additional CoAP service offered by the Controller of the domain. Being based on CoAP, it runs over UDP, so it is a link-layer agnostic solution. It also establishes a security association between the IoT device and the Controller.

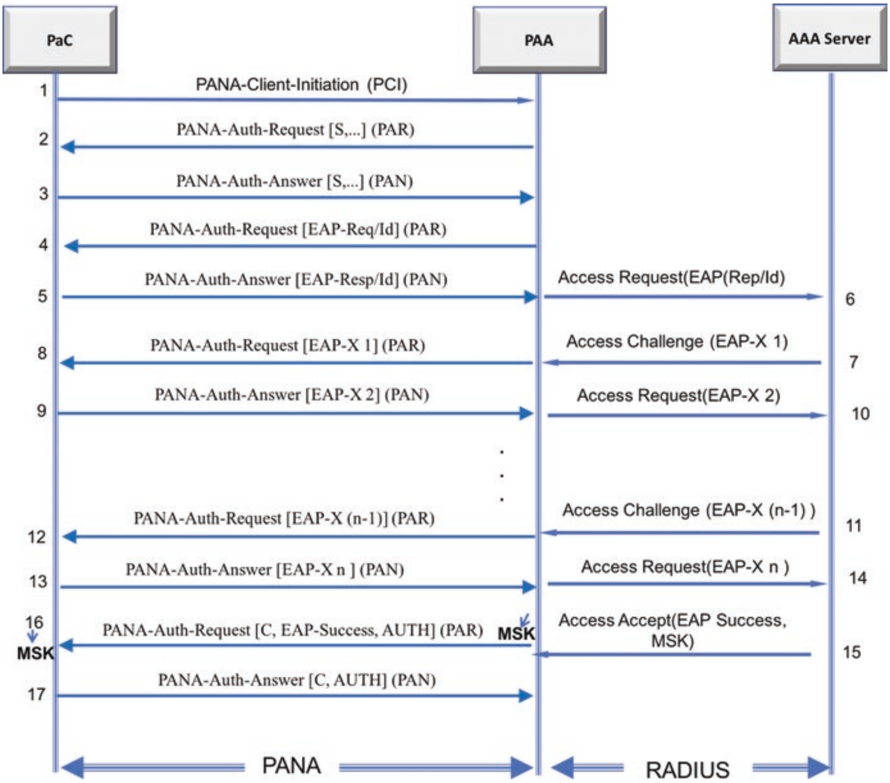

PaC
PAA
AAA Server
1 PANA-Client-Initiation (PCI)
2 PANA-Auth-Request [S,...] (PAR)
3 PANA-Auth-Answer [S,...] (PAN)
4 PANA-Auth-Request [EAP-Req/Id] (PAR)
5 PANA-Auth-Answer [EAP-Resp/Id] (PAN)
Access Request(EAP(Rep/Id) 6
8 PANA-Auth-Request [EAP-X 1] (PAR)
Access Challenge (EAP-X 1) 7
9 PANA-Auth-Answer [EAP-X 2] (PAN)
Access Request(EAP-X 2) 10
12 PANA-Auth-Request [EAP-X (n-1)] (PAR)
Access Challenge (EAP-X (n-1)) 11
13 PANA-Auth-Answer [EAP-X n] (PAN)
Access Request(EAP-X n) 14
16 MSK
PANA-Auth-Request [C, EAP-Success, AUTH] (PAR)
MSK
Access Accept(EAP Success, MSK) 15
17 PANA-Auth-Answer [C, AUTH] (PAN)
PANA
RADIUS

Fig. 3.4 PANA flow of operation

In Fig. 3.5, we can see the flow of operation of CoAP-EAP. It starts when the IoT device sends a POST message to the Controller/*boot* service (*steps 1 and 2*). This indicates the Controller of the network, as EAP authenticator; the IoT device is ready to be authenticated. At this point, the Controller acts as CoAP client and the IoT device as server. They first exchange nonces (*steps 3 and 4*), which give way to the EAP request identity and response identity exchange (*steps 5 and 6*). After this, the Controller sends the EAP response identity to the EAP server, which decides the EAP method to be used (*step 7*). The EAP method is exchanged between the EAP server and EAP client (*steps 8–15*), using an AAA protocol between the EAP server and the EAP authenticator and CoAP-EAP between the EAP authenticator and the EAP peer.

After a successful authentication, the EAP success message arrives to the EAP peer (*step 17*), which is able to establish a security association with the Controller, embedding an authenticated tag in a new CoAP option called AUTH option (*steps 17 and 18*). This provides mutual authentication between the IoT device and Controller and starts the post-bootstrapping phase for the IoT device, which can access services from the Controller, such as network access.

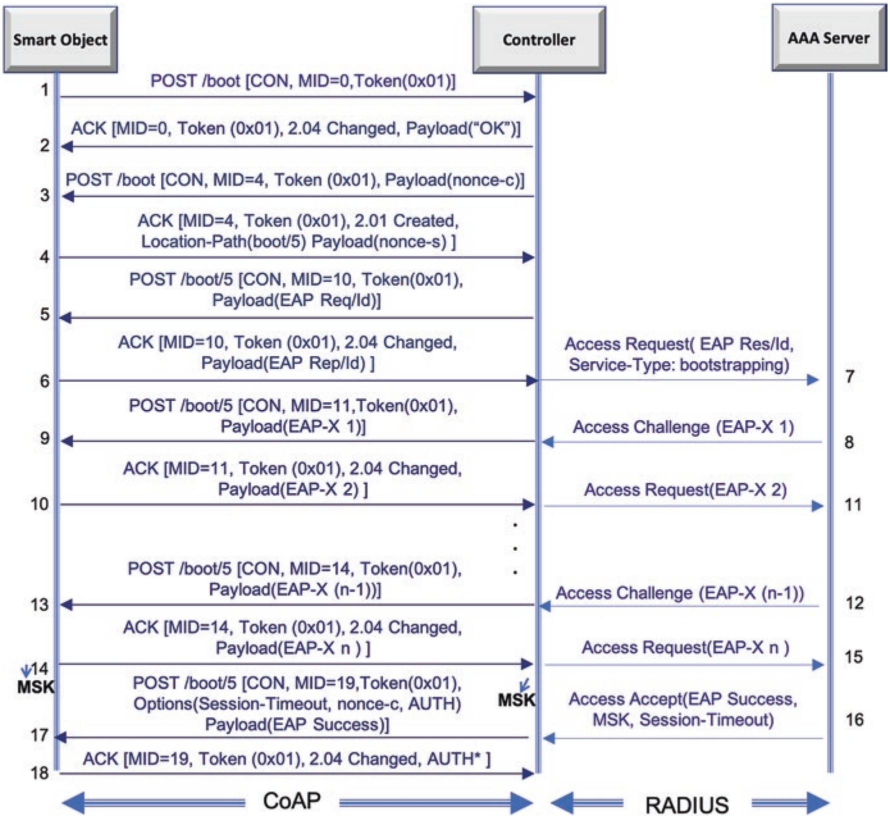

Smart Object
Controller
AAA Server
1 POST /boot [CON, MID=0,Token(0x01)]
2 ACK [MID=0, Token (0x01), 2.04 Changed, Payload("OK")]
3 POST /boot [CON, MID=4, Token (0x01), Payload(nonce-c)]
4 ACK [MID=4, Token (0x01), 2.01 Created, Location-Path(boot/5) Payload(nonce-s)]
5 POST /boot/5 [CON, MID=10, Token(0x01), Payload(EAP Req/Id)]
6 ACK [MID=10, Token (0x01), 2.04 Changed, Payload(EAP Rep/Id)]
7 Access Request(EAP Res/Id, Service-Type: bootstrapping)
8 Access Challenge (EAP-X 1)
9 POST /boot/5 [CON, MID=11,Token(0x01), Payload(EAP-X 1)]
10 ACK [MID=11, Token (0x01), 2.04 Changed, Payload(EAP-X 2)]
11 Access Request(EAP-X 2)
12 Access Challenge (EAP-X (n-1))
13 POST /boot/5 [CON, MID=14, Token(0x01), Payload(EAP-X (n-1))]
14 ACK [MID=14, Token (0x01), 2.04 Changed, Payload(EAP-X n)]
MSK
15 Access Request(EAP-X n)
16 Access Accept(EAP Success, MSK, Session-Timeout)
MSK
17 POST /boot/5 [CON, MID=19,Token(0x01), Options(Session-Timeout, nonce-c, AUTH) Payload(EAP Success)]
18 ACK [MID=19, Token (0x01), 2.04 Changed, AUTH*]
CoAP
RADIUS

Fig. 3.5 CoAP-EAP flow of operation

3.4 Instantiating Bootstrapping in IoT

In Fig. 3.6 we instantiate a generic bootstrapping framework in a scenario with two IoT networks, one from *Organisation A* and another from *Organisation B*. Each IoT network is connected to the Internet and has IoT devices from its own organisation and the other that need to be authenticated to join the network and have access to the services offered by the IoT network (e.g. network access). We identify three entities that are involved in the process of bootstrapping, mapped in EAP terms as EAP server (AAA server), EAP authenticator (Controller) and EAP peer (IoT device).

In the section that communicates the IoT network with the Internet, the AAA server that authenticates the IoT device communicates with the Controller of the network through an AAA protocol (e.g. RADIUS or Diameter) transporting EAP between them. When the EAP authentication is completed, the Master Session Key (*MSK*) is sent to the Controller (the EAP authenticator). In the IoT network, the IoT device communicates with the Controller of the network to authenticate. This exchange is done with an EAP lower layer. When the authentication is completed,

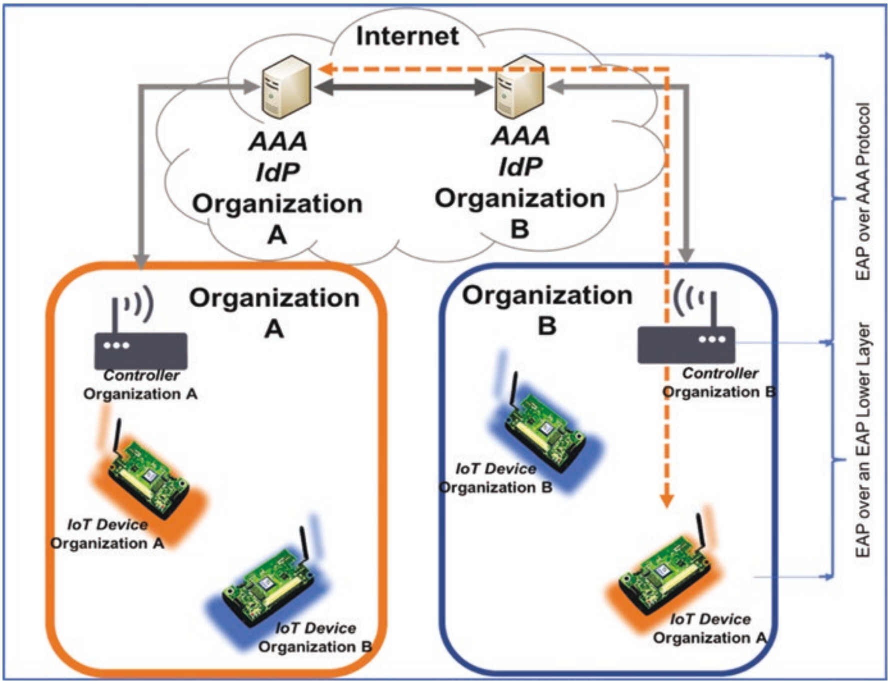


Fig. 3.6 Instantiation of Bootstrapping with AAA and EAP for IoT

the Controller receives the necessary key material (i.e. MSK) to mutually authenticate with the IoT devices, establishing a security association (SA) with the possibility of deriving new key material to bootstrap different security association protocols (SAP) (e.g. DTLS) with fresh key material derived from the MSK.

The architecture to complete a bootstrapping phase using the protocols explained in the previous section is illustrated in Fig. 3.6. As an example of a complete process of bootstrapping, we suppose we have two organisations: Organisation A (represented by the colour orange) and Organisation B (represented by the colour blue). Organisation A installs a device in Organisation B, and when it starts, it has to be authenticated and authorised in the AAA server of Organisation A. For this it starts an EAP authentication, transporting EAP over an EAP lower layer (CoAP-EAP or PANATIKI) between the IoT device and the Controller or the Organisation B. Then the Controller of Organisation B checks the identity of the IoT device of Organisation A and acts as a forwarder between the IoT device of Organisation A and the AAA infrastructure, using AAA to transport the EAP messages. This process is done once, until the session or key material has to be renewed, or following the policy established by each organisation.

3.4.1 After the Bootstrapping: The Operational Phase of the IoT Device

Once the IoT device joins the network, should be able to commence its operational phase. The IoT device (be it is a sensor, or an actuator) should be able to communicate with the Controller or other entities to carry out its main task. These communications have to be secured as well, for what key management and distribution is needed in this phase. If we are talking about establishing a secure channel with the Controller, we can use the existing key material to bootstrap the security association protocol (SAP) that will carry out the communications in the operational phase. As for instance, we can assume that the IoT device needs to establish as COAPS channel (CoAP over DTLS) to send some information. To achieve this the DTLS channel should be established between the IoT device and the Controller, and a pre-shared key can be generated from the MSK to bootstrap DTLS.

3.4.2 Enabling Security Association Protocols (SAPs)

When the bootstrapping is finished, the IoT device is authenticated and authorised to join the network as a consequence of a successful EAP authentication, key material is generated (the MSK), and we can use it to bootstrap other security association protocols (SAP) such as DTLS, OSCORE, etc. to further secure the communications.

The DTLS channel between the IoT device and the Controller of the domain can be bootstrapped in the following ways: (1) The device is authenticated and integrated as part of the security domain through EAP. (2) The IoT device receives a Master Session Key (MSK) that can be used to derive keys to run different security association protocols (SAP) such as DTLS. (3) After a specific key for DTLS (let's call it DTLS_PSK) is derived from the MSK, the DTLS handshake runs activating the DTLS record layer and enabling secure communications over the transport layer.

3.4.3 Communication Between IoT Devices

If the communication is done between the two IoT devices belonging to the same network, both under the security domain of the same Controller, and they need to share key material between them to establish a secure channel, different mechanism can be used to distribute the said key material. This part falls outside of the bootstrapping phase described here, and we will not delve into the details, but we will mention the current work, for instance, in the Internet Engineering Task Force (IETF) Authentication and Authorisation for Constrained Environments Working

Group (ACE WG) that is working in this area. The ACE WG proposes the use of OAuth as a framework for this purpose. The Controller in this case would instantiate the KDC or authentication entity, with which the IoT device would communicate and request the necessary credentials to establish a secure channel between two IoT devices.

3.4.4 Evaluation of EAP Lower Layers PANA and CoAP-EAP

Here we consider the impact of the lower layer has on the performance of the bootstrapping process, based on the comparison between PANA and CoAP-EAP done in [7]. An EAP lower layer imposes an overhead that directly affects the performance of the bootstrapping process in constrained networks.

PANA provides an extensible solution for bootstrapping, but it was not designed considering the constraints of IoT. CoAP-EAP design considers those constraints and provides a lightweight alternative to PANA for IoT.

Overhead as EAP Lower Layer

Although the EAP method used is a big factor in a performance evaluation, among EAP lower layers, the relevance lies in the overhead of the EAP lower layer being used. In the comparison, EAP-PSK is used as EAP method. Although the EAP method could be different, EAP-PSK provides a lightweight method and a concrete example for comparison of both EAP lower layers.

As a base for the experimental results in [7], the message size and the total number of bytes are concluded to be the main factor in the authentication time, the percentage of authentications that are able to finish from all the authentications that start and the energy consumption of both solutions. As it is discussed there, the longer the messages, the more probable is to generate fragmentation in the link, which affects the time and the medium being used, by the messages and through increased number of retransmissions when messages are loss.

Table 3.1 summarises the comparison of PANATIKI and CoAP-EAP message size overhead and the reduction of CoAP-EAP over PANATIKI. In terms of lower layer, CoAP-EAP reduces to approximately half the number of bytes, which is an important improvement. If we consider the exchange as a whole, using the EAP-PSK method as a concrete example, the reduction is of approximately 30% which is also considerable.

Table 3.1 Improvement in percentage, comparing PANA and CoAP-EAP message size overhead

	PANATIKI (bytes)	CoAP-EAP (bytes)	Reduction (%)
EAP lower layer	385	192	~50
EAP lower layer + EAP method (PSK)	596	403	~30

Time, Success Ratio and Energy Consumption

Other important measurements that are influenced by the overhead of the EAP lower layer are the time it takes to complete the bootstrapping (network authentication), the number of authentications that finish in relation with how many start (success ratio) and the energy it takes to complete the bootstrapping (energy consumption). These measurements are done with a Contiki simulator (Cooja) and in different scenarios: (1) with different number of hops between the IoT device and the Controller and (2) with different loss ratios.

These results are summarised in Table 3.2, and we see that the authentication time is improved ranging from 8% to 38%, the success ratio from 8% to 100% and the energy consumption from 5% to 32%. Having this into account, we can say with confidence that the overhead of the EAP lower layer does influence in the performance of the bootstrapping process. Having to choose a solution that fits the needs of IoT, we propose CoAP-EAP when a good performance is a requisite in the IoT deployment.

3.4.5 Conclusions About Security Bootstrapping and Commissioning

As we reviewed the concept of the life cycle of an IoT device and identify the bootstrapping phase as bases for a secure operation within the network and the security domain, bootstrapping sets requirements that need to be met by devices with very different capabilities and with different radio technologies being used in IoT. For this we proposed the use of Authentication, Authorisation and Accounting (AAA) infrastructures, to manage a great number of devices, with advanced features such as identity federation. We also describe how the use of the Extensible Authentication Protocol (*EAP*) can be used to achieve authentication and derive key material. This enables the support of the secure communications of other protocols providing fresh key material. Two different EAP lower layers, PANA and CoAP-EAP, are described. The first, a current standard, and the second, a lightweight alternative. We remark that an EAP lower layer that works independently of the link-layer technology is important when we deal with different radio technologies in IoT, to provide interoperability. We also showed how a lightweight EAP lower layer has an effect on the performance of the bootstrapping process which is important if the constraints of the link and the capabilities of devices are an issue.

Table 3.2 Comparing PANA and CoAP-EAP experimental results (authentication time, success ratio and energy consumption)

CoAP-EAP vs. PANA	Authentication time (%)	Success ratio (%)	Energy consumption (%)
0.0 Loss ratio	8–22	8–100	5–17
0.1 Loss ratio	9–47	11–100	22–29
0.2 Loss ratio	18–38	31–100	27–32

3.5 Intrusion Detection Systems for the Internet of Things

An intrusion detection system (IDS) continuously monitors an asset in order to detect ongoing malicious activities and react to them. As such, IDSs belong to the class of *reactive* security systems, as opposed to *preventive* security systems. While the latter aim at preventing a malicious player from gaining access to critical resources (e.g. by means of cryptography, access control lists or authorisation policies), the former continuously survey critical assets in order to detect attacks that may have passed the preventive systems protection. These two classes of security systems ideally complement one another, the reactive systems typically offering a second line of defence, against stealth or internal attackers that would not have been defeated by the—mandatory—preventive first line of defence. Examples of systems belonging to these two classes are given on Fig. 3.7.

Various classes of IDSs are defined, depending on the asset type. One distinguishes especially host IDS (HIDS), which is in charge of detecting suspicious activities occurring on a host (e.g. failed login attempts, unusual access to system files, etc.), and network IDS (NIDS), which focuses on network-based threats (e.g. botnet control traffic, port scanning, etc.). NIDSs can exist under a monolithic form (one single physical entity hosts all IDS-related functions) or a distributed form (the NIDS is made up of a plurality of components, typically many detection probes interconnected with alert monitoring and/or reaction systems). Intrusion detection systems can be qualified as intrusion prevention systems (IPSs) if they support attack deterrence mechanisms. A typical example is that of an IPS located within an enterprise firewall and capable of dynamically interrupting malicious network traffic upon identifying it as detrimental. Note that while qualified as belonging to the class of reactive security components, an IPS actually plays a prevention role.

While historically restricted to being used for protecting corporate intranets, IDSs are gaining momentum in a wide variety of technical areas [18, 19]. Recent subtle, combined or multistage attacks have indeed shaken the opinion [20] and have made security designers attempt to design systems as secured as possible, especially featuring both preventive and reactive security mechanisms. This is especially true with respect to critical infrastructures such as water or energy distribution, collaborative transport infrastructures or autonomous vehicle and advanced manufacturing. As part of this trend, specific IDSs had to be designed for the Internet of Things.

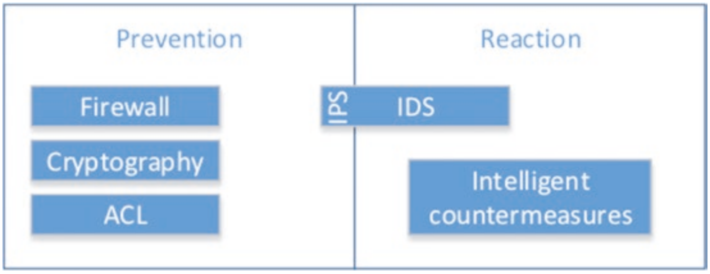


Fig. 3.7 Examples of prevention and reaction security mechanisms

3.5.1 Introduction of the Challenge

The problem of IDS specifically designed for the IoT is both unique and challenging. This is due to four combined causes, which are further elaborated below. First, the IoT environment exhibits several characteristics that emphasise the need for both preventive and reactive security systems. Second, the IoT presents specificities that make existing prevention solutions less efficient—and consequently increase the interest of reactive solutions. Third, the IoT also present specificities that also make the development of reactive systems more complex; this means that “classical” primitives used for building IDS in other environments will have to be largely adapted. Fourth, the IDSs that are being proposed for the IoT are still at their early stages today; especially, they cannot be used straightforwardly in the wide variety of contexts that characterise the IoT.

3.5.2 IoT Environment and the Need for IDS

There are multiple reasons that prompt the use of intrusion detection systems in the IoT world. First, IoT devices are often interacting with physical world entities without active human user involvement. As such, they represent a target of choice for an attacker, since their compromise does not only mean a point of entry to an IT communication system but also the capability to impact the behaviour of other functional systems with good chances of remaining unnoticed. While the consequences can be potentially critical for corporate systems (e.g. disruption or destruction of manufacturing units), they can also be serious for an individual (e.g. theft of private data, hack of physical objects, physical intrusions). The second reason does not relate to the criticality of IoT-driven scenarios but to the very essence of IoT devices and networks. Indeed, when compared to legacy communication networks, IoT (edge) networks exhibit the following specificities:

- Involvement of a number of nodes greater by multiple orders of magnitude than that of the legacy intranet networks. From the viewpoint of security, this massive deployment can be critical because large numbers of these nodes are fully identical (and thus exhibit the same, potentially flawed, static preventive countermeasures) and also because swarm deployment can lead to the emergence of unplanned group behaviours for which static preventive countermeasures would prove inefficient and which pre-release threat analyses are likely to have missed.
- Nondeterministic communications path with a mesh structure. Especially, it can in general not be assumed that all communication flows will at some point cross a security gateway in which they can be scrutinised. Recent past has shown that efficient attacks could propagate from IoT end node to IoT end node, without crossing a single IP router [21].
- Diversification of communicating device manufacturers, especially new players with limited knowledge on security analyses, primitives and protocols—and

security by design in general. Typically, the systems designed by these new players will have to be secured *after* they are on the market, which advocates for an independent security monitoring system, typically an intrusion detection system. A concurring specificity is the fact that the lifetime of IoT devices, even if produced by security-capable players, is likely to outlive their manufacturing company and thus to be left for years without proper support.

- Vulnerability of end devices to physical attacks, due to their location in emplacements outside of a security perimeter. This means that end devices in an IoT network are more likely to be compromised and have therefore to be scrutinised from an external viewpoint.
- Complex security patching system, often relying on heavy firmware update procedures, which users are reluctant to carry out due to their difficulty, the resulting temporary interruption of service and the lack of sensitivity to security problems.

Shortcomings of Prevention Systems in the IoT World

In addition to the points highlighted in the previous section, reactive security solutions are also even more interesting as classical preventive ones perform in a suboptimal manner in an IoT environment. This is due to the shortcomings of IoT devices present in terms of computational power, battery and memory.

Limited computational power and battery are problematic in that they mean that complex cryptographic algorithms (as usual as the Diffie-Hellman key agreement scheme) may not be supported, which in turn decrease the efficiency of integrity-preserving or anti-spoofing protocols.

Limited memory space may also alter the proper operation of cryptographic algorithms. For example, it can prevent a node from remembering already used nonces, thereby exposing it to replay attacks. It will also make the implementation of stateful systems (such as stateful firewalls) more problematic, thereby decreasing their efficiency. Finally, it would also lead to oversimplification of communication security schemes, leaning these into insecure approaches such as static and/or short shared secrets.

Limited computing power and memory space also mean that hypervised execution environment and virtualisation in general can barely be suitable to the IoT world, which in turn exposes IoT nodes to more compromising attacks.

Having highlighted the shortcomings of prevention systems for the IoT, it is worth repeating that these systems are nevertheless always mandatory and that reactive schemes can only come as complement to them.

IoT-Induced Challenges for the Development of IoT-Specific IDSs

The same physical constraints that restrain the efficiency of preventive security mechanisms can also affect that of reactive ones such as IDSs. It is worth considering these constraints from the viewpoint of a security system based on network monitoring and misbehaviour identification. Of course, these constraints that pertain to IoT nodes characteristics are relevant only if the IDS system has to run on these very devices.

- Limited computing power may limit the strength of mathematical behavioural analyses carried out for attack detection. This type of attack detection methods will be reviewed in what follows.
- Limited battery especially means that a battery-powered device cannot afford to continuously monitor a radio link in order to identify ongoing attacks, since keeping its antenna in a receiving state would consume energy at an unacceptable rate.
- Limited memory will straightforwardly limit the number of attacks that can be recognised by an IDS. As it is the case with a firewall, a limited memory space means that fewer attack signatures can be stored. It also means that less complex data structures can be kept in memory, as would be required to identify subtle or combined attack scenario. For example, identifying a port scanning attack requires to be able to associate together multiple connection attempts originating from the same node and destined to different ports on a single target, which in turn requires a corresponding data structure to be maintained for each possible attacker.

In addition to these IoT device-specific constraints, another constraint exists that is specific to the IoT environment in general and that holds even if the IDS is not implemented on IoT end devices.

- The effort required to monitor IoT communication technologies such as 6LoWPAN/802.15.4 or Z-Wave is considerably higher than that required to monitor classical wireless technologies such as 802.11. Specific antennas, chipsets and kernel modules are likely to be required as prerequired building blocks for an IoT-specific IDS, which make these systems more difficult to develop and maintain.

Finally, three other constraints affect the development of reactive systems in general:

- The lack of memory means that IoT devices will in general provide no single line of log for postmortem analysis. Whatever attacker traces should preferably be obtained “in real time”, because it will very likely be too late once the attack has been carried out.
- The lack of a graphical interface, combined with the complexity of remote access (UART/JTAG), means that an IoT device under attack will be all the more complex to pinpoint as such.
- A large number of attack deterrence mechanisms will not be suitable to the IoT traffic; for example, QoS degradation of a suspicious flow whose bandwidth is already very would likely prove inefficient.

Limitations of the Existing Art

A fair number of solutions have started being proposed for the IoT environment. Historically, a very large of them were defined for the wireless sensor networks (WSNs) [22–25] or the mobile ad hoc networks (MANETs) [26, 27] architecture. These approaches complementarily pioneered important aspects of IoT intrusion detection.

WSN IDSs largely concentrated on detecting routing-based attacks such as black hole, grey hole, worm hole and Sybil attacks. These attacks still exist in today's IoT world, and the ability to detect them is critical for an efficient design. WSN IDSs also addressed complex problems of network monitoring responsibility, trying to answer the question of the location of the monitoring function in a battery-constrained world. This question was diversely answered to, certain systems proposing to instantiate the detection function in non-battery-powered hierarchical nodes (e.g. cluster head), others designing complex methodologies for ensuring fairness in the regular assignment of the monitoring role to all nodes within the WSN topology.

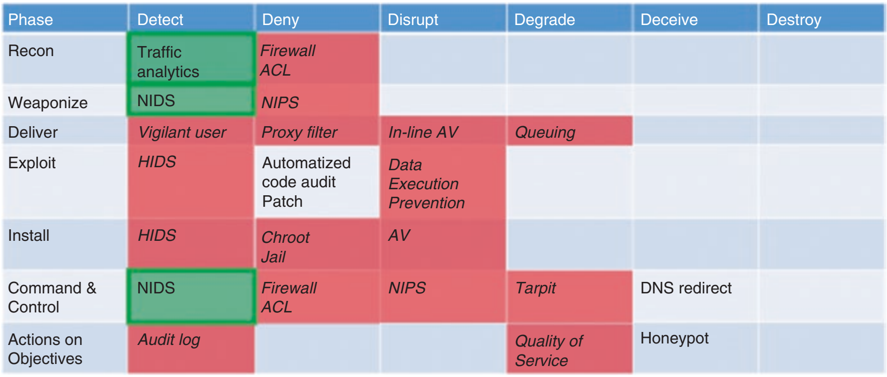
IDSs for MANETs were designed for highly mutable environment where nodes would dynamically change their respective location. As such, they further improved the quality of routing-specific attack detection. They also considered relationship between competing nodes, part of the same topology but possibly subject to selfishness without having been compromised. They contributed to the development of trust models allowing to assess the trustworthiness of a misbehaviour report.

Recent trends in the development of IoT intrusion detection systems include the extension of existing legacy IDSs to support IoT-specific protocols [28, 29] and the development of new detection methods based on machine learning techniques [30–32]. While the former aspect is relevant to practical deployment, it needs to be complemented with more dynamic techniques such as those investigated in the latter. Nevertheless, the corresponding scientific works are however often far from practical considerations. For example, some machine learning-based threat detection systems are designed so as to maximise the detection capability (which is good); yet this comes at the expense of impractical (and even, prohibitive) false-positive rate.

Synthesis

As a short synthesis, an extended version of the cybersecurity reactive countermeasure table introduced by Shostak in [30] is presented in Fig. 3.8.

Most proposed countermeasures in the degrade/disrupt/deceive classes fail, because of their unsuitability to the IoT world, as highlighted above. This advocates for a major focus to be applied in the detection of the attack, where traffic analysis—capable or more subtle network intrusion detection systems—proves of paramount importance.



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Recon	Traffic analytics	*Firewall ACL*				
Weaponize	NIDS	*NIPS*				
Deliver	*Vigilant user*	*Proxy filter*	*In-line AV*	*Queuing*		
Exploit	*HIDS*	Automatized code audit Patch	*Data Execution Prevention*			
Install	*HIDS*	*Chroot Jail*	*AV*			
Command & Control	NIDS	*Firewall ACL*	*NIPS*	*Tarpit*	DNS redirect	
Actions on Objectives	*Audit log*			*Quality of Service*	Honeypot	

Fig. 3.8 Cybersecurity countermeasures at various attack stages

3.5.3 Architectural Solution

Having identified the need for an IDS in order to appropriately secure an IoT system, it is now worth defining the architecture that the IDS has to use. A few questions have to be answered. How to design the probes? How to interconnect them securely with the system under surveillance? Which detection methods to choose? What to do once an attack has been detected? These questions are answered in what follows.

Probes Location

The first and paramount decision pertains to the number and location of the detection probe(s). From the topologies of most IoT deployment, more than one probe should be deployed in order to monitor the maximum possible surface (if not the entirety) of the IoT network. The choice of the locations of the probes typically conforms to one of the two following approaches:

- IDS probes are logical functions hosted by physical entities that are part of the monitored IoT network. This approach ensures that attack detection components are on the path to the vulnerable components. If the device hosting the IDS probe is powerful enough, the IDS may be enriched with additional feature such as host monitoring (HIDS) or intrusion prevention (IPS). However, battery-powered devices can hardly monitor a wireless link for a long time, and eventually this approach would end up putting the most detection-capable functions within sector-powered nodes, which in turn contradict the "maximum coverage" requirement.
- IDS probes are physical entities that are external to the monitored IoT network. This approach comes at the expense of the deployment of a parallel network to the IoT network being monitored, which could be costly and somewhat complex to manage. On the other hand, this approach allows deploying probes wherever necessary.

Unless the IoT network topology so permits (e.g. powerful sector-powered end nodes + wired links – both existing in CPL networks, for example), the second approach is recommended.

Security Enforcement

A very important point in the deployment of an IDS system is the fact that the probes should not themselves create a vulnerability in the system being monitored. This represents an additional reason for separating the architecture of the monitoring network from that of the monitored network. Even then, the software and hardware architectures of the probe should be carefully designed so as to protect them from harmful intrusions. A robustified probe software should have been audited by means of specific software validation tools. A robustified hardware probe architecture may rely on data diode, in order to make sure that the diode will behave in a purely passive way.

Detection Methods

Intrusion detection systems rely on two detection method families in order to identify malicious activity.

Signature-Based Detection

Signature-based detection compares network traffic (inner packet content, communication patterns, etc.) with a signature base that contains signatures of known attacks. It allows efficient identification of known attacks, as long as the database is up-to-date.

Behavioural Analysis Detection

Behavioural analysis identifies possibly malicious activity by comparing network traffic (again, the set of parameters that are considered can include packet-specific and pattern-specific data) to a model of benevolent traffic. It requires that a model of “normal” network behaviour has been generated first, from which it will raise alerts when a deviation exceeding a certain threshold has been observed. Behavioural analysis can therefore identify malicious activity for which no signature exists. Conversely, behavioural analysis can mistakenly raise an alert for a non-malicious activity that corresponds to an unusual network traffic.

As explained, behavioural analysis requires that a “normal” behaviour be defined. For doing so, the underlying machine learning primitive has to be trained in order to recognise this normal traffic. This implies the following constraints:

- Traffic example with 0% malicious activity must be available, in a sufficient duration/with a sufficient variability to allow the training.
- The said variability is important in order to avoid overfitting the machine learning to a very limited set of communication patterns, thereby making it trigger false-positive alarms whenever the network somewhat deviates from the learnt behaviour.

Better results can be achieved if one does not only restrict to teaching the machine learning primitive to recognise the legitimate network behaviour but actually teaches it to recognise classical attack patterns. This embodiment of behavioural analysis requires the availability of a labelled data set, indicating for each packet (or connection) whether this packet (or connection) is a malicious one and optionally the attack class it involves. Of course, the detection quality only improves insofar the detection system encounters attacks that belong to classes that it was taught to recognise.

3.5.4 Reaction Systems

Intrusion detection systems do not restrict to the "detection" part. Once an attack has been detected, the system takes appropriate action(s) in order to limit the harm it may cause to the monitored system. These actions are carried out by dedicated reaction subsystems. These latter can be qualified as passive or active according to whether they dynamically reconfigure the network under attack (active systems) or not (passive systems).

Passive Reaction Subsystems

Passive reaction subsystems will mostly rely on notifying a network administrator. This notification can occur immediately after an incident has been detected or after a few suspicious activities have been identified and correlated. The form the notification takes can be highly diverse, ranging from a basic email to an advanced alert displayed within a security information and event management (SIEM) system visualisation console.

Active Reaction Subsystems

Active reaction systems dynamically reconfigure the network under attack, in line with the cognitive network's *self-healing* property. This property can prove especially useful in IoT scenarios, where machine-to-machine interactions without human user involvement make it largely inefficient to wait for patching actions carried out by a network administrator.

Yet, active reaction interest has to be carefully weighed, since:

- It breaks the separation rule between the monitored infrastructure and the monitoring infrastructure.
- It can itself be exploited by an attacker who may thus trigger the monitored network to be reconfigured in an advantageous way.

A large number of reactive countermeasures exist such as:

- Exclusion of a malicious node from the IoT network. This exclusion can occur, for example, by means of layer 2 filtering, layer 3 filtering (iptables) or by rekeying the legitimate nodes without letting the malicious one learn the new key.
- Redirection of a supposedly malicious flow towards a honeypot for further observations and analyses.

3.5.5 Deployment Scenario and Validation

Figure 3.9 below presents an IDS deployment architecture wherein both the monitoring network (interconnected IDS probes) and the monitored network (asset to protect) can be controlled by means of software-defined networking (SDN).

The interest of this approach is threefold.

- First, the IDS security service can be implemented as a centralised SDN service, hosted by an SDN controller and communicating with SDN devices (IDS probes) through the southbound interface of the controller. This guarantees a robust and efficient information transport framework between the probes and the central IDS server.

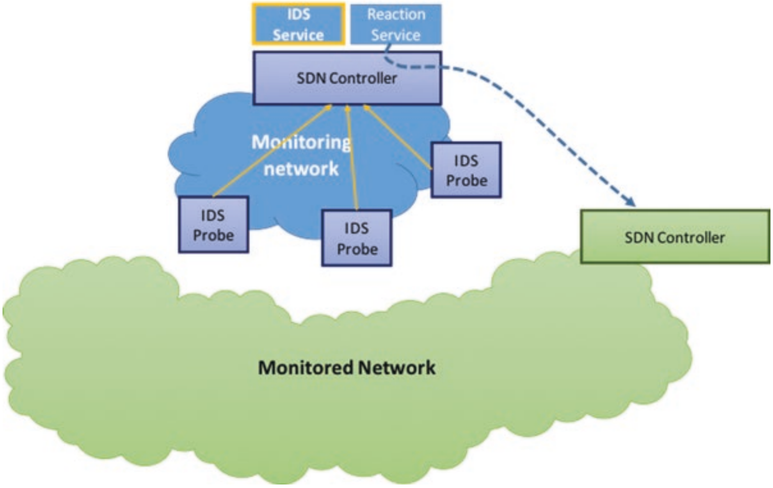


Fig. 3.9 SDN-based deployment

- Second, the detection and reaction subsystems are instantiated as two separate SDN services running on top of the SDN controller. This allows for better control of orders flowing from the detection to the reaction part.
- Third, the reaction countermeasures are themselves carried in a standardised and controllable form from the SDN controller of the monitoring network to that of the monitored network, which further increases the security of the reaction subsystem.

3.5.6 Conclusion

The best practices listed in Table 3.3 should be enforced when designing an intrusion detection system for the Internet of Things.

Security involves many aspects of the IoT devices: the process of commissioning, authentication and authorisation to join the network, getting the necessary key material or credentials to operate securely, etc. Furthermore, preventing and detecting intrusions are also part of maintaining the network secured, minimising their influence on the overall system.

Here we reviewed the life cycle of an IoT device and focused on the first step that lays the groundwork to secure the communications throughout the IoT device; we presented how AAA infrastructures can support authentication, authorisation needs of large IoT deployment, how EAP can provide the needed flexibility to select the appropriate authentication method according to each organisation's needs, plus how key material can be derived to bootstrap different security association protocols; and we propose two different EAP lower layers (protocols to transport EAP) in IoT. We also reviewed mechanisms to prevent and detect intrusions minimising the influence of rogue or planted IoT devices into the system as well as saw new approaches to managing the intrusion detection systems (IDS) using software-defined networking (SDN).

Table 3.3 Best practices for IoT IDS design

Generic architecture	Probe location	A distributed architecture should be favoured
		The monitoring devices should be separated from the monitored ones
Detection	Probes	Hardware security (e.g. diode) should be enforced
		Software security (e.g. code auditing or hypervised environment) must be enforced
	Methods	Attack signatures must be used
		Behavioural analysis could be used especially in deterministic systems
Reaction	Interface	A controlled interface between from the reaction subsystem to the monitored system should be used

Acknowledgments This chapter includes results shared by the European research project USEIT (Grant Agreement N° 731558), which has received funding from the European Union's Horizon 2020 Research and Innovation Programme and CHIST-ERA PCIN-2016-10.

References

1. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
2. O. Garcia-Morchon, S. Kumar, M. Sethi, "State-of-the-art and challenges for the internet of things security." [Online]. https://tools.ietf.org/html/draft-irtf-t2trg-iot-seccons-05
3. H. Tschofenig, Enriching bootstrapping with authorisation information. Internet-draft draft-tschofenig-enroll-bootstrapping-saml-02, internet engineering task force, 2005. Work in Progress
4. J. R. Vollbrecht, B. Aboba, L. J. Blunk, H. Levkowetz, J. Carlson, "Extensible Authentication Protocol (EAP)." [Online]. https://tools.ietf.org/html/rfc3748
5. "Zigbee IP and 920IP | Zigbee Alliance"
6. Y. Ohba, B. Patil, D. Forsberg, H. Tschofenig, A.E. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)." [Online]. https://tools.ietf.org/html/rfc5191
7. D. Garcia-Carrillo, R. Marin-Lopez, Lightweight CoAP-based bootstrapping service for the internet of things. Sensors **16**(3), 358 (2016)
8. Z. Shelby, K. Hartke, C. Bormann, "The Constrained Application Protocol (CoAP)." [Online]. https://tools.ietf.org/html/rfc7252
9. J. Arkko, G. Zorn, V. Fajardo, J. Loughney, "Diameter Base Protocol." [Online]. https://tools.ietf.org/html/rfc6733
10. S. Willens, A.C. Rubens, C. Rigney, W.A. Simpson, "Remote Authentication Dial In User Service (RADIUS)." [Online]. https://tools.ietf.org/html/rfc2865
11. F. Bersani, H. Tschofenig, "The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method." [Online]. https://tools.ietf.org/html/rfc4764
12. "The EAP TLS Authentication Protocol." [Online]. https://tools.ietf.org/html/rfc5216
13. A. D. <aland@freeradius.org>, "The Network Access Identifier." [Online]. https://tools.ietf.org/html/rfc7542
14. B. Aboba, H. Levkowetz, D. Simon, P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework." [Online]. https://tools.ietf.org/html/rfc5247
15. IEEE Standard for Low-Rate Wireless Networks, *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)* (2016), pp. 1–709
16. IEEE Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams, *IEEE Std 802.15.9-2016* (2016), pp. 1–74
17. P.M. Sanchez, R.M. Lopez, A.F.G. Skarmeta, PANATIKI: a network access control implementation based on PANA for IoT devices. Sensors **13**(11), 14888–14917 (2013)
18. K.M. Sharmilee, R. Mukesh, A. Damodaram, V. Subbiah Bharathi, *"Secure WBAN using rule-based IDS with biometrics and MAC authentication," HealthCom 2008-10th International Conference on e-health Networking* (Applications and Services, Singapore, 2008), pp. 102–107
19. M. Gmiden, M.H. Gmiden, H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," 2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Sousse, 2016, pp. 176–180
20. G. Liang, S.R. Weller, J. Zhao, F. Luo, Z.Y. Dong, The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Trans Power Syst **32**(4), 3317–3318 (2017)
21. E. Ronen, A. Shamir, A.O. Weingarten, C. O'Flynn, IoT goes nuclear: creating a ZigBee chain reaction. IEEE Symp. Secur. Privacy **2017**, 195–212 (2017)

22. S. Shin, T. Kwon, G.Y. Jo, Y. Park, H. Rhy, An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. IEEE Trans: Indust. Informat. **6**(4), 744–757 (2010)
23. R. Roman, J. Zhou, J. Lopez. “Applying intrusion detection systems to wireless sensor networks,” In Proceedings of IEEE Consumer Communications and Networking Conference (CCNC'06), Las Vegas, USA, 2006, pp. 640-644
24. K. Ioannis et al., *Toward intrusion detection in sensor networks* (13th European Wireless Conference, Paris, 2007)
25. M. Bahria, A. Olivereau, A. Boudguiga, A hybrid threat detection and security adaptation system for industrial wireless sensor networks, in *Self-Organizing Systems*, (Springer, Berlin, Heidelberg, 2014), pp. 157–162
26. C.V. Zhou, C. Leckie, S. Karunasekera, A survey of coordinated attacks and collaborative intrusion detection. Comput. Secur. **29**(1), 124–140 (2010)
27. C. Xenakis, C. Panos, I. Stavrakakis, A comparative evaluation of intrusion detection architectures for mobile ad hoc networks. Comput. Secur. **30**(1), 63–80 (2011)
28. S. Raza, L. Wallgren, T. Voigt, SVELTE: real-time intrusion detection in the internet of things. Ad Hoc Netw. **11**(8), 2661–2674 (2013)
29. P. Kasinathan, C. Pastrone, M.A. Spirito, M. Vinkovits, *Denial-of-Service detection in 6LoWPAN based internet of things. In Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference* (IEEE, New York, 2013), pp. 600–607
30. C. Liu, J. Yang, Y. Zhang, R. Chen, J. Zeng, *Research on immunity-based intrusion detection technology for the Internet of Things. In Natural Computation (ICNC), 2011 Seventh International Conference*, vol 1 (IEEE, New York, 2011), pp. 212–216
31. C. Jun, C. Chi, *Design of complex event-processing IDS in internet of things. In Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference* (IEEE, New York, 2014), pp. 226–229
32. A. Gupta, O.J. Pandey, M. Shukla, A. Dadhich, S. Mathur, A. Ingle, *“Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks”, 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (IEEE, New York, 2013), pp. 1–7

Chapter 4
IoT and Cloud Computing: Specific Security and Data Protection Issues

Luca Bolognini and Paolo Balboni

4.1 Introduction

The ongoing demand of IT services suited to meet the increasing needs of individuals and, in general, the economy has resulted in a steady increase in the number of servers used in data centres and in the use of virtualisation, as a storage technique.

Cloud computing (hereinafter referred to as "cloud") may represent the right answer to this growing demand and, at the same time, the result of a technological revolution, which has started during the last decade.

The combination of ease of use and cost-efficiency characterises the cloud infrastructure, which in turn aims at guaranteeing a significant saving in administrative costs for those who choose to make a use of it, when compared to standard non-cloud software.

That is, by adopting a system for storing and processing resources in the cloud infrastructure, the customer purchases computing, storage and other IT services.[1] It is clear the reason why Gartner, a major market research firm, estimated that cloud computing could become "one of the most disruptive of IT spending since the early days of the digital era".[2]

At the same time, other technological innovations propose new modalities for the development of the Internet and determine the affirmation of the Internet of things.[3]

[1] P. Balboni, Il cloud computing e l'internet of things ("IoT"): come minimizzare i rischi legali, 2016, p. 27.

[2] ivi, p. 26.

[3] The definition of the "Internet of things" has been given by Kevin Ashton while working at Procter & Gamble: "[i]f we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best" (Web Magazine Radio Frequency Identification Journal, 1999).

L. Bolognini (✉) · P. Balboni
Istituto Italiano per la Privacy, Rome, Italy
e-mail: l.bolognini@istitutoprivacy.it

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_4

This could be considered as a true revolution, no less important and disruptive than the cloud, which began with the development and spreading of smartphones and then determined technological evolution characterised by somewhat uncontrollable and inscrutable implications.[4]

Therefore, both IoT and cloud could become central assets for businesses, often inseparably linked to each other. Their interaction is determined, on the one hand, by the large amount of data that the IoT is able to generate and, on the other hand, by the power and flexibility with which the cloud is capable of in supporting the IoT.

4.2 Cloud Computing

The word "cloud" recalls the main feature of the technology, that is, virtualisation. In particular, cloud consists of a series of service technologies and models focused on the use and supply of computer applications, processing capabilities, storage and memory usage based on the use of the Internet.

Although many definitions of what can be qualified as cloud have been given throughout the years, the National Institute of Standards and Technology (NIST) has provided a formal interpretation, in the following terms:

"Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction".[5]

Such description certainly emphasises the peculiarity of the technology itself, which at the same time puts into practice the innovative nature of eliminating the physical component of the single computer server and storing the data in data centres located in areas where maintenance and administrative costs are lower and then made accessible to the customer via the Internet connection of any type of device.

4.2.1 Subjects of the Cloud Computing

The above-mentioned definition focuses on cloud's features, with no information on the structure that the cloud itself might assume: given its complexities, practical models are, in fact, many as well as indefinable. Corresponding to the indefiniteness of the cloud, several are the subjects involved in its structure.

However, it is assumed that the main players/subjects are two[6]:

[4] See also, Aspen Institute: https://www.aspeninstitute.it/system/files/inline/Internet%20of%20Things.pdf.

[5] P. Mell, T. Grance, The NIST Definition of Cloud Computing, Version 15, 2009.

[6] G. Malgieri, I soggetti coinvolti nel trattamento dei dati personali nel cloud computing la rottura del dualismo controller—processor, Op. J. Vol. I, n. I/2015.

1. The cloud consumer: that is, the end user or the subject that has a business relationship with the cloud provider, who/that uses a service under a contract.
2. The cloud provider: that is, the subject that provides, guarantees and ensures the service. It purchases and manages the infrastructure in order to provide cloud services and makes all that is necessary for the cloud customer to access such services. However, it should be noted that there are more levels of service provision, and therefore it is possible to further distinguish between:
   (a) Primary cloud provider, whose services are "original".
   (b) Intermediary cloud provider that provides services of other providers, incorporating them into its own service and thus making this "sub-supply" invisible to the end user.[7]

The trick of cloud environments is, therefore, primarily to identify who has a certain role and, consequently, who should fall under the different responsibilities and obligations set out by the European law on data protection.

In view of the enforcement of Regulation EU 2016/679, the General Data Protection Regulation (hereinafter "Regulation" or "GDPR"), starting from May 25, 2018, many of the main cloud providers operating in the European market have chosen to adopt the Code of Conduct on Data Protection proposed by the association of Cloud Infrastructure Services Providers in Europe (CISPE),[8] which brings together suppliers of millions of customers across Europe. CISPE Code of Conduct provides for a framework of compliance standards that allow customers to clearly identify whether their infrastructure provider is adopting adequate data protection standards in line with existing European standards, and above all, with the GDPR.

4.2.2 Personal Data Protection in the Cloud

There are currently no specific regulatory provisions in the field of data protection in the cloud environment, so what is below referred to are interpretative, though authoritative, indications.

At European level, the interest of lawyers and technicians, especially at the starting point of the cloud phenomenon, has been addressed to the guidelines issued

[7] Under a data protection point of view, it should be then further assessed when the provider is to be considered as a data controller (defined by Article 4.1.7 GDPR as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law) or as a data processor (described by Article 4.1.8 GDPR as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller).

[8] Cloud Infrastructure Services Provider in Europe.

by the European Union Agency for Network and Information Security (ENISA), which provided several useful indications.[9]

An in-depth study of the legal implications of cloud was then carried out by the Article 29 Working Party (hereinafter referred to as “WP”), in Opinion 5/2012, on cloud computing.[10] The analysis made by the WP has also been the main reference for the Italian Data Protection Authority for all those who, at European level, have come up in understanding and facing the complexities of the cloud world.[11]

The WP has focused its work mainly on highlighting the risks to personal data protection arising out from the cloud and in particular identified two macro-areas where the main critical issues emerge: lack of control and lack of information on processing operations.

4.2.3 Lack of Control

The processing of personal data through cloud services means that the data provided is in a continuous flow, that is, they are transferred as fast as possible from one place to another and are potentially replicated in multiple copies.[12] Therefore, customers risk losing their control over their personal data and to not be able to adopt the appropriate security measures.

This continuous flow of personal data increases the complexity of issues regarding data protection that shall be considered, as it may also involve the transfer of an individual’s personal data outside the European Union to third countries. While the circulation of personal data within the European Economic Area (EEA) is free, their transfer outside the EEA is forbidden unless specific safeguards are considered and applied.

Data transfer across borders outside the European Union (Recitals 101–116 and Articles 44–49 of the GPDR) shall occur by taking into consideration, among others, the envisaged country or countries of destination and the possibility of further transfers or the likelihood of transfers based on derogations for specific situations set forth by the Regulation; this could imply to verify the existence or absence of an adequacy decision by the Commission or, in the cases referred to in Articles 46, 47 and 49.2 GDPR, the existence of appropriate or suitable safeguards under Article 46 GDPR, such as standard contractual clauses or binding corporate rules.

[9] https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security.

[10] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[11] L. Bolognini, Servizi di cloud computing e protezione dei dati personali in ambito bancario, 2015.

[12] Article 4.1.1 describes personal data as any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In the absence of at least one of the above conditions, the transfer takes place under one of the following derogations, such as when:

(a) The data subject explicitly consents.
(b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
(d) The transfer is necessary for important reasons of public interest.
(e) The transfer is necessary for the establishment, exercise or defence of legal claims.
(f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
(g) The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled.
(h) Only on a residual basis, if the transfer is not repetitive, it concerns only a limited number of data subjects and is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

4.2.4 Lack of Information on the Processing of Personal Data

The lack of information on processing operations performed though the provision of cloud services may involve significant risks, both for the subject responsible for the processing and for the data subject. In fact, it is possible to create mechanisms that lead to responsibility for the service provider without it being aware of it.

For this reason, the data subject, whom data are subject to processing, shall always be kept informed about the identity of the data controller/processor and the purposes and methods involved in the processing activities. The lawfulness of personal data processing in cloud services is in fact closely linked to the compliance to the basic principles of providing information by the supplier to the customer.[13]

[13] Recitals 60 and 62, Article 13 GDPR.

Firstly, "transparency" is a prerequisite for ensuring the lawfulness and fairness of the processing of personal data. In particular, the cloud provider is required to provide the data subject with information on its identity and the purposes of the processing. At the same time, transparency shall also be ensured in the relationship between cloud consumer, cloud provider and (if any) subcontractors.

Secondly, the principle "of purpose limitation", as already envisaged by Directive 95/46 on the processing of personal data, and now reaffirmed by the GDPR, requires that the collection of personal data be made for determined, explicit and legitimate purposes and that the data are subsequently processed in a manner consistent with the same purposes.[14] In other words, the data subject must be informed about the purposes of processing of his personal data.

Lastly, the principle of "storage limitation" implies the obligation to set a period of time after which personal data shall be deleted or rendered anonymous.[15] So said, the data relating to the identification of the data subject may not be stored for a longer time than is necessary to achieve the purposes originally envisaged. In addition to this period, the data must be deleted or rendered anonymous. If it is not possible to delete the data, access to them shall be in any case prevented.

4.3 Internet of Things

As briefly anticipated, IoT is a phenomenon that is supposed to have an ever-deeper impact on the life of individuals. The possibilities that of objects and devices have to interact with each other entail a number of advantages that certainly contribute to the simplifying of individual's daily life.

However, such technological development generates a number of critical issues from the point of view of data protection. On the other hand, what characterises the IoT is the great amount of data—personal and not personal—that such technologies are able to collect.

The major problems are, of course, caused by the capability of some devices to store sensitive data, such as data related to the health status, potential sexual habits or, more generally, habits related to daily life.

For these reasons, the WP has issued Opinion 8/2014 on the Recent Developments on the Internet of Things.[16] This Opinion examines potential threats to individuals and gives recommendation to the stakeholders involved in the development of devices, devices' application and the use of them for purposes of processing personal data.

The WP29 focuses, above all, on the criticality of the phenomenon, namely, the information asymmetry and lack of control over the personal data by the data

[14] Recitals 42 and 43, Articles 7 and 13 GDPR.

[15] Recitals 65 and 66, Article 17 GDPR.

[16] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

subjects as well as the data controllers. That is, the main issue that WP29 finds is that there might be a distinction on personal data processed for different purposes (so-called secondary use) than those directly associated with a particular device (so-called primary use).

The WP warns users may find themselves under monitoring, especially when the collection and processing of their data are not made in a transparent manner. Then, stakeholders in the IoT field shall apply the principles of privacy by design, when developing new systems, applications and tools.

Moreover, the WP points out that data subjects and users must be able to exercise their rights and so be "in control" of their personal data at any time. It follows that devices and applications shall be designed so as to inform users and non-users about the means and purpose of the collection and the processing of their data. This may be achieved, for example, by allowing users to receive notices or warnings, designed to frequently remind them that sensors are collecting data, also by allowing the application on which the IoT tool is running to periodically send a notification to the user to let him know that the device is actually recording data.

Furthermore, developers shall pay attention to the types of data being processed and to the possibility of inferring sensitive personal data from them: this particular aspect shall be taken in due consideration, since there might be cases where it might occur to collect and process special categories of data, which shall be processed in accordance to the provision set forth by Article 9 of the GDPR.[17]

The WP concludes by stressing that developers shall apply a data minimisation principle: for example, if the purpose of the processing may be achieved using aggregated data, then developers shall not access the raw data.

Following a privacy by design approach, minimising the amount of collected data, makes compliance with the mentioned recommendation easier: moreover, it is suggested to perform a data protection impact assessment ("DPIA") on the device and the processes involved in its functionalities.

The performing of a DPIA, under Article 35 of the GDPR,[18] shall take into due account the respect of data subjects' rights and the principle of data minimisation.

[17] Article 9.1 prescribed that processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, unless one of the exception listed in Article 9.2 applies.

[18] Article 35.1 GDPR: Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

4.4 Critical Issues in the Interaction Between IoT and Cloud

Cloud is the beginning of a revolution in information technology that will affect the entire economy in the coming years. This new technology, due to its more typical features such as scalability, power, cost-effectiveness and flexibility, is involving different fields and increasing both production and market economy. At the same time, it has proved to be indissolubly linked to the ever-present spread of IoT.

However, despite the several benefits of both the cloud and the IoT, the high risks associated with these technologies and their combination shall not be overlooked. First of all, there is no clear delimitation of the roles and responsibilities of the subjects involved in data-processing operations. In fact, a set of different levels of responsibility between the cloud consumer and the cloud provider would be needed as only the latter may always be clearly aware of the type of data collected and the purposes and means of the processing, while the end user seems to play a role of a merely passive subject of a service, who should not be in charge of verifying the lawfulness of the processing activities that occur through the cloud infrastructure.

This issue has already been tackled and resulted apparent with respect to the sole cloud technology per se, considering that it already poses sufficient criticalities on the functioning of the data protection measures in a virtualised, and somewhat questionable, environment, that is, further enhanced by its interaction with IoT.

In fact, massive data collection may only take place through dematerialised and virtualised systems, which make it easier to manage the data collected but make it even less controlled and therefore more dangerous.

On the other hand, the automatic collection of data by IoT devices seems to result in a necessary rethinking of the traditional categories of consent and purpose of the processing, as it has been correctly pointed out by the WP.[19]

That is, personal data collected by tools implementing IoT technologies could potentially lead to concerning scenarios if not properly regulated. For example, profiling seems to be a direct consequence of the IoT environment, since the data collected are of different categories and, although individually considered, may not be in all cases qualified as "sensitive" data; however, they may be eligible to assume this quality when considered as a whole.

Such circumstance should certainly be taken into account by the legislator or by the providers themselves in offering their IoT and cloud services: for this reason, the adoption of codes of conduct is increasingly gaining popularity, so that it is possible to think about, in the near future, an evolution and affirmation of such practices as

[19] Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC): "With the development of the Internet of things, more and more data could be transmitted 'by default' for technical reasons, but used for intrusive purposes (notably marketing purposes) not related to the initial purpose of the broadcasting. In short, the rules governing the collection of information from user devices should not depend on the kind of device owned by the data subject nor on the technology employed by an organisation, especially with regard to the use of information for marketing and market analysis purposes".

true mandatory market access standards, thanks to their power to simultaneously ensure compliance for the provider, and protection of the end users affected by the processing operations.

In line with the mentioned standardisation processes, a European Horizon 2020 project called CloudWatch[20] has launched 4 years ago, with the task of creating services for small- and medium-sized enterprises (SMEs) interested in having access and using a cloud service and therefore having the necessity to understand all legal aspects implied by the cloud technology. To this end, the purpose of the CloudWatch project was—and still is—to create guidelines that could make the life easier for small and medium businesses when purchasing cloud services, even if it is likely that it might not be possible to radically erase all the risks but significantly reduce burdens and obligations.

Beyond these perspectives, which have a rather collective dimension for SMEs, nevertheless, individual customers and providers could still decide to take certain precautionary steps in light of the compliance to the rules of the GDPR.

First, by carrying out a deep and targeted DPIA over personal data processed and the purposes of the processing, according also to the principle of minimisation and privacy by design. Minimisation also extends to the configuration of software and information systems, since their design phase, used to process personal data, so as to minimise their use (so-called privacy by design), as well as to the development of technologies and/or processes with the aim of collecting and processing only the personal data strictly necessary to enable the data subject to benefit from the required functionality: all crucial aspects when combining the use of cloud and IoT technologies, with the aim of reducing impacts on and minimising risks for individuals.

On the other hand, the necessity, clearly inevitable, of acting in accordance with the principles of lawfulness, fairness and transparency of the processing remains to be taken into due account, in view of the opportunity to draw transparent and comprehensible information notices in compliance with the criteria set by Articles 13 and 14 of the GDPR.

Furthermore, the fact that the GDPR itself recognises the rights for the data subjects to be achieved directly, as well as indirectly, by means of the adoption of appropriate technical and organisational security measures; through the identification of a proper legal basis for the transfer of personal data outside the European Union; with the establishment of solid data retention procedures and timing; by drafting clear and complete information notice, together with the guarantee of an effective exercise of rights by the data subjects; and with the drafting of strong data protection agreements between all the subjects involved in the process that allows controllers and processors to precisely assess their respective duties and responsibilities.

[20] http://www.cloudwatchhub.eu/cloudwatch2-think-cloud-services-government-business-and-research-0.

Chapter 5
Network Threat Analysis

Anna Brékine, Anastasios Papathanasiou, Dimitrios Kavallieros, Sébastien Ziegler, Christopher Hemmens, Adrian Quesada Rodriguez, Georgios Germanos, Georgios Kokkinis, Georgios Leventakis, Jart Armin, and John Bothos

5.1 Introduction

As technology has developed, the obstacles that people have had to overcome to use it have dissolved. Unfortunately, this applies not just to the general population but also to criminals and others who are engaged either directly or indirectly in illegal activity. This does not merely apply to activity conducted purely on digital devices, as technology can facilitate more traditional forms of crime. For example, TOR, or The Onion Router, is a method anyone can use to (almost) completely anonymise themselves online, which has enabled trade in illegal materials without the ability to identify the people taking part in the transaction and, combined with Bitcoin—electronic currency that is also heavily based on anonymity; it has become easier than ever to circumvent the law.

As IoT becomes an immediate reality to the public, the need to know where attacks are likely to come from is getting more important than ever, as this knowledge may help prevent further attacks or minimise their potential consequences. The following chapter on Network Threat Analysis incorporates a number of results established in the framework of the SAINT project. SAINT is a research project funded by the EU's Horizon 2020 program and is dedicated to identifying the stakeholders and economic ecosystems that make up modern cybercrime. The project

A. Brékine (✉) · S. Ziegler · C. Hemmens · A. Quesada Rodriguez
Mandat International, Geneva, Switzerland
e-mail: abrekine@mandint.org

A. Papathanasiou · D. Kavallieros · G. Germanos · G. Kokkinis · G. Leventakis
University of Thessaly, Thessaly, Greece

J. Armin
CyberDefcon, England, UK

J. Bothos
IIT Demokritos, Athens, Greece

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_5

uses expertise in cybersecurity, law enforcement and economics to perform an in-depth analysis of the situation and provides recommendations regarding investment needs to be made and how to best defend against the threats that we are likely to face in the modern technological environment.

5.2 Stakeholders of Cybercrime and Cybersecurity

5.2.1 Attackers

The term “cyberattackers” represents the individuals or groups targeting infrastructure, computer networks and systems as well as electronic devices with Internet connectivity (e.g. mobile phones, IP cameras, smart houses, etc.). They have malicious intent which varies based on the type of attacker and their motivation. This section presents a taxonomy of cybercrime actors, trying to map their motives, scope and targets. The cybercrime actors can be broken down into nine categories:

- Cyberterrorists: Terrorist groups are increasingly using the Web to recruit and train new members, share information and organise attacks in the real world. Furthermore, terrorist organisations using the anonymity and security of the Dark Web disseminate training guidelines for cyberattacks to less experienced supporters [1].
- Cybercriminals: Criminals are using the Web to sell and transfer illicit goods and materials. For this taxonomy, the term “cybercriminals” is adopted for a variety of cybercrime stakeholders in order to depict traditional crimes through the use of computer systems (e.g. drug and firearm dealers, production and distribution of child abuse material, financial fraud, human trafficking, etc.).
- Hacktivists: Hacktivism is a digital form of activism that often employs hacking skills and tools in order to attack governmental institutions and private organisations. Hacktivists work in groups motivated by socio-political beliefs and ideology. Hacktivists act anonymously and, in most cases, instead of engaging in healthy debates and sharing their ideas, are more aggressive to criticism [2].
- Script Kiddies (SK) and Cyberpunks (CP): These two groups share many similarities. They are not “professional” hackers and have limited technical knowledge, using existing tools to deploy their attacks (UNODC, 2012). SK’s main motives are fun, fame and an adrenaline rush, while CP’s motives are predominantly based on their ideology against authority and to achieve fame and public recognition [3].
- Black Hat Hackers: Hackers, either black hat, white hat or grey hat, almost all use the same tools and techniques but have different motives and goals. Black hats are elite hackers undergoing illegal activities. Even though other actors in this chapter can be characterised as black hats (e.g. hacktivists), for this taxonomy we identify as black hats, individuals or groups with excellent computer skills (elites). Their primary motivation is to earn money (e.g. hacking as a service) and, on occasion, to cause significant damage (e.g. destroy/steal confidential data) [4, 5].

- Cyberwarfare Actors/State-Sponsored Attackers: Sponsored and driven by countries, cybersyndicates and cyberterrorists, in both times of war and peace, aim to cause damage by gaining illegal access to state and trade secrets, technology concepts, ideas and plans and, in general, artefacts of value for a country or state. Their intentions often include harm and damage to critical infrastructure, and, in general, they seek to damage other states' economies [6].
- Insider Threats: These cause monetary losses to an organisation and are the results of actions or errors caused by individuals within the organisation. As referenced in the 15th annual CSI Computer Crime and Security Survey reports, there are two separate threat vectors contributing to insider threats. They are attributed to (1) employees with malicious intent against the organisation they're working for (e.g. leaking/selling non-public information, data breaches, etc.) and (2) employees within the organisation who have made some kind of unintentional blunder. The report reveals that the majority of losses are due to non-malicious actors [7].
- Virus and Hacking Tool Coders: Individuals or teams of expert programmers – elite hacking tool coders with excellent computer skills. The main focus of these actors is to develop computer viruses/malware/rootkits/exploits (malicious code) and hacking toolkits, which are either sold on the black market or distributed freely. The main buyers are non-expert individuals who want to become hackers (e.g. script kiddies) [5].

Although this is a general summary of threats, as IoT becomes more prevalent and controls more everyday "things" with which the general population comes into contact, knowing the biggest threats to IoT security will be the first step in ensuring that the technology is adequately protected.

5.2.2 Defenders

The term "defenders" represents the individuals or organisations who stand opposed to the aforementioned cyberattackers and seek to combat criminal activities online. The list of stakeholders participating in the war against cybercrime is extensive and varies from one country to another. It usually involves members of the national police, government agencies and private companies. In spite of the multitude of actors involved, the defenders of cybercrime may be broken down into two categories: public and private. In the European Union, the defenders belonging to the public sector are:

- The European Commission: The Directorate-General for Migration and Home Affairs (DG HOME) has a unit specifically dedicated to cybercrime, which falls under the larger Directorate (D) of "Security". The unit actively works with other European Commission's Directorates, such as the Directorate-General for Justice and Consumers (DG JUST) and the Directorate-General for Communications Networks, Content and Technology (DG CNECT) in shaping the EU cybersecurity policy. Additionally, the European Commission cooperates with other European organisations like the

European Parliament, the European Council, INTERPOL, EUROPOL, EUROJUST, members of the industry and academia to construct the EU policy.
- INTERPOL: The International Criminal Police Organisation (INTERPOL) is an intergovernmental organisation created in 1923, which seeks to improve international police cooperation aided by its National Central Bureaus (NCBs) in 190 member-states. The latter constitute the core of INTERPOL by contributing to criminal databases and cooperating on international investigations, operations and arrests. The role of INTERPOL is to facilitate information exchange to efficiently combat any form of crime, including cybercrime.
- EUROPOL: The European Union Agency for Law Enforcement Cooperation (EUROPOL) is the law enforcement agency of the 28 member-states of the European Union. At the EU level, it is accountable to the Council of Ministers for Justice and Home Affairs. EUROPOL seeks to facilitate information exchange between national police services in the field of illicit drugs, human trafficking, terrorism, money laundering, online fraud, international crime and paedophilia.
- EUROJUST: The European Union's Judicial Cooperation Unit (EUROJUST) is an agency of the European Union which seeks to guarantee cooperation, information-sharing and coordination between national authorities from the 28 EU member-states on criminal affairs, such a cybercrime.

As far as the private sector defenders are concerned, the cybersecurity industry plays a key role in fighting cybercrime by providing individual end-users, businesses, and organisations with the appropriate tools and services to protect themselves and manage a cyberattack. So far, the USA is taking the global lead in terms of the number of security vendors. However, five EU countries (the UK, Germany, France, Sweden and Ireland) have made the top 10 ranking.

5.2.3 Victims

Information systems are an integral part of everyday life for citizens. Smaller or larger information systems with Internet access in the form of laptops, smartphones, tablets, gaming machines, servers or other devices included in the "Internet of Things" category are being used by individual citizens, businesses, organisations or other government agencies.[1] Cybercriminals attempt to exploit this vast pool of candidate victims in order to achieve their goals.[2] Depending on their motivation, each category of perpetrator (e.g. economic benefit, fun, reputation, ideological reasons, etc.) targets a particular category of victim. In this section, we will discuss the victims of cybercrime. It's important to remember that IoT is still nascent so we feel it's important to accurately describe the threats we know of so that, should IoT break into similar areas, we are well-informed as to the risks and dangers.

[1] Cui, X. (2016). The internet of things. In Ethical Ripples of Creativity and Innovation (pp. 61-68). Palgrave Macmillan, London.

[2] Marion, N. E. (2010). The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation. International Journal of Cyber Criminology, 4(1/2), 699.

The first identifiable category of victim we might identify is that of underage physical persons (the age at which a person is defined as a minor varies from country to country). Minors, who are often using the Internet to have fun and communicate, may be victims of sexual exploitation and/or abuse online.[3] While browsing social networking sites, it's possible that an unknown person will seek to communicate with them so as to force them into obscene acts in the virtual or physical world.[4] It is equally likely that the actor seeks financial rewards in order not to reveal to the child's friends and acquaintances the existence of pornography material that the child has created (e.g. selfie photos or obscene video).[5] Cyberbullying is also frequently reported as part of juvenile delinquency. The perpetrators here almost always belong to the friendly environment of the victim.[6] Lastly, underage people may be victims of financial deception if they unknowingly – and without the consent of their parents or guardians – make credit card charges (e.g. to participate in online gambling) or telephone bills.[7]

Subsequently, the next major category of victim is adults, who can become victims of any form of crime whether cyber-only or those for which the Internet is a means of facilitating the perpetrators or the communication between them.[8] Therefore, in this case, victims of crimes of an economic nature, where the motivation of the perpetrators is financial profit, are mentioned first.

The potential perpetrators of cyber- and economic crimes, as well as the potential victims or targets, meet in a common "space": the Internet, computer network or telephony. The two sides are users of the same network which is the "reservoir" of both potential criminals and attractive targets.

This is accomplished in a number of ways, namely, (a) victims are deceived by false information and are then persuaded to send money to the perpetrators;[9] (b) perpetrators with various tricks intercept the credentials of e-banking users, and, by gaining access to the bank accounts of the victims, they transfer large amounts of money to their own accounts;[10] or (c) the perpetrators infect victims' computer

[3] Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimisation among young people: a multi-nation study. Journal of Scandinavian Studies in Criminology and Crime. Prevention, 16(2), 203-210.

[4] Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2010). Use of social networking sites in online sex crimes against minors: an examination of national incidence and means of utilisation. Journal of Adolescent Health, 47(2), 183-190.

[5] Acar, K. V. (2016). Sexual Extortion of Children in Cyberspace. International Journal of Cyber Criminology, 10(2), 110.

[6] Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth.

[7] http://www.belfasttelegraph.co.uk/news/northern-ireland/hundreds-of-kids-cyber-crime-victims-and-its-tip-of-iceberg-psni-has-warned-30267519.html

[8] Koops, B. J. (2010). The internet and its opportunities for cybercrime.

[9] Ross, S., & Smith, R. G. (2011). Risk factors for advance fee fraud victimisation. Trends and Issues in Crime and Criminal Justice, (420), 1.

[10] Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., & Wang, L. (2010, August). On the analysis of the zeus botnet crimeware toolkit. In Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on (pp. 31-38). IEEE.

systems with ransomware, cryptoware or malware and then seek money to reset them to their pre-infected state.[11] In other cases, perpetrators seek access to victims' data (video files, photos, text documents, spreadsheets, etc.), and, for this reason, they seize the credentials of online accounts and services.[12] Cyberbullying cases are also reported by older victims,[13] and there are a few cases where the perpetrators are trying to take revenge from their victims for events that occurred earlier (e.g. revenge porn,[14] jealousy, defamation).

In summary, risky Internet behaviour that exposes adult users and makes them vulnerable targets by bringing them in close proximity to potential offenders may include daily routines on the Internet such as:

- Participation of users in chat rooms
- Accepting strangers as "friends" in social media
- Frequent online transactions to purchase products through auctions or online stores
- Frequent use of e-banking
- Engaging the victim himself in illegal online activities such as using a broadband connection to download free or pirated software or files, engaging in hacking activities, visiting pages with controversial content and viewing prohibited material such as pornography
- Capturing images
- Disclosure of personal information and data
- Opening suspicious emails (e.g. spam)

A distinct category of cybercrime victims are businesses, whether public or private, and other bodies and organisations. The perpetrators of the crimes committed against these entities usually seek financial benefit,[15] but their purpose could also include damaging the profile and credibility of said business or entity or gaining access to valuable business information (industrial espionage).[16] Thus, a large percentage of victims are enterprises whose information systems are infected with malicious software (especially ransomware and cryptoware) and where the perpetrators require ransom in the form of digital cryptocurrencies by the victims. Additionally, a DDoS attack on an organisation's website or information system

[11] O'Gorman, G., & McDonald, G. (2012). Ransomware: A growing menace. Symantec Corporation.

[12] Hutchings, A., & Holt, T. J. (2014). A crime script analysis of the online stolen data market. British Journal of Criminology, 55(3), 596-614.

[13] Kokkinos, C. M., Antoniadou, N., & Markos, A. (2014). Cyber-bullying: An investigation of the psychological profile of university student participants. Journal of Applied Developmental Psychology, 35(3), 204-214.

[14] Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn

[15] Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.

[16] Hyman, P. (2013). Cybercrime: it's serious, but exactly how serious?. Communications of the ACM, 56(3), 18-20.

may benefit its competitors, directly or indirectly.[17] An equally important blow to a business or organisation may be leakage – interception of valuable data (especially documents and databases concerning individuals, transactions, etc.). In this case, an operator or business may be the victim of an (former) employee, who thus expresses dissatisfaction with his employers/supervisors.[18]

The last category of victim is countries. A state and, in particular, its infrastructure (mainly critical) may become a victim of serious cyberattacks. This online attack can take place both individually and within the frame of a wider cyberwar that may have erupted. The consequences of such a cyberattack may be particularly serious when critical infrastructure related to transport, energy, health, etc. is affected.[19]

This last point is particularly important when considering the security of IoT infrastructure as this is the type of IoT that is most likely to impact the greatest number of people should an attempted attack be successful. However, with the rise of domestic IoT, individuals need to make sure they are aware of the other types of attack and that they are adequately protected or are taking the necessary precautions so that they are less likely to be the victims of an attack.

5.3 Information and Markets

The role of information is crucial for the ecosystem of cybercrime and cybersecurity. All stakeholders (cybercriminals, potential cybercrime victims, cyber-defence services providers, cybersecurity regulatory and law enforcement authorities, researchers) value all information on developments in the area of cybersecurity as a way of realising the best outcomes.

5.3.1 Cybercriminals

Cybercriminals, either individually or by forming coalitions, develop Fraud-as-a-Service (FaaS) cybercrime business models, providing hired services for malware attacks, stolen digital goods, etc. An alternative way to obtain money is by hunting bug bounties issued by cybersecurity technology suppliers and organisations as reimbursements for providing confidential information regarding previously unknown vulnerabilities in available cybersecurity technologies. Demonstrating their deficiencies and by keeping this information private, they are able to demand

[17] Walters, R. (2014). Cyber attacks on US companies in 2014. The Heritage Foundation, 4289, 1-5.

[18] Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. IEEE Communications Surveys & Tutorials.

[19] Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: cyber conflict in the international system. Oxford University Press, USA.

high prices from their clients. Another potentially lucrative pool of profitable information for cybercriminals is the social networks. A successful cybersecurity breach of relevant profiles and/or discussion forums could result in the acquirement of valuable information and sensitive data that can be used for blackmailing in the form of demanding money for not disclosing them publicly.

In the Deep Web cybercrime markets, cybercriminals' revenue depends on the net value of purchased products, acquired through criminal activities. The relevant price fluctuations are indicative of the cybercriminals' profits. Trends in Deep Web cybercrime markets follow accurately the latest updates regarding the cybersecurity level of widely used technologies and changes on the cybersecurity mechanisms, which could increase or decrease, respectively, the price of Deep Web-purchased cybercrime products.

To minimise the risk of misusing valuable resources and time, cybercriminals diversify their actions towards multiple, potentially profitable targets and illicit actions that could yield substantial earnings, allocating time and resources accordingly. To this end, the value of as good as possible relevant information is high and a considerable asset. This is reflected in the prices that cybercrime products purchased on the Deep Web have; however, the information's usefulness is subject to change, and, therefore, its price can be volatile.

In that framework, cybercriminals act as investors in a stock market, allocating time and resources in activities that are more prone to profitability in terms of cost-benefit analysis. These activities of the underground economy are treated as stocks, with those with the best potential and strong future prospects have higher stock prices. The rapid change of the value of any service offered on the Deep Web market is an indication for cybercriminals regarding the actual price of purchased cybercrime products on Deep Web markets and helps them to evaluate the cost-effectiveness of the allocation of their resources and transform their revenue models accordingly.

5.3.2 Potential Cybercrime Victims

The role and value of information about potential cyber-risks and past cyberattacks that have taken place are also vital for organisations as potential cybercrime victims, in order to enhance the structure of their cyber-defence. On the other hand, revealing "sensitive" inside information about cyberattacks that have occurred might indicate weaknesses that could damage to some degree, intangible assets of an organisation like reputation, future potential for cooperation, etc.

Organisations come to a position where they have to strike and hold a sensitive balance regarding their policies of information-sharing about cyberattacks they've been affected by. The key aspect of that dilemma is the amount by which information-sharing affects investment and the operational costs of the organisation, also taking into account subsequent losses from cyberattacks. There is a dual-nature, risk analysis problem at hand for organisations, namely, the maximisation of the cost-benefits of relevant investments and the minimisation of operational costs and losses in relation to information-sharing regarding these subjects.

In some cases, organisations, in an attempt to avoid dealing with all these necessary procedures all by themselves and to mitigate the relevant costs, choose the solution of subcontracting these cyber-defence processes as relevant services to other external organisations by participating in managed security service provider (MSSP) networks. Inside these networks, organisations of different sizes, expertise and needs exchange information regarding cyberattacks, jointly test cybersecurity measures and share relevant staff training. Through this joint enhancement of their cyber-defence, they achieve the construction of a mutual cybersecurity framework for mitigating their vulnerabilities.

5.3.3 Cyber-Defence Services Providers

Providers of cyber-defence services are expected to provide for their clients an adequate level of protection and coverage against potential large cyberattacks. As suppliers of cybersecurity services, they are also expected to guarantee a minimum basic level of resilience, inoperability, flexibility and scalability of the cybersecurity services they provide for their clients so that they can accommodate a minimum level of support for an organisation's systems after a cyberattack.

To achieve adequate provision of the above, effective resource-allocation management is required. Concerning business performance in the cyber-defence service industry, information is a valuable prerequisite for allocating economic resources efficiently. Useful intelligence about cyberthreats and relevant vulnerabilities can be derived from various sources of the cybersecurity community as well as the surface and deep web. These can help cyber-defence service providers to provide methodologies, recommendations, behaviour protocols and best practices on cyber-defence with respect to the recovery and reduction of associated losses.

All these information feeds about the trends in exploiting vulnerabilities and malware attacks, the respective market prices and the relation between vulnerabilities and supply and demand in the cybersecurity market can be analysed in order to extract early warning patterns on possible cyberthreats. These attributes can be further explored in the relevant business models of the cyber-defence services providers for business investment efficiency and thus enabling them to offer enhanced cyber-protection and to achieve market competitiveness in the relevant industry.

5.3.4 Cybersecurity Regulatory: Law Enforcement Authorities

Information is also needed by the Cybersecurity Regulatory and Law Enforcement Authorities for the issuing of regulatory recommendations and guidelines regarding cybersecurity and the controlling of cyberspace. Authorities gather requirements concerning cybersecurity from all the other stakeholders and produce directives for application throughout Europe.

The role of information in setting benchmarking industry standards is very important. Respective regulatory recommendations have to be on par with most relevant, existing, unofficial cybersecurity and privacy standards and norms. In order to provide a set of effective official recommendations and standards against cybercrime, authorities explore various sources of cyberthreat information and perform comparative analyses of approaches and interactions throughout the cybercrime and cybersecurity ecosystem.

This serves to identify systematically different factors whose roles in the reduction of cybercrime contribute to the cost-benefit effectiveness of relevant industry investments. A comprehensive ecosystem comparative analysis with the potential to identify incentive mechanisms helps the introduction of new regulations for official certification and labelling of cybersecurity standards, addressing cybercrime and mitigating its effects. Moreover, it is also proactive in the development of relevant business models' performance in a much more credible way from a scientifically point of view, shifting attention to end-users' and stakeholders' requirements and needs.

5.4 The Future of Cybersecurity in the Context of IoT

The fast-evolving Internet of Things aspires to connect ICT smart devices and people into a large-scale information gathering and processing infrastructure. The advances in microelectronics and hardware architectural design have led to the development of portable devices of unprecedented computational, storage and communication capabilities. We now have, for instance, smartphones based on multicore (4 or, even, 8 cores) processors with memory capacities close to desktop computers, powerful sensor capabilities and a multitude of wireless communications protocols (e.g. Wi-Fi, Bluetooth, NFC, etc.). Furthermore, microchip developments have made possible the design and construction of other types of devices with similar computing and communicating power such as smartwatches and drones (which have the advantage of autonomous or directed movement) as well as general purpose open development platforms such as the Arduino and Raspberry Pi 3.

The IoT presents an opportunity for innovative applications since it enables the creation of distributed, self-organising, ad hoc (unstructured) networks. These networks possess unlimited sensor, computational and data generation capabilities much like a massively parallel, distributed computer, "diffused" over the Internet. The resulting system can collect and, at the same time, rapidly process large amounts of data inferring, in real time, useful information. This IoT-based application model (called "crowd-sensing" or "collective intelligence" model) creates numerous opportunities for building new, distributed, computationally demanding services, based on the joint power of numerous portable, but powerful, devices.

The IoT is a vehicle for harnessing the power of people especially in the context of smart cities which are now a reality across the world. Cities seek to attain a high level of end-user satisfaction while contributing to a thriving economy by deploying ICT infrastructures inextricably intertwined with their physical facilities. This integration results in a "smarter" city, in the sense that the city "senses" and "understands" its inhabitants' needs. Thereafter, it can adjust or rectify itself in order to satisfy them mainly through monitoring itself and its inhabitants' opinions and suggestions, finally notifying the local governors (e.g. municipality or local government). Moreover, within the last and current decades, many ICT companies created and invested in technologies which are able to transform cities into smart cities in the above sense. As evidenced from the ongoing work of the Technical University of Vienna, Austria, available in [http://www.smart-cities.eu/], the EU has been steadily developing a major strategic advantage in the smart city domain by having numerous EU cities equipped with smart city infrastructures and applications.

What was described above, however, was only the good picture that people and many decision makers and entrepreneurs usually see or prefer to see. The other side of the coin is that privacy and cybersecurity threats now enter the scene in a more pervasive and dramatic way, mostly for people and organisations whose devices and ICT infrastructures are part IoT application. The Internet, itself, has long been a dangerous place. One can only imagine what could happen when an uncountable number of (often unprotected) devices of any kind, origin and functionality are, dynamically, attached to it at any time, at any place. Cybersecurity threats are multiplied, both in number and severity, by orders of magnitude in going from the Internet to the IoT. Since successful IoT applications rely on gathering and analysing massive volumes of crowdsourced data as well as numerous streams of environmental parameters, it is also important to enhance the IoT's security and privacy preservation in order to elicit people's trust and willingness to use IoT applications. The main reason is that collecting and storing data coming from users and their activity pattern, which is something which lies in the heart of many of the IoT business deployments, is a subtle business, and enterprises developing IoT services may be at risk of violating privacy protection policies and legislation. Some services which are based on data which are considered sensitive (e.g. location-based services, LBS, or services based on user profiling) may even operate on the verge of legality in some jurisdictions. Adding to this picture, the already cybersecurity attacks in the Internet suffices to ring a bell that things may easily go out of control if sufficiently strong cybersecurity measures are not taken on a global scale and all granularity levels, i.e. from individuals to multinational organisations and businesses. One must always advance according to worst-case scenarios, and this is especially so if the worst-case scenario is rather probable to occur now or in the near future.

Acknowledgments This chapter includes results shared by the European research project SAINT (Grant Agreement N° 740829), which has received funding from the European Union's Horizon 2020 Research and Innovation Programme and the Swiss State Secretariat for Education, Research and Innovation.

References

1. Council of Europe, Cyberterrorism: the use of the internet for terrorist purposes. United Nations Office on Drugs and Crime **12**(1), 497 (2007)
2. T. Sorell, Human rights and hacktivism: the cases of Wikileaks and anonymous. J. Human Rights Pract. **7**(3), 391–410 (2015)
3. M.K. Rogers, *The psyche of cybercriminals: a psycho-Social perspective', in Cybercrimes: a multidisciplinary analysis* (Springer, Berlin, 2011), pp. 217–235
4. C. Dianne Martin, Taking the high road: white hat, black hat: the ethics of cybersecurity. ACM Inroads **8**(1), 33–36 (2017)
5. R. Sabillon et al., Cybercrime and cybercriminals: a comprehensive study. Int. J. Comput. Netw. Commun. Secur. **4**(6), 165–176 (2016). http://www.ijcncs.org/published/volume4/issue6/p1_4-6.pdf
6. N. Rasmussen, Homeland Security and Governmental Affairs "Cyber security, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland" Framing the Threat' (2014), pp. 1–4.
7. R. Richardson, 2010/2011 computer crime and security survey. Director **2011**, 1–40 (2011). https://doi.org/10.1108/09685229810209414

Chapter 6
Evolution of Data Protection Norms and Their Impact on the Internet of Things

Luca Bolognini and Sébastien Ziegler

6.1 Introduction

The new Regulation (EU) 2016/679 on the protection of personal data (General Data Protection Regulations, hereinafter referred to as the "Regulation" or "GDPR") takes a decisive step forward in enhancing the protection of individuals with regard to their personal data, allowing a better free flow and valorisation of such data.[1]

The adoption of a Regulation is certainly the result of two different aspects:

– First, there is a need for a minimum standard of uniform protection across all European Member States, since the protection of personal data is a fundamental right of the individual, recognised as such by Article 8.1 of the Charter of Fundamental Rights of the European Union.
– Second, the spread of new technologies, including the Internet of Things ("IoT") and cloud computing, has resulted in the abolition of national boundaries, and the processing of personal data in those two fields has become more cross-border and international.

In order to harmonise the regulatory framework with regard to the circulation of personal data in electronic communications, the European Commission also took the chance of beginning a process of reforming Directive 2002/58 (the so-called e-Privacy Directive).[2] The new EU e-Privacy Regulation, still a proposal by the EU

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=IT.

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=IT.

L. Bolognini (✉)
Istituto Italiano per la Privacy, Rome, Italy
e-mail: l.bolognini@istitutoprivacy.it

S. Ziegler
Mandat International, Geneva, Switzerland

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_6

Commission, published in January 2017[3] and commented by Article 29 (hereinafter also referred to as "WP") in April 2017,[4] regulates, among others, machine to machine communications, which characterise the technological phenomenon of the IoT and the Big Data, under an international perspective.

Among all, the Internet of Things (IoT) phenomenon has been clearly one of the main starting points of the whole process of reform, as it poses new challenges to the protection of individuals' personal data. In the IoT environment, objects "come to life" and may acquire a sort of own "intelligence", making such devices interoperable with other devices, allowing exchanging and communication of data between them (many started calling such devices "e-objects").

These are a few examples of IoT technologies in our everyday life: think of the home lock that opens or closes with a touch of smartphone, the drug's box that sends an alert when it needs to be refilled, or sneakers that count the steps made during the day.

All these objects and devices are designed to collect and process personal data and information that may be communicated over the network to other devices so as to elaborate analysis of behaviours, characteristics, and habits of their users.

In these respects, the IoT ecosystem lends itself to many criticalities in terms of personal data protection. Indeed, while it is true that smart objects and devices make life simpler and easier by creating new opportunities for the wellbeing of the individuals, on the other hand, it is not safe to underestimate the inevitable repercussions that they might have on the same individuals.

For all these reasons, it is necessary to examine in higher details all relevant provision of the GDPR that come into play, with reference also to Opinion 8/2014 issued by the WP on the Recent Developments on the Internet of Things.[5]

6.2 The European General Data Protection Regulation: A Step Change for the Protection of Personal Data in the World of the Internet of Things

The GDPR envisions a great amount of novel provisions aimed at strengthening the individual's protection in a digital era in which he may be constantly monitored and traced by a "big brother", where the observer eye is a smart device. IoT players will have to pay due attention to new data protection principle of accountability[6] and the

[3] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[4] http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

[5] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[6] Accountability is dependent on, and completed by, the respect of the above principles and the capacity of the data controller/processor to prove the compliance; the data controller is required to put in place appropriate and effective measures to demonstrate, at the request of the supervisory authority, the compliance of the processing activities with the GDPR, including the effectiveness of the mentioned measures.

privacy by design approach, when acting as data controllers,[7] as well as data processors.[8] IoT devices shall always be focused on compliance towards guaranteeing users'—and, for certain aspects, all individuals'—rights under Articles 12 to 22 of the GDPR.

6.2.1 *Accountability*

The respect of the above described rights will ensure a first step towards a good degree of accountability of the data controller and the data processor. On the other hand, by implementing appropriate technical and organisational measures of data protection by design, in all stages of the development of intelligent devices, security measures and data minimisation certainly play an essential role.

Minimisation also extends to the configuration of software and information systems – since their design phase – used to process personal data so as to minimise use of such data (so-called privacy by design), as well as to the development of technologies and/or processes with the aim of collecting and processing only the personal data strictly necessary to enable the data subject to benefit from the required functionality.

6.2.2 *Stakeholders and Risks in the IoT*

What above just described is strongly connected to what the Working Party 29 (WP) points out in its Opinion 8/2014 on the Recent Developments on the Internet of Things, where it examines potential threats to individuals and gives recommendation to the stakeholders involved in the development of devices, devices' application, and the use of them for purposes of processing personal data.

The WP warns users may find themselves under monitoring, especially when the collection and processing of their data are not made in a transparent manner. Then, stakeholders (not to be referred to only to data controllers and processors but also to device's developers, manufacturers, etc.) in the IoT field shall apply the principles of privacy by design, when developing new systems, applications, and tools.

[7] The data controller is defined by Article 4.1.7 GDPR as the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, where the purposes and means of such processing are determined by Union or Member State law and the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[8] The data processor is defined by Article 4.1.8 GDPR as a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Moreover, the WP points out that data subjects and users must be able to exercise their rights and so be "in control" of their personal data at any time. It follows that devices and applications shall be designed so as to inform users (data subjects) and non-user (any individual) about the means and purpose of the collection and the processing of their data. This may be achieved, for example, by allowing users to receive notices or warnings, designed to frequently remind them that sensors are collecting data, also by allowing the application on which the IoT tool is running to periodically send a notification to the user to let him know that the device is actually recording data.

Furthermore, stakeholders (as per the definition we have given above) shall pay attention to the types of data being processed and to the possibility of inferring sensitive personal data from them: this particular aspect shall be always taken in due consideration, since it is possible to process special categories of data only to the extents allowed by Article 9 of the GDPR.[9]

The WP concludes by stressing that developers shall apply a data minimisation principle: for example, if the purpose of the processing may be achieved using aggregated data, then stakeholders shall not access the raw data.

Following a privacy by design approach, minimising the amount of collected data, and so aligning with the accountability principle, will make compliance with the mentioned recommendations a lot easier: moreover, to fully comply with the GDPR, the performing of a data protection impact assessment ("DPIA") on the device, and the processes involved in its functionalities, will come to full circle.

6.2.3 Data Protection Impact Assessment

The above comments lead us back, then, to the GDPR, by considering that the performing of a DPIA on a IoT device (meaning one or more implied processing activities) under Article 35 of the Regulation that is mandatory in the cases listed in paragraph 3,[10] nevertheless strongly recommended in general, shall take into due

[9] Article 9.1 prescribed that processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation shall be prohibited, unless one of the exception listed in Article 9.2 applies.

[10] A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
(b) Processing on a large scale of special categories of data referred to in Article 9 (1) or of personal data relating to criminal convictions and offences referred to in Article 10.
(c) A systematic monitoring of a publicly accessible area on a large scale.

account the respect of individuals' and data subjects' rights and the principle of data minimisation. The author highlights that recently, on April 4, 2017, the WP published the proposed Guidelines on DPIA[11] and that he would like to integrate the suggested scheme, by splitting the preliminary risk assessment in two different steps:

1. The first step shall be focused on the analysis of the severity and likelihood of risks threatening personal data and the whole processing activity/supporting assets; this first phase may be necessary in order to assess the possible "IT pathological/extrinsic risks" implied by, for example, data breaches in the IoT environment.
2. The second step shall analyse the severity and likelihood of risks of impacts on the rights and freedoms of natural persons, as implied, further:
   (a) By the possible pathological/extrinsic risks (i.e. data breaches) taken into account in the first phase.
   (b) As a possible/likely "physiological" and intrinsic consequence of that specific data processing, considered in itself, even in absence of pathological/extrinsic risks (the above data breaches).

Only at the end of this two-pronged evaluation, it is possible to ascertain the intrinsic burden of potential negative impact on the rights and freedoms of individuals by the processing operations, as well as to identify any necessary mitigation measures.[12]

Hence, in the opinion of the author, it is clear the purpose of the DPIA applied to the Internet of Things: it is intended to require the data controller (and, where appropriate, the data processor) to perform a conscious appraisal of the impact that a smart object might have on the rights and freedoms of the individuals.

The IoT environment does not only imply risks associated with the use of personal data collected (which, as above described, are evaluated in the DPIA) but also may present further potential risks of data breaches, and so security in general.

6.2.4 Data Breach

In the IoT environment, several potential feared impacts could involve a wide variety of data and of data subjects (and individuals) to whom those data referred to. Think about the possibile collection, through IoT devices, of sensitive data revealing racial or ethnic origin, political opinions, religious or philosophical convictions,

[11] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

[12] For more information, please also refer to the article available at the following link http://www.istitutoitalianoprivacy.it/it/2017/09/12/dpia-guidelines-new-recommendations-from-the-italian-institute-for-privacy/.

health data, or sexual life data; or think about the potential monitoring and analysis of IoT-sourced data, that could lead to the forecasting aspects of earning performance, economic situation, health, preferences or personal interests, reliability or behaviour, and location or transfers, in order to build or use personal profiles, often used by providers in their commercial activities.

According to Article 4 of the GDPR, "data breach" means a violation of the security that entails an unlawful or accidental destruction, loss, modification, and unauthorised disclosure of or access to personal data transmitted, stored, or otherwise processed[13]. In case a data breach could result in a risk to the rights and freedoms of natural persons, the controller shall activate a strict procedure. The purpose of this procedure is to provide practical information to the data controller and to the data processor in case of data breach under Article 33 and 34 of the GDPR.

In view of the new obligations imposed on the data controller by the GDPR, it shall assess whether the anomalous event shall be considered a breach of security (e.g. a cyberattack or abusive access or accident, fire and other disasters, etc.), following which it occurs, unlawfully or accidentally, an unauthorised destruction, loss, modification, and disclosure of or access to any personal data transmitted, stored, or otherwise processed. Moreover, the controller shal assess the possibility of a risk to the rights and freedoms of natural persons, implied by such a breach.

A possible positive aspect, if implemented, appears in Article 34, paragraph 3.a, which provides that the communication to the data subject is not required if, among others, the controller (or the processor) has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption (as well as pseudonymisation, when properly achieved).

6.2.5 Security Measures

Since IoT involves an infrastructure made up of multiple sensors built into each other, each of them is then a potential entry door for hackers. As we saw, the DPIA has precisely the aim to identify and evaluate the potential risks, both pathological and physiological, to the rights and freedoms of the data subjects and individuals, such as data breaches, unauthorised access, involuntary modification or deletion or loss of personal data, voluntary modification or deletion or loss of personal data, etc., stemming from the implementations of systems, in view of evaluating the adequate technical and organisational security measures.

A good approach to security is based on an analysis of the risks associated with information, which shall also be aimed at identifying threats that may pose risks to IT systems and assets, and in general to the personal data processed and to the data

[13] L. BOLOGNINI, E. PELINO, C. BISTOLFI, Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Milano, 2016, p. 336.

subjects; it seems, then, essential to assess whether security measures in place are providing an adequate level of protection (as provided for by Article 32 of the GDPR).

For these reasons as well, the security of the Internet of Things is at the top of agendas of all world governments, as appeared in the meeting that took place at the end of July in Tokyo, for the Japan-US Cyber Dialogue; on that occasion, cybercrime has been discussed, and the two nations have agreed to increase bilateral cybersecurity and their efforts towards the prevention of data breaches.[14]

The provision of the obligation to notify a data breach is certainly an expression of the radical change introduced by such occurrences in the world of the information technology, since the phenomenon is perceived by the legislator as a real public danger.

6.2.6 Data Subject's Rights

The (last but not the least) major topic related to the Internet of Things is the lack of awareness on the side of the data subject with respect to the collection and processing of his personal data that, in some case, may result in a continuous monitoring. New technologies seem to have started a process of "exclusion" of the user from choices about his personal information. This is caused mainly because the automatic interaction modalities on which IoT devices are based are not adequate (or too willing) to provide correct and complete information to the user.[15]

This issue has been highlighted by WP as well in the above-cited Opinion 8/14, where, in order for a processing operation to be considered legitimate, "users must remain in full control of their personal data throughout the product lifecycle" (principle of self-determination). In many cases, the user may not know that he is actually using a "connected" device, because it is apparently unrecognisable; think, for example, of clocks or bracelets equipped with sensors (so-called wearable devices) that measure heart rate frequency.

Even the use of a device, such as a smartphone, in which an app is set up to extract the aggregated data and extrinsic information from the raw data collected on the user's geographic location or his health status, could represent a scenario of possible data protection violations.

In fact, most of the IoT devices interact through sensors by collecting data that are then used by companies to elaborate and generate trends and improve their "tailor-made" services to be offered in return to their customers.

It is clear that what has just been discussed may be in contradiction with the principles of lawfulness, fairness, and transparency mandated by the GDPR and

[14] Joint Statement of the Japan-US Cyber Dialogue. Available at https://www.state.gov/r/pa/prs/ps/2017/07/272815.htm.

[15] J. VAN DEN HOVE, R. WEBER, A. GUIMARAES PEREIRA, F. DECHESNE, Fact Sheet-ethics Subgroup Iot -version 4.0,2012, 17.

that, again, are at the foundation of the compliance to the accountability principle. The processing of personal data must be performed by informing data subjects about the collection, use, and storage of their data. Thus, data processing shall have a lawful basis, either the data subject's consent or an exception to the consent rule, for the processing activities to be legitimate (Article 6.1 GDPR).

Consent is the manifestation of willingness, made by the data subject, to accept the processing of his; for such consent to be valid, it shall be clear (free of constraints), preceded by the information notice, unambiguous, and expressed. Furthermore, if the consent is requested through electronic means, such request must be clear and concise and shall not interfere with the service for which consent is required.

The main issue with consent in the IoT environment concerns the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. It should also be noted that consent is free when it is revocable; this may pose a concrete issue with IoT technologies, since they do not often possess any interface and do not allow the user to revoke the consent previously granted. Such situation may concern the risks associated with any subsequent use of the information collected, or the reuse of the personal data originally processed, for purposes other than the ones stated at the moment of collection, by also crossing the data acquired with other information through complex cross-matching methods.[16]

The GDPR gives indication on what information and how that information shall be given to the data subject. Where personal data relating to a data subject are collected from the data subject, the information notice under Article 13 GDPR shall be given at the time when, and right before, personal data are obtained, with all of the following mandatory information (so-called "direct" information notice).[17] Where

[16] Opinion 8/2014, cit.

[17] Which shall include:

(a) The identity and the contact details of the controller and, where applicable, of the controller's representative, including reference to the agreement under Article 26 GDPR, and of the DPO, where appointed.

(b) The purposes of the processing for which the personal data are collected (e.g. marketing, for performing the service).

(c) Obligations imposed by law or by a contract under which the data are collected and consequence of not providing consent.

(d) Lawful basis under Article 6 GDPR (consent, contract, legal obligation, public interest, legitimate interest). If the processing is based on point (f) of Article 6 (1), such legitimate interests pursued by the controller shall be described.

(e) The recipients or categories of recipients of the personal data, to whom data shall or might be communicated (whether data processor or persons in charge of the processing).

(f) The fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission or of an agreement such as the EU-US Privacy Shield, standard contractual clauses, binding corporate rules, code of conduct, and certification mechanism, as well as reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

personal data have not been obtained from the data subject, the information notice shall be provided, in a reasonable time, within 1 month from the collection (subsequent information notice); if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; and if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.[18] In the event of a change in the purpose of the processing with respect to the purposes for which data were previously collected, the data controller shall provide a second information notice (additional information notice) which shall in any case be given before the processing begins for further purposes.[19]

(g) The period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period.

(h) The existence of the right to withdraw consent at any time, the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability and the right to lodge a complaint with a supervisory authority.

(i) The existence of automated decision-making, including the creation of profiles on the preferences and habits of the data subject (“profiling”), and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

[18] The following information shall be added to the ones listed in the previous note:

1. From which source the personal data originate and, if applicable, whether it came from publicly accessible sources.
2. The categories of the personal data and if such data belong to common, special, or judicial data.

Also, the information notice may not be provided insofar as:

- The provision of such information proves impossible or would involve a disproportionate effort.
- Obtaining or disclosure is expressly laid down by law, which provides appropriate measures to protect the data subject’s legitimate interests.
- Where the personal data must remain confidential subject to an obligation of professional secrecy.

[19] In addition to the information provided in the direct information, the following additional information shall be added:

1. Indication of the new purpose.
2. Data retention times with respect to the new purpose and, if not possible, the criteria used to determine this period.
3. Any legal or contractual obligations underlying the provision of personal data and consequences of the refusal.
4. The existence of automated decision-making processes, including profiling, and, in that case, the indication of the applied logic, as well as the importance and consequences of such processing for the data subject.
5. The rights of the data subject to withdraw consent, access the data, or request rectification or erasure of personal data, or the limitation of the processing of personal data concerning him; the right to data portability, to object to the processing, and to lodge a complaint with the supervisory authority.
6. If the data controller has not collected the data directly from the data subject, the additional information must contain the following further information:
7. The origin of personal data (i.e. how and from what sources have been collected), in particular any expressed indication that the data comes from sources accessible to the public.

Additionally, one other issue with consent appears in case of "tracking walls", which are mechanisms that exclude users from a given service if they refuse to extend their consent to other services.

The implications of this phenomenon for the IoT panorama induced the European Data Protection Supervisor ("EDPS") in recommending that, next to a general prohibition for any processing performed without consent, a similar but specific prohibition on tracking walls should be placed for e-objects where "no one shall be denied access to any information society services (whether these services are remunerated or not) on grounds that he or she has not given his or her consent under Article 8 (1)(b) to the processing of personal data that is not necessary for the provision of those services".[20]

The "non-centrality" of the user in IoT is also apparent in relation to the exercise of the right of access, pursuant to Article 15 of the GDPR;: as noted by the WP, users are in most cases unable to access the personal data collected by IoT devices, which inevitably results in the impossibility of making choices about such data; this, not forgetting also all the other rights that have to be guaranteed to the data subject under the GDPR: the right to rectification (Article 16); the right to erasure (Article 17); the right to restriction of processing (Article 18); the right to data portability (Article 20); the right to object (Article 21); and the right not to be subject to automated individual decision-making (Article 22).

In order to ensure greater protection for individuals, not only users, the legislator has imposed on economic operators using IoT devices to think about privacy as an instrument that should intervene not just after the damage has been caused but rather as a general preventive measure, that is, to ensure a "data subject-centric" approach aimed at preventing constant dialogue between devices and continuous processing of personal data, which could easily result in a violation of the individuals' right to self-determination in managing and control over their data.

Privacy enhancing technologies ("PETs") could be also a valid approach in ensuring privacy when using IoT devices. PETs consists of technologies or software products useful to enhance or improve data protection, for example, devices for blocking cookies, encryption systems, software that automatically set anonymity after a certain period of time, and P3P (Platform for Privacy Preferences) standards. The latter, in particular, is a protocol that allows users to compare their privacy settings with those of websites, so as to be able to decide in the course of navigation whether or not to accept the eventual risks displayed by P3P.[21]

Again, as above anticipated, a privacy by design approach that takes into great account data subjects' rights – as well as individuals' rights – in the IoT could prevent the described issues from arising. With such approach in mind, it is also pos-

8. Legal basis of the processing (e.g. consent, contract, legal obligation, public interest) and, if there is a legitimate interest of the data controller or the third party, the specification of such legitimate interest.

[20] https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf.

[21] See also http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1680228.

sible to think of instruments such as PETs or even simpler solutions, such as sticky policies, through which users are able to understand the processing of their personal data and give their informed consent.

6.3 Internet of Things and Big Data: A Dangerous Liaison?

The fast development of IoT and the resulting amount of data collected by e-objects lead to the inevitable growth of Big Data. The EDPS described the Big Data as "[t] he practice of combining large volumes of diversely sourced information and analyzing them, using more sophisticated algorithms to inform decisions".[22]

IoT technologies give a great contribution to Big Data by generating huge volumes of data, widely distributed and often unstructured but consistently produced. For these reasons, the Internet of Things and the analysis of Big Data are two issues that inevitably intersect on several aspects.

In recent years, great attention has been paid to the fact that every single data controller may have gathered large personal databases (i.e. collected through e-objects) from which to conduct analysis on, and profiling interests of, data subjects through the use of particular tools that can recombine information in a single dataset that in turn allows to get an exhaustive profile of subjects to be the potential target of, in most cases, commercial activities. There could be also the possibility that each pooled database may be sold to third parties, who already have some personal information, for enrichment in order to increase the level of knowledge of each individual's preferences.

In this perspective, a real "digital subconscious" is defined, considering that often Big Data analysis could generate entirely new data over the initial data, so the data subject may be unaware of the existence of other information.

It is evident that the assessment of compatibility between original and additional purposes takes on particular relevance when referring to Big Data. For these reasons, due attention shall be paid to the evaluation of privacy by design approaches and the performing of impact assessment on the processes related to the collection of personal data.

6.4 The US and UK Approaches

In the United States, the 2017 Internet of Things Cybersecurity Improvement Act, under discussion, sets the minimum security requirements for IoT devices.[23]

[22] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

[23] Internet of Things (IoT) Cybersecurity Improvement Act of 2017 available at https://www.congress.gov/bill/115th-congress/senate-bill/1691/text.

The legislation requires vendor commitments, such as IoT devices are patchable and devices don't contain known vulnerabilities. It also requires if a vendor identifies vulnerabilities, it must disclose them to an agency, with an explanation of why the device can be considered secure notwithstanding the vulnerability and a description of any compensating controls employed to limit the exploitability/impact of the vulnerability. Moreover, the legislation requires that the devices rely on standard protocols and that the devices don't contain hard-coded passwords.

Even the British Information Commissioner's Office ("ICO") has provided some suggestions for the management of IoT devices. First, the ICO suggests doing a thorough search before starting to use intelligent devices without focusing only on information and product features but extending these obligations on the manufacturer as well. Furthermore, it must be ensured that all access points, whether physical (router) or logical (login) devices, are secured through multiple layers of authentication, encryption, or other specific security features. Lastly, the ICO suggests periodically checking for security updates and making sure that the new version of the software is downloaded to all devices, considering that earlier versions might be more vulnerable to threats.

6.5 A New Perspective: "Data Protecy"

In this brief analysis, the author illustrated how the development of new technologies can revolutionise individuals' daily life despite the great risks that they bring with them. Prior to the advent of the Internet of Things, privacy on one side and the protection of personal data on the other have been kept separate. Intelligent "things" are objects belonging to the personal sphere as they deal with personal data, aggregate them, and create new information about the individual; the personal sphere, in fact, in the IoT era, has lost its traditional features and boundaries, opening the doors to objects that are able to act autonomously.[24] At the same time, there is a reversal of the role of the users/data subjects that become "non-users": objects that capture data have no interface and do not correctly inform the user who is often unaware of the ongoing data collection.

For all these reasons, the continuous processing of personal data in the IoT field could result in the intrusion into the private and family life, as defined by Article 7 of the Charter of Fundamental Rights of the European Union. In light of these considerations, the concepts of privacy and data protection need to be reconsidered not as two separate aspects but as a unicum, the "data protecy", a new form of protection which simultaneously ensures the protection of the personal sphere and that of personal data.[25]

Thanks to the intrinsic features of the IoT, we are witnessing the reunification of the rights that Articles 7 and 8 of the Charter of Fundamental Rights of the European

[24] L. BOLOGNINI, E. PELINO, C. BISTOLFI, op. cit., 723.

[25] ivi, 725.

Union has split. The concrete application of the data protecy will induce the user to activate several forms of protection but, above all, to self-enforce them; think about 3D privacy means that take into account the three-dimensional nature of the data collection, virtuality, and materiality, together with the necessary protection of the individual. Individual will probably start using tools that can prevent IoT sensors from the collection of personal data, in order to fill the interface shortcomings which are inner to the e-objects, silent spies of our private lives.[26]

The goal of all data protection authorities is to consider the technological process by evaluating its legal acceptability in terms of the protection of the rights of the individual. All of this is part of a broader perspective, namely, the necessity to realise the full compliance to the European rules: this can be achieved through the production of tools that make up a real physical shield for individuals and by the new provisions set out by the GPDR, to which the author referred to at the beginning of this paper, namely, accountability principle and the privacy by design approach, as well as all the several, different implementing and compliance actions which originate from them.

[26] ivi, 726.

Chapter 7
Universal Privacy Risk Area Assessment Methodology

Sébastien Ziegler

7.1 Introduction

In 2012, we started working on EAR-IT [1], a European research project on audio monitoring in smart cities and smart buildings. The main research focus was on audio signature recognition: the ability to leverage on Internet of Things deployment to listen to the urban environment and to identify events through their acoustic signatures. The researched technology enabled to identify car accidents, gunshots and other events that are relevant for municipalities. It could also be used to recognise the human activity in an office to adapt the heating and lighting, and to save energy. It could also be used in hospitals to detect patients needing help. The project implied effective tests and validation in the smart city of Santander in Spain, as well as in an office space in Geneva, Switzerland.

While the technological part of the research was quite exciting, we had to address the legal requirements in terms of personal data protection. Back then, the European norms for personal data protection were already quite strict and complex. A key challenge was to enable the researchers and the municipality to assess and ensure that deployed acoustic systems comply with the regulation. One of the main challenges was to translate complex legal obligations into a methodology that enables users who do not have a legal background to perform the compliance assessment by themselves. The project led to the creation of a first methodology named "Privacy Risk Area Assessment Tool", which was successfully applied to the IoT deployment in the context of the smart city and the smart office too.

Following the completion of EAR-IT, we decided to continue refining and extending the methodology to make it more universal. This effort has been supported through several projects, including the Privacy Flag European research project [2, 3], a 3-year

S. Ziegler (✉)
Mandat International, Geneva, Switzerland
e-mail: sziegler@mandint.org

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_7

Horizon 2020 European Innovation Action co-founded by the European Commission and the Swiss Ministry for Research and Education. Privacy Flag researched innovative approaches to assess the compliance of applications, products and services with data protection regulation. It more specifically focused on the obligations related to the European General Data Protection Regulation (GDPR) [4] and the Swiss data protection regulation. This effort has led to the development and specification of the Universal Privacy Risk Area Assessment Methodology (UPRAAM). While the UPRAAM was designed to assess the compliance of IoT deployments with the GDPR, it can also be applied to websites, smartphone applications and other objects to be evaluated.

7.2 Initial Requirements

The UPRAAM intends to efficiently assess the privacy compliance of Internet of Things deployments (and other technological solutions) with the applicable data protection regulations. It intends to provide a methodology for checking the GDPR requirements in an efficient manner and for identifying potential gaps or breaches.

In order to ensure the genericity of the methodology, the UPRAAM was designed to satisfy two quite distinct purposes of use:

- Simple assessment of the compliance of Internet of Things deployments, websites or smartphone applications by regular end users (crowd assessment).
- In-depth evaluation of the data protection compliance by experts, such as auditors or data protection officers.

The former requires a methodology that is easily understood and used by non-specialists. The latter requires to have a strong and highly accurate methodology that can be used in labelling or certification processes.

A set of key requirements has been used to guide the UPRAAM development, including:

- Reliability and trustability.
- Domain agnosticism, in order to be applicable to diverse objects, including websites, smartphone applications and IoT deployments.
- User-friendliness, enabling non-specialists to easily use and understand the methodology.
- Ability to encompass and address both legal and technical risks.
- Encompassing international, European and Swiss regulations.

7.3 Universal Privacy Risk Area Assessment Methodology

Privacy Flag has further extended and refined the Privacy Risk Area Assessment Tool [5, 6] designed in a previous European research project, EAR-IT, to prevent privacy breach when deploying audio monitoring solutions in smart cities and smart

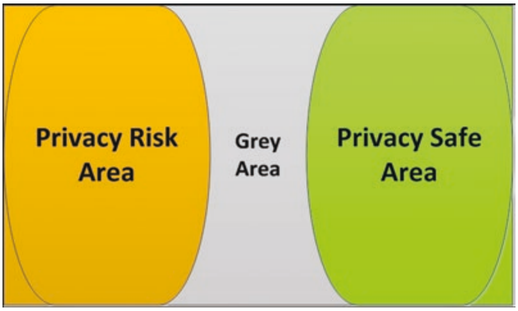


Fig. 7.1 Privacy Risk Area (PRA) and Privacy Safe Area (PSA)

buildings. The model has been extended to enable the assessment of data protection compliance of any product or service. The new methodology has been named "Universal Privacy Risk Area Assessment Methodology" or "UPRAAM" in short. The objective of this methodology is to overcome the inherent complexity of data protection regulations. In order to tackle this complexity, the UPRAAM uses the concept of "Privacy Risk Area", which is defined as an area in which the risk to breach someone's privacy rights is high. By opposition, a "Privacy Safe Area" is an area in which the risk to breach someone's privacy rights is very low. A grey zone area is implicitly emerging between those two previous notions, where the level or risk to breach someone's privacy rights is not clearly identified (see Fig. 7.1).

The Universal Privacy Risk Area Assessment Methodology (UPRAAM) leverages the abovementioned concepts in order to provide a user-friendly approach, which enables non-specialists without legal education to assess if a product, a service or an information management system is rather compliant with privacy obligations (in a Privacy Safe Area) or likely to breach some privacy rights (in a Privacy Risk Area). The proposed tool does not pretend to provide an absolute answer but a highly accurate estimation of the privacy compliance.

7.3.1 Comprehensive Data Protection Approach

In the context of the research, an important challenge was to develop a methodology that would be as universal as possible in terms of object to be evaluated, as well as to ensure that the results of the methodology will be relevant across various jurisdictions. The UPRAAM development started by identifying and analysing a set of legal obligations in terms of privacy and data protection, including:

International data protection obligations:

It analysed and took into account the relevant treaties and conventions from major international organisations, including inter alia:

- International Telecommunication Union (ITU).
- Organisation for Economic Cooperation and Development (OECD).
- United Nations (UN).

- Council of Europe (CoE).
- World Trade Organization (WTO).

European data protection regulations:

- The European General Data Protection Regulation [4], Regulation (EU) 2016/679 of the European Parliament and of the Council.
- Directive 2000/31/EC (electronic commerce) [7].
- Directive 2002/58/EC (privacy and electronic communications) [8].

In order to develop a fully compliant methodology with the EU law scenarios, this analysis has also taken into account the Opinions of Article 29 Working Party, which has been in charge of clarifying data protection related grey areas.

Swiss data protection obligations:

- Switzerland has a specific legal framework for data protection. In order to avoid any gap, the design took into account the specific Swiss obligations and more specifically:
- Swiss Federal Act on Data Protection (FADP).
- Swiss Federal Ordinance on Data Protection (DPO).
- Swiss Federal Ordinance on Data Protection Certification (DPCO).

US norms and regulations:

The project performed a gap analysis and extended the UPRAAM methodology towards the US federal and state obligations.

The legal requirements analysis enables to clarify and translate the requirements into a set of checks and controls. However, this is not sufficient. It requires to be completed by a complementary and systematic analysis of technical risks, which can be specific to a given scope of certification.

The following picture from the Privacy Flag project summarises the comprehensive approach of UPRAAM assessment criteria combining various sources of legal requirements together with identified technical risks in order to deliver a comprehensive evaluation (Fig. 7.2).

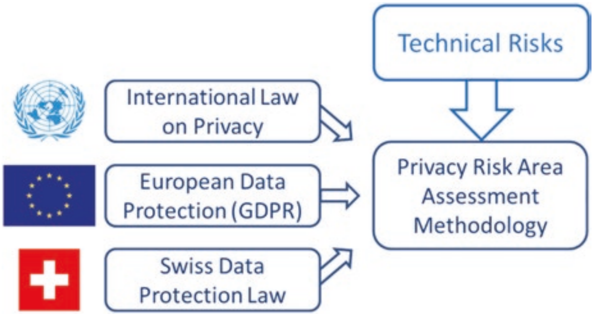

Technical Risks
International Law on Privacy
European Data Protection (GDPR)
Swiss Data Protection Law
Privacy Risk Area Assessment Methodology

Fig. 7.2 UPRAAM requirements

7.3.2 Generic Process

The UPRAAM is a multi-criteria assessment methodology based on a sequence of checks and controls, including:

1. A preliminary step, named "UPRAAM Profile Selection", which enables to pre-select and filter questions according to a category of objects. This is due to the fact that different objects correspond to different profiles of risks. For instance, the presence of cookies is a risk to be considered for a website, but not for an IoT deployment. This preliminary step enables to better target the questions and avoid the unnecessary ones.
2. An initial set of controls is proposed, where the user is invited to check a first list of criteria to determine if personal data are exposed to a risk. If the answers provided by the user leads to the conclusion that no personal data are exposed to risk, the assessment result is a Privacy Safe Area, and the analysis can be stopped there. If one or several criteria indicate a risk for personal data, complementary checks are triggered and presented to the user, in order to complete the assessment.
3. A set of contextual complementary checks are submitted to the user according to the information provided during the previous stage. This model enables also the possibility to extend the process with additional questions for in-depth analysis. According to the answers provided by the user, the assessment is refined until a reliable assessment can be made on whether the systems are in Privacy Safe Area. If not, it has a high probability to be either in a Privacy Risk Area or in a grey area.
4. The UPRAAM methodology enables users to focus on key factors of risk. In case of an unsuccessful result, the UPRAAM methodology preconises an iterative process. The user is invited to examine the key factors having caused a negative result and consider some adaptation to the deployment plan in order to mitigate those risks. Then the UPRAAM should be then applied again to the adapted deployment plan. If despite the iterative process (see Fig. 7.3) the result remains negative, a deeper analysis and consultation with the competent authorities are required.

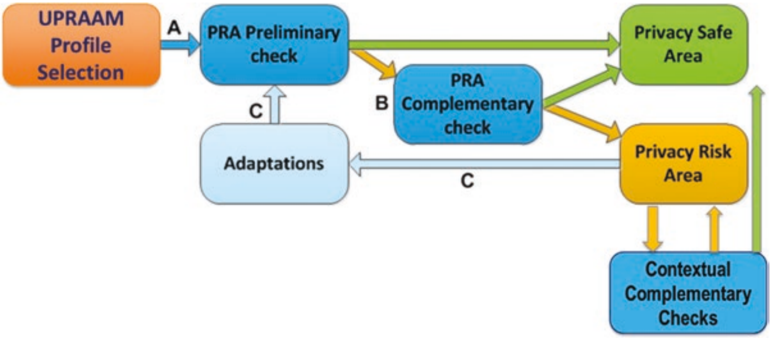


Fig. 7.3 UPRAAM iterative process scheme

7.3.3 Customisation

The UPRAAM can be customised to the scope of evaluation, as well as to the intended users. In order to test its genericity and reliability, the UPRAAM methodology has been researched and extended in two opposite directions:

(a) Simplified UPRAAM

Part of the research team worked on a simplified UPRAAM model designed for a crowdsourcing application. The objective was to enable regular citizens to assess the GDPR compliance of IoT deployments, websites and smartphone application. In order to enable non-specialist users to go through the process, key requirement was to make it as user-friendly as possible. This highly simplified version of the UPRAAM was able to reduce the process to less than 15 questions.

(b) In-depth UPRAAM

Another part of the research team worked with specialists in certification to design a highly reliable and systematic GDPR compliance assessment tool. The UPRAAM was adapted to the applicable ISO requirements and optimised to ensure a high trustable and efficient process to support detailed gap analysis and certification. Such models are designed for professionals, to support in-depth evaluation. This UPRAAM model comprises several hundreds of checks and controls. More details will be provided in this model in the next chapter.

Both models have been successfully tested and validated.

7.3.4 Asymmetric Access to Information

Beyond the level of granularity, the two models are asymmetric in terms of access to information.

The first UPRAAM model for crowdsourcing relies on the information which are directly available and easily accessible to the public. The UPRAAM model for the in-depth analysis requires access to a larger set of information, including from the data controller. It shall encompass information on the network and connectivity with the servers, the data storage, log and backup policies, contractual relations with data processors, etc. The level of granularity of the evaluation has obviously an impact on the level of reliability of the results: the more systematic the analysis will be, the more reliable the results will be.

The following drawing (Fig. 7.4) illustrates a simplified set of IoT and ICT deployments by a smart city or a company that are outlined in red. The blue outlined area illustrates the scope of in-depth compliance analysis compared to the simplified risk assessment by the crowd, which is outlined in green. This asymmetry in terms of access to information requires to adapt accordingly the UPRAAM implementation.

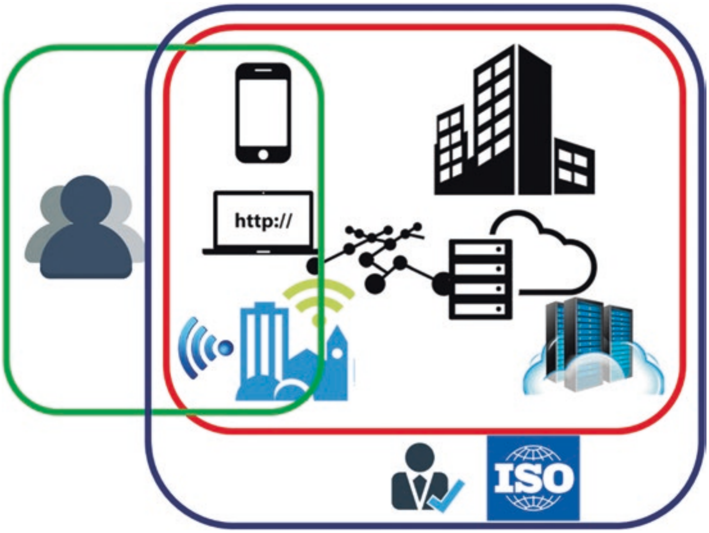


Fig. 7.4 In-depth evaluation scope

7.4 UPRAAM for Crowdsourcing

The Privacy Flag crowdsourcing model intended to research and combine the potential of crowdsourcing, ICT technologies and legal expertise to protect citizens' privacy when visiting websites, using smartphone applications, or living in a smart city. Its intension was to enable citizens to collectively monitor and control their privacy with a user-friendly solution made available in three distinct options: as a smartphone application, a web browser add-on and a public website—all connected to a common knowledge database. It provides a new paradigm of privacy protection combining "endo-protection" with locally deployed privacy enablers protecting the citizens' privacy from unwanted external access to their data and "exo-protection" with a distributed and crowdsourced monitoring framework able to provide a collective protection framework, together with increased citizen awareness and implicit incentives for companies to improve their privacy compliance.

7.4.1 UPRAAM Customisation for Crowdsourcing

The initial UPRAAM model developed in Privacy Flag was including about 150 checks and controls, defined to assess the compliance with most applicable data protection obligations. However, this initial theoretical model had to be adapted in order to address the specific needs and requirements of distinct applications. There are major differences regarding the UPRAAM adaptation to the crowd and to the

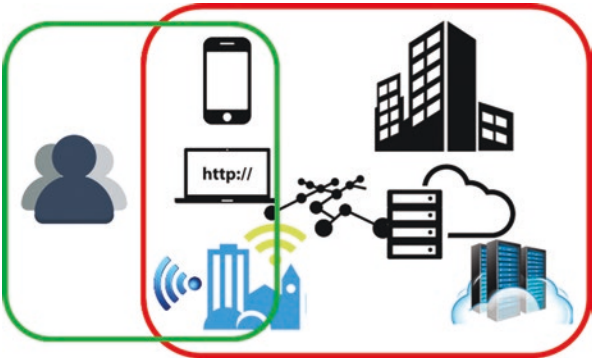


Fig. 7.5 Asymmetric access to information

certification requirements that led to two very distinct UPRAAM adaptations and implementations.

First of all, the crowdsourcing tools required to simplify as much as possible the UPRAAM model and to reduce it to about 15 questions in order to satisfy the end user adoption constraints and limitations. This simplification has a cost in terms of precision and reliability of the assessment results. The UPRAAM model for certification required exactly the opposite: a very systematic and detailed analysis of the compliance in order to maximise the reliability of the assessment result. This process led Archimede Solutions to develop a detailed UPRAAM with up to 650 potential checks and controls.

Another fundamental difference relates to information access. The crowd users can only access partial information, because part of the information is controlled and not disclosed by the owner of the solution or the service to be assessed. This cognitive limitation directly impacts and restricts the questions that can be answered by the end user. This is illustrated by the green delimited area of the following, Fig. 7.5, which constitutes the focus of the UPRAAM version for crowdsourcing.

By contrast, in the context of in-depth evaluation, the certification requires to access to a complete set of information and requires implicitly the cooperation of the owner of the object to be certified. As a consequence, the UPRAAM implementation for the certification needs to encompass the whole red area of the image.

7.4.2 *UPRAAM for Crowdsourcing Description*

In the Crowdsourcing model, the end user is at the core and assumes the central role in the process:

1. An end user in the crowd starts spotting and identifying a suspicious Internet of Things deployment (or a smartphone application, website, etc.).
2. The end user implicitly enables automatic ranking of the objects to be assessed according to the number of clicks/alerts received by the crowd.

3. The end user then contributes to assess the objects of concern according to a clear methodology, by applying the Universal Privacy Risk Area Assessment Tool and Methodology.
4. The crowd mutualises and shares the collective knowledge generated by the users into a common knowledge database benefitting to all the users.
5. The crowd finally contributes to disseminate and outreach the platform and tools.

The following section present the generic UPRAAM instantiation for the crowd-sourcing tools developed by the Privacy Flag project, from a user perspective, as indicated in the Fig. 7.6 below:

1. *Category selection*: A first step consists in selecting the category of object to be assessed. In Privacy Flag, we propose the three targeted options:

   (a) Websites evaluation.
   (b) Smartphone applications evaluation.
   (c) IoT deployments evaluation.

2. *Object description*: The user is invited to provide information on the object to be assessed, such as name, version, short description, company, and URL. Then, two threads are followed in parallel:

   (a) Automated tests (step 3).
   (b) User-driven evaluation (step 4 and subsequent).

3. *Remote tests*: A set of remote tests can be automated by Privacy Flag server, enabling, for instance, to identify cookies, check if SDNS is enabled, etc.

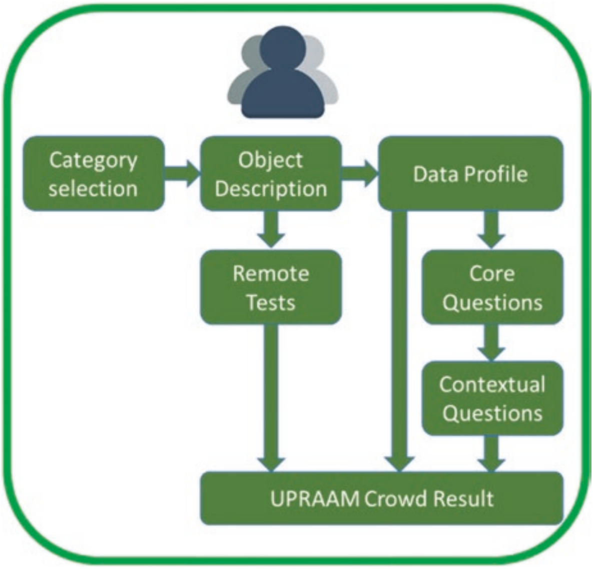


Fig. 7.6 UPRAAM crowd-driven evaluation methodology

4. *Data profile*: The end user is invited to identify the categories of personal data that are collected by the service or application to be assessed. If no personal data is collected, the evaluation leads to a privacy safe area situation. Otherwise, the process continues with the next step.
5. *More questions*: A set of core questions are submitted to the user in order to assess various dimensions of privacy risk and legal compliance.
6. *Contextual questions*: Additional contextual questions are submitted to the user according to the previous inputs provided by him.
7. *UPRAAM automated result*: Finally, once all the questions have been answered, the system provides an evaluation of the level of privacy risk.

7.5 Privacy Flag Crowdsourcing Assessment Tools

Leveraging on the UPRAAM, the Privacy Flag project has developed a distributed crowdsourcing privacy monitoring platform enabling the crowd to mutualise their efforts and resources by running a local Privacy Flag application on their smartphone and/or an add-on in their Internet browser. The designed platform monitors and identifies privacy breaches, informing the user about the alert and uploading the information in a central database to tag the application or website as suspicious and share this information with others. Privacy Flag has developed three components enabling interactions with the crowd through distinct interfaces:

- A Privacy Flag browser add-on to be included in the user's web browser.
- A Privacy Flag smartphone application.
- A Privacy Flag Observatory accessible to the public.

The two former ones enable the users to monitor and identify threats on their privacy when browsing on a website or using smartphone applications. They inform them through a user-friendly interface and enable them to contribute to the crowdsourcing platform. The latter one provides access to information on identified sources of privacy breaches.

7.5.1 Privacy Monitoring Agents

Privacy Flag also researched and developed privacy monitoring agents (PMA), which are software modules that users can deploy on their devices for monitoring and detecting suspicious smartphone applications or websites behaviour. They perform local checks on sensitive functions and data transmissions in order to inform the end user on identified risks for their data protection. It informs the users about any identified risk and may share information on suspicious applications or websites with the common knowledge database. Any information transfer is fully anonymised and filters out any personal data. An additional tool has been developed to enable full anonymisation of the remote connection to the Privacy Flag servers by using an onion routing protocol.

7.5.2 Privacy Flag Browser Add-On

The Privacy Flag web browser add-on is a tool that allows users to acquire information about potential privacy risks when browsing on the Internet. The add-on provides information on whether a website is considered safe—or not—based on an analysis conducted by the Privacy Flag back-end system. The analysis includes input gathered by technical enablers and exploits the power of crowdsourcing data from end users using the UPRAAM methodology. The Privacy Flag web browser add-on is one of the main points of interaction between end users and the Privacy Flag project.

7.5.3 Privacy Flag Apps

The Privacy Flag smartphone application allows users to collect and share information on potential privacy risks from installed applications in their mobile phones and tablets. The application informs users whether installed software is considered as "privacy friendly", or as "not privacy friendly", based on the analysis conducted by the Privacy Flag back-end system. The analysis includes input gathered by technical enablers and exploits the power of crowdsourcing data from end users using the UPRAAM methodology. In combination with the Privacy Flag web browser add-on, the smartphone application is one of the main points of interaction between end users and the Privacy Flag project.

7.5.4 Privacy Flag Observatory

The Privacy Flag Observatory provides a holistic overview of the privacy and security situation on the Internet. It visualises empirical data in a clearly and understandable way, in numerical and graphical formats, showing the adoption of best practices and standards on the web as well as identifying issues with obsolete, insecure, but still widely deployed, technologies. The PF Observatory is of use to stakeholders, legislators, web developers, security researchers, scientists and enterprises but primarily to European Citizens concerned about their digital data privacy.

Acknowledgments This chapter includes results shared by the European research project Privacy Flag and EuroPrivacy development led by Archimede Solutions. Images are shared on a non-exclusive basis as a courtesy of the contributors.

References

1. EAR-IT FP7 European Research project on IoT-based audio monitoring for smart cities and smart buildings, http://www.ear-it.eu. Accessed 28 July 2016
2. Privacy Flag is a European Research project on data protection, http://www.privacy-flag.eu. Accessed 28 July 2016
3. S. Ziegler, I.P. Chochliouros, L. Ladid, Privacy flag—collective privacy protection scheme based on structured distributed risk assessment, in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT)*, Milano, Italy, 14–16 Dec 2015
4. 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)(EU) 2016/679, in eur-lex.europa.eu
5. S. Ziegler, P.M. Kémo Sonko, P. Maló, Privacy risk area assessment tool for audio monitoring—providing a pragmatic solution, in *Proceedings of the ICT Law Conference 2013*, Porto, Portugal, 8–9 Nov 2013
6. S. Ziegler, P.M. Kémo Sonko, Privacy risk area assessment tool for audio monitoring—from legal complexity to practical applications. J. Int. Commer. Law Technol. **9**(3), 138 (2014). http://www.jiclt.com/index.php/jiclt/article/viewFile/210/207
7. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), in eur-lex.europa.eu
8. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("Directive on privacy and electronic communications"), in eur-lex.europa.eu

Chapter 8
GDPR Compliance Tools for Internet of Things Deployments

Ana Maria Pacheco Huamani and Sébastien Ziegler

8.1 Complying with Data Protection Regulations

The adoption of the European General Data Protection Regulation (GDPR) [1] had a global impact on the industry. It exposes all companies and public administrations that process personal data collected in Europe to massive legal and financial risks: non-complying companies are exposed to fines up to 20 million Euros or 4% of their worldwide turnover, whichever if the highest. Moreover, Internet of Things (IoT) deployment in smart cities brings an additional risk: the reputational and political risk. In many countries, a mayor that would suspected of spying on its citizens by deploying Internet of Things solutions in public space would probably face a political turmoil and difficulties to be re-elected.

In a more subtle manner, the GDPR requires that all European data controllers select data processors that are fully compliant with the GDPR, regardless of their location. This implies that non-complying data processors are likely to be excluded from the European market. IoT service providers storing and/or processing data in the Cloud are likely to be impacted by this regulation.

In such conditions, ensuring that IoT solutions deployed are fully compliant with the applicable data protection regulations is of utmost importance. We can identify three sets of needs and demands emerging from this new regulatory paradigm:

(a) **The need to identify, assess and minimise the risks** related to non-compliance with the GDPR, by performing a systematic gap analysis and addressing any identified non-conformity.

A. M. Pacheco Huamani (✉)
Archimede Solutions, Geneva, Switzerland
e-mail: ampacheco@archimede.ch

S. Ziegler
Mandat International, Geneva, Switzerland

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_8

(b) **The need to express the willingness of a company to comply with the GDPR**, by adopting a code of conduct, a seal, or a contractually binding commitment.
(c) **The need to demonstrate GDPR compliance**, for instance through independent third-party assessment and certification.

We will present emerging approaches and tools that have been researched and developed through the European research programme to address these demands.

8.2 Normative Heterogeneity

The GDPR intended to homogenise the data protection regulation among members States of the European Union. It triggered many countries to adopt similar regulations. In parallel, several international conventions are recognising some key principles in terms of personal data protection. There is a clear convergence towards an increased level of personal data protection.

However, there are still substantial differences from one jurisdiction to another. Even within the European Union, countries may rule additional and specific obligations at the national level. IoT deployments shall take into account the applicable rules in the jurisdiction where the IoT is deployed, as well as in the jurisdiction where the IoT data are to be processed.

8.2.1 Examples of Normative Asymmetry

Privacy Flag performed a few gap analysis. It analysed and compared the European GDPR with the US regulation. The US privacy law is specified through a large number of US federal and state norms. They were developed over time and are often domain specific. The US gap analysis resulted in concluding that, except for a few sector-specific obligations, the GDPR tends to provide a substantially higher level of protection of personal data. In such a context, there is an asymmetric situation, where a European IoT service provider has limited risks to breach a US obligation in terms of personal data protection, while a US-based company that is complying with the US law will not necessarily comply with the European regulation and may be exposed to legal and financial risks.

A gap analysis of the GDPR with the Swiss law on data protection led to more complex conclusions. The Swiss regulation on data protection is specified through three main norms:

- Swiss Federal Act on Data Protection (FADP) [2].
- Swiss Ordinance to the Federal Act on Data Protection (DPO) [3].
- Swiss Ordinance on Data Protection Certification (DPCO) [4].

Switzerland has a long tradition of privacy protection which impacted its regulatory framework. The Swiss regulation includes a set of specific obligations that are not formally included in the GDPR. Here are a few examples:

- Data processors in the health insurance domain have the legal obligation to certify their data protection management systems, with a dedicated Ordinance that frames the requirements for such certifications.
- Data controllers and processors have the duty to keep up to date their data, regardless of the data subject rights: *"Anyone who processes personal data must make certain that it is correct. He must take all reasonable measures to ensure that data that is incorrect or incomplete in view of the purpose of its collection is either corrected or destroyed"*. (FADP, Art 5.1.d).
- Data controllers and processors must inform the Swiss Data Protection Authority and declare *"their data files if:*

  (i) *They regularly process sensitive personal data or personality profiles, or*
  (ii) *They regularly disclose personal data to third parties"* (FADP Art. 11.3).

- Personal data requested by the data subject must be made available in printed format (FADP Art. 8.5).
- Inalienable right to information: *"No one may waive the right to information in advance"*. (FADP Art. 8.5).
- Data controllers and processors must apply very specific security measures, including:

  (i) *"a. Entrance control: unauthorised persons must be denied the access to facilities in which personal data is being processed.*
  (ii) *b. Personal data carrier control: unauthorised person must be prevented from reading, copying, altering or removing data carriers.*
  (iii) *c. Transport control: on the disclosure of personal data as well as during the transport of data carriers, the unauthorised reading, copying, alteration or deletion of data must be prevented.*
  (iv) *d. Disclosure control: data recipients to whom personal data is disclosed by means of devices for data transmission must be identifiable.*
  (v) *e. Storage control: unauthorised storage in the memory as well as the unauthorised knowledge, alteration or deletion of stored personal data must be prevented.*
  (vi) *f. Usage control: the use by unauthorised persons of automated data processing systems by means of devices for data transmission must be prevented.*
  (vii) *g. Access control: the access by authorised persons must be limited to the personal data that they required to fulfilment their task.*
  (viii) *h. Input control: in automated system, it must be possible to carry out a retrospective examination of what personal data was entered at what time and by which person"*. (OFDAP Art 9.1).

Reciprocally, some GDPR obligations are not covered by the Swiss regulation. One example is the right to data portability. As a consequence, there are effective risks that a European company complying with the GDPR may breach a Swiss regulation, and reciprocally a Swiss company may comply with the Swiss regulation but not necessarily with all the obligations of the GDPR. Despite the fact that the Swiss regulation is under revision, with the intent to bridge the identified gap with the GDPR, some specificities may remain in the future regulation.

8.3 Data Protection Risks Mitigation

The first measures to reduce the legal and financial risk is to properly identify any potential non-conformity. This process can be performed spontaneously by mobilising the compliance office of the company or by hiring some experts or consultants.

In order to reduce the legal and financial risks of IoT companies and IoT deployment owners, it is recommended to proceed with method. Here is a logical sequence of steps and actions that can be applied to minimise the risks:

1. This first step consists in identifying the applicable jurisdiction(s) and regulation(s), according to the location of the IoT deployment and IoT data processing.
2. The second step aims at identifying any personal data that may be collected and/or processed by the deployed system. Bear in mind that for the European regulation, the notion of personal data encompasses any data that can be linked to a natural person. As a consequence, IP addresses, video streams, car plate numbers, and geolocation data of mobile devices and vehicles will easily fall into the category of personal data. In order to be on the safe side, it is recommended to label all data that "could be" potentially linked to a natural person as personal data.
3. Where applicable, clear information shall be provided to the data subject on the processing of their data (purpose, process, retention, etc.), as well as a mechanism to easily contact the data protection officer of the controller.
4. It is recommended to perform a Data Protection Impact Assessment (DPIA) as specified in Article 35 GDPR. The DPIA intends to assess the potential risks of a data processing on data subject. It should be performed before collecting any data. It can also serve as an evidence to demonstrate the good faith of the data controller.
5. A systematic gap analysis should be performed, preferably by third party, to identify any potential non-compliance with the data protection regulation. The gap analysis should be as systematic as possible and should rely on a clear methodology.
6. All identified non-compliance shall be systematically addressed with the active support of the top management and where applicable with legal and technical experts.

7. Once all the non-compliances have been resolved, a third-party evaluation and certification can be considered.
8. A process should be put in place to regularly check and review the compliance.

8.3.1 UPRAAM In-Depth Evaluation

In the previous chapter, we introduced the Universal Privacy Risk Area Assessment Methodology (UPRAAM). Archimede Solutions, together with an international group of experts in data protection and certification, leveraged on the UPRAAM methodology in order to develop a tool for the in-depth assessment of GDPR compliance.

This UPRAAM in-depth evaluation model has been designed to address each and every obligations of the data protection regulation, with a focus on the GDPR and where applicable extending it towards complementary norms. The in-depth evaluation process comprises several hundreds of point of control, which are selected and applied according to the object to be evaluated. They are regularly updated and refined according to practice and the evolution of the obligations, including *juris prudency,* in order to ensure a seamless and comprehensive compliance assessment.

8.3.2 Voluntary Commitment

Another risk for companies delivering IoT services is to be excluded from the European market. European data controllers have the obligation to select data processors that commit to comply with the GDPR. For IoT service providers located outside of Europe and wishing to be active on the European market, it may be relevant to demonstrate their commitment to comply with the GDPR obligations. This is likely to become a standard requirement in call for tenders.

In order to address this need, Privacy Pact (www.privacypact.com) has been developed. It is a voluntary legally binding mechanism for entities located outside of the European Union. It enables them to voluntarily and contractually commit to respect and conform to the GDPR. It provides organisations located in countries such as Japan, Korea, China and the USA, with a legally binding label that shows their clear commitment to comply with European privacy and data protection law.

8.4 GDPR Certification Scheme

The GDPR makes over 70 references to certification. It recognises independent certifications as a means to demonstrate the compliance of a data controller with the law. The adoption of a certification is expressly mentioned by the GDPR as a factor to be taken into account by the judges when settling complaints and fixing the amount of the fines. The certification is also an opportunity to strengthen and protect the reputation of a company, a product or a service, and potentially to benefit from a competitive advantage.

As a continuation of the UPRAAM in-depth analysis tool, a GDPR certification scheme has emerged. The EuroPrivacy certification scheme (www.EuroPrivacy.org) was researched and developed by Archimede Solutions, a Swiss company, with the help of an international group of experts in data protection and certification, and the support of the European research programme. It is the only certification scheme whose development has been jointly supported by the European Commission and Switzerland.

8.4.1 Addressing Emerging Technologies

Certifying GDPR compliance for Internet of Things deployments require models and methodologies able to cope with emerging technologies. With increasing agility in data analytics, the risk of deanonymization of IoT data becomes higher and higher. A simple accelerometer in a smartphone can reveal a lot of information on its owner and its behaviour. A well-calibrated sensor able to report the precise level of gravity force, which varies from one place to another, can reveal information on the location of the data subject.

The EuroPrivacy certification scheme has been designed to adequately encompass emerging technologies with a focus on the Internet of Things, as well as on other emerging technologies, such as big data and artificial intelligence. It leveraged on international experts in these domains and close links with the International Internet of Things Forum. It also benefited of inputs from several Horizon 2020 European research projects on privacy and cybersecurity, such as ANASTACIA (privacy and security seal) [5], SAINT (cybersecurity) [6], Create-IoT [7] and U4IoT [8]. The latter aimed at promoting personal data protection among the five European Large-Scale Pilots (LSPs) on the Internet of Things financed by the European Commission. The LSPs encompass domains such as smart cities, wearables, smart transportation, smart agriculture and smart homes. Altogether, they gather over 150 European companies and research centres.

8.4.2 Initial Requirements

The EuroPrivacy certification scheme has been designed to address several objectives:

1. To design a methodology enabling an efficient and highly reliable evaluation of GDPR compliance.

2. To address specific risk-related emerging technologies, such as the Internet of Things, data analytics and artificial intelligence.
3. To increase the reliability of the result by performing a more systematic analysis and by reducing the subjective dimension of the evaluation.
4. To develop a methodology to provide a seamless certification scheme encompassing various data protection regulations, including of course the European General Data Protection Regulation (GDPR) but also other complementary national data protection obligations, such as the Swiss data protection law and applicable obligations contained in international conventions related to privacy and data protection.
5. To provide a comprehensive certification scheme that can be applied to:

   (a) Products, processes and services, in line with ISO/IEC 17065.
   (b) Information management systems and companies, in line with ISO/IEC 17021-1.

6. To optimise the cost by increasing the efficiency of the process.
7. To comply with Article 42 of the GDPR in order to be eligible as an official European data protection certification scheme.

The in-depth evaluation is expected to be performed through an active collaboration with the data controller, in order to effectively assess their compliance with data protection regulations and to potentially deliver a certification and/or labelling.

In-depth evaluation of GDPR compliance requires a quite deep, systematic and comprehensive analysis, in order to be trustable and meaningful. It needs combined expertise in data protection law and information and communication technologies, including cybersecurity.

Beyond the complexification of the analytical process, another challenge consists in aligning the methodology with the relevant and applicable ISO requirements for such certification processes. Such alignment is required to support proper certification processes and is requested by the GDPR itself.

Finally, the process must be very well structured in order to limit the risk of subjective biases in the assessment of conformity. It shall ensure homogeneous evaluation results, regardless of who are the auditors involved in the evaluation, as long as they are qualified.

- Reviewing and maintaining the EuroPrivacy certification scheme.
- Addressing and solving questions submitted to the board.
- Serving as an impartiality mechanism.

8.4.3 Normative Comprehensiveness

The GDPR defines a common framework for personal data protection among EU member States. However, within the EU, national regulations may still contain additional rules and requirements. Similarly, some countries, like Switzerland, have quite distinct regulations with additional and specific legal obligations. Similarly, several international conventions contain specific obligations in terms of privacy and personal data protection.

An important part of the work has focused on identifying and compiling all relevant legal and normative obligations and requirements to ensure a comprehensive data protection certification. The certification scheme was designed to ease the integration of complementary international and national regulations. The client and the certification body can decide to extend the scope of certification to additional data protection requirements. This enables companies to avoid duplicating the process and cost of certification.

As a consequence, EuroPrivacy encompasses:

- European General Data Protection Regulation (GDPR)—Regulation 2016/679 of 27 April 2016.
- Fundamental international law obligations related to privacy, such as:
  - The Universal Declaration of Human Rights [9].
  - International Covenant on Civil and Political Rights [10].
  - Convention on the Rights of the Child [11].
  - Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families [12].
  - International Telecommunication Convention of Nairobi [13].
  - Convention 108 of the Council of Europe [14].

It can be extended to complementary data protection related obligations, including:

- Specific national laws, such as the Swiss Federal Act on Data Protection (FADP) and its two ordinances.
- European Directives such as 2002/58/EC (ePrivacy) or 1148/2016 (NIS Directive).
- European Regulations such as 910/2014 (eIDAS).

It has been optimised to be easily combinable with Information Security Management System (ISMS) audit and certification according to ISO/CEI 27001.

8.4.4 Overcoming ISO Certification Gap Through a Hybrid Certification Scheme

On one hand, IoT deployments are based on products and services. On the other hand, the main risk may reside in the way collected data are processed and stored, which is more related to the information management system.

According to ISO standards, the methodological approaches to certify a product and an information management system are quite distinct in terms of normative references and processes. The certification of products, services and processes is usually based on the standard ISO/IEC 17065. The certification of data protection management systems would be in principle based on the standard ISO/IEC 17021–1.

The EuroPrivacy certification schemes has managed to overcome this divide by providing an integrated and comprehensive approach with a hybrid model that complies with both sets of ISO norms and requirements, as well as with the GDPR requirements regarding certification.

It enables the process to be comprehensive in terms of applicable scope, from devices and software to online services and companies. This is particularly important for IoT deployments, which are often characterised by a dual nature. The risk for personal data in IoT deployment may occur at the level of the IoT devices (as a product) and at the level of the information management system.

8.4.5 Effective Application

After being specified, the EuroPrivacy certification scheme has been shared with the European Centre for Certification and Privacy (ECCP) [15], which has established a board of international experts in data protection. This board gathers seasoned experts who encompass data protection law covering national, European, and international data protection law, cybersecurity, certification and end users. It is in charge of:

- Reviewing and maintaining the EuroPrivacy certification scheme.
- Supervising the use of the certification scheme.
- Serving as an appeal, complaint and impartiality mechanism.

The EuroPrivacy certification scheme has been successfully applied to IoT deployments in smart cities, as well as to software as a service, products and information management systems. It enabled to deliver independent and comprehensive assessments of compliance, and, where applicable, certification of such compliance with the data protection regulations. Apart from the certification itself, the process enables performing a quite systematic and detailed gap analysis for identifying areas of improvement.

The EuroPrivacy certification scheme has been particularly successful in addressing the dual nature of IoT deployments: product (IoT devices) and information management system (processing of data by the infrastructure owner).

In order to test and validate the normative comprehensiveness, the certification scheme has been applied to joint certification on the GDPR and the Swiss data protection law, as well as on joint certification with ISO/IEC 27001.

In 2018, the EuroPrivacy scheme has been officially adopted by the SGS, the world leader on the market of inspections and audits [16].

8.5 Conclusion

The GDPR adoption will require a general effort to align a myriad of products and services with the new regulation, including IoT deployments. Data controllers and processors have a strong incentive to ensure compliance with the regulation and to demonstrate their compliance by certifying their products and services. The UPRAAM in-depth evaluation tool, the EuroPrivacy certification scheme, and Privacy Pact are examples of emerging solutions to ensure and demonstrate compliance with privacy and personal data protection. These solutions have been designed to specifically address the European requirements, but they can easily be applied in other regions. While the GDPR has been perceived as a major challenge by the industry, demonstrating personal data protection may also be an opportunity to increase the level of trust in IoT deployments and probably an unavoidable requirement to obtain market acceptance for massive IoT deployments.

Acknowledgments This chapter includes results shared by the European research project Privacy Flag, which has received funding from the European Commission and the Swiss State Secretariat for Education, Research and Innovation. The images included in this article are shared with the editor on a non-exclusive basis by their authors.

References

1. European General Data Protection Regulation (GDPR)—Regulation 2016/679 of 27 April 2016
2. Swiss Federal Act on Data Protection (FADP)
3. Swiss Ordinance to the Federal Act on Data Protection (DPO)
4. Swiss Ordinance on Data Protection Certification (DPCO)
5. H2020 research project: Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures (ANASTACIA), www.anastacia-h2020.eu
6. H2020 research project: Systemic Analyzer In Network Threats (SAINT), www.saint-h2020.eu
7. H2020 research project: CRoss fErtilisation through AlignmenT, synchronisation and Exchanges for IoT (Create-IoT)
8. H2020 research project: User Engagement for Large Scale Pilots in the Internet of Things (U4IoT), https://u4iot.eu
9. The Universal Declaration of Human Rights, http://www.ohchr.org/EN/UDHR/Documents
10. International Covenant on Civil and Political Rights, New York, 16 Dec 1966, http://treaties.un.org/pages/CTCTreaties
11. Convention on the Rights of the Child, http://www.ohchr.org
12. Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, http://www2.ohchr.org/english/bodies
13. International Telecommunication Convention Concluded at Nairobi, 1982
14. Convention 108 of the Council of Europe
15. European Center for Certification and Privacy based in Luxembourg, www.eccpcenter.com
16. SGS Partners with EuroPrivacy to deliver the first Comprehensive Data Protection Certification for Demonstrating GDPR Compliance, https://www.sgs.com/en/news/2018/11/EuroPrivacy-certification-demonstrates-gdpr-compliance

Chapter 9
Towards Trustable Internet of Things Certification

Lucio Scudiero and Sébastien Ziegler

9.1 Introduction and Problematic

IoT is booming. In 2017 the number of connected devices has overcome that of human beings on the planet, with 8,4 billion of objects against 7,5 billion inhabitants of the Earth.[1] Sensors, mobile phones, wearable objects, RFID tags, cameras and middleware components have a common feature: they are all points of entrance of data, and some of them can be personal data. As the IoT industry heavily leverages on data analytics to deliver services and increase consumers' welfare, personal data protection and security constitute critical elements in the "value creation chain" of IoT.

The IoT makes traditional cybersecurity challenges escalate and multiply. This happens for several reasons. The IoT environment is uncertain and dynamic. It is based on the interactions of heterogeneous components, including embedded systems, networking equipment, smart sensors, cloud infrastructures and humans. IoT systems are imbricated at different scale, including highly constrained networks, that rely on diverse security standards and privacy policies.

From a data protection viewpoint, data subject's control on personal data becomes more difficult due to the dispersed number of data sources and entities processing personal data; as the chain of providers of IoT services stretches, allocation of responsibilities and enforcement of data protection law become more complex than before; and the same can be said with regard to compliance to the principles of purpose limitation and data minimisation. Moreover, it is not always easy to identify the viable legal ground for personal data processing. The data subject's

[1] Estimates by the research company Gartner. Available at https://www.engineering.com/IOT/ArticleID/15594/IoT-Devices-to-Outnumber-Humans-in-2017.aspx.

L. Scudiero (✉)
Archimede Solutions, Geneva, Switzerland
e-mail: lscudiero@archimede.ch

S. Ziegler
Mandat International, Geneva, Switzerland

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_9

consent is quite difficult to collect for IoT deployments, and the legal basis—especially in the Smart Cities domain—may depend on a complex combination of legal basis at various levels.

While end-users are looking for trustable IoT deployments, it is difficult for end-users to fully trust IoT solutions because of their complexity. Individuals sharing personal data usually do not have a complete understanding of how the architecture is built up, how security measures are implemented and who has access to the data. This highlights an important challenge for IoT: the information asymmetry.

Information asymmetry can be addressed by means of technical and organisational solutions. One of those measures is certification of IoT, from privacy and security standpoints. Certification may, in fact, cover each and all the main privacy and security concerns spurred by the deployment of IoT and—besides demonstrating the compliance of the organisations behind it—may help establishing a relation of trust amongst IoT services/goods providers and users. As Recital 100 of the European General Data Protection Regulation (EU/679/2016, hereinafter the "GDPR") puts it: "In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services".

Certifications may, for example, help data subjects assessing major privacy issues identified during a sweep on IoT by the Global Privacy Enforcement Network, which comprises 60 data protection regulators from 39 jurisdictions. The study was carried out on 300 devices and revealed that:[2]

- 59 percent of devices failed to adequately explain to customers how their personal information was collected, used and disclosed.
- 68 per cent failed to properly explain how information was stored.
- 72 percent failed to explain how customers could delete their information off the device.
- 38 percent failed to include easily identifiable contact details if customers had privacy concerns.

In the following section, we will introduce the potential of certification mechanisms as a tool to fill the structural and intrinsic knowledge gap between IoT data controllers and the end-users. We will consider solutions such as Trusted IoT Label (or Seal)[3] and/or a Dynamic Security and Privacy Seal.[4]

[2] More information on the GPEN's survey can be found at https://www.privacyenforcement.net/node/717/.

[3] This subject is at the core of the research in the project Create-IoT, which has partly funded the research for this article. Create-IoT is funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation, under Grant Agreement N° 732929.

[4] This subject is at the core of the research in the project ANASTACIA, which has partly funded the research for this article. ANASTACIA is funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation, under Grant Agreement N° 731558.

9.2 The Framework for Data Protection Certification in the GDPR

There is a strong and widely disseminated emphasis on certifications in the GDPR, which reflects the centrality of this item in the policy option underlying this Regulation. Certifications emerged as a pivotal tool which reconciled both business and regulators' needs.[5] Certification mechanisms enhance the internal market dimension, and "EU-wide certification system for data controllers' compliance with their data protection obligations would provide them with full legal certainty in an ex-ante verification process".[6] The certification is also key beyond the border of the European Union: "Development of an EU-wide certification/standardisation scheme (privacy seal) (…) could be beneficial for both controllers, in the EU and in 3rd countries, as it could make their compliance more 'visible', and for individuals, who would be reassured that their data are effectively protected".[7]

The central provision for certifications is Article 42 of the GDPR, pursuant to which the establishment of certification mechanisms (and of data protection seals and marks) should be encouraged by all the institutional stakeholders in the Union for the purpose of demonstrating compliance with the Regulation of processing operations by controllers and processors.

The underlying idea is clarified by a systematic reading of the GPDR, where 72 references to certification mechanisms are scattered in connection with specific legal devices and legal obligations. The GDPR highlights that the following requirements can be demonstrated by means of certification mechanisms:

1. Compliance with the principles of privacy by design and by default (Article 25.3)
2. Sufficient guarantees provided by the processor, namely:
   (a) Implementation of appropriate technical and organisational measures in compliance with the GDPR (Article 28.1)
   (b) Compliance with the controller's instructions on the engagement of further processors in the context of the same personal data processing (Article 28.2)
   (c) The typical content of the so-called data processing agreement binding the processor to the controller (Article 28.3; read in conjunction with Article 28.6)
   (d) The legal arrangements made by the first processor to shift downstream in a chain of sub-processors the obligations undertaken in respect of the data controller upstream of the chain (Article 28.4)

[5] Commission Staff Working Paper—Impact Assessment accompanying the GDPR and the Directive on personal data protection in law enforcement, {COM(2012) 10 final}, {COM(2012) 11 final}, {SEC(2012) 73 final}. Available at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

[6] Commission Staff Working Paper - Impact Assessment accompanying the GDPR and the Directive on personal data protection in law enforcement, {COM(2012) 10 final}, {COM(2012) 11 final}, {SEC(2012) 73 final}, p. 71.

[7] Ibidem, p. 73.

   (e) The typical content of the "data processing agreement" binding the subprocessors downstream to the first processor upstream (Article 28.6 read in conjunction with Article 28.4)

3. Compliance with the requirements for the security of processing (Article 32.1; read in conjunction with Article 32.3)
4. The existence of appropriate safeguards for the transfers of personal data to third countries or international organisations from controllers and processors established in the EU (Article 46.2.f):

   (a) This will be symmetrically applicable to controllers and processors not subject to the Regulation, which may adhere to certification mechanisms recognised in the EU in order to be considered offering adequate safeguards and receive personal data from EU-based organisations (Article 42.2; read in combination with Article 46.2.f).

The importance of adhering to a certification mechanism is reinforced by the fact that it constitutes an element against which the supervisory authorities can measure—in both positive and negative terms—the behaviour of controllers and processors when deciding if an administrative fine shall be imposed and for what amount (quantum), as set out by Article 83.

This having been said regarding the potential content and the "legal incentives" to adhere to a certification mechanism, it remains to be seen how such certification can be obtained, by whom and with what legal value.

Certifications are issued by certification bodies ("CBs") or the competent Data Protection Authorities ("DPAs"), on the basis of criteria elaborated by the latter (Article 42.5) or by the European Data Protection Board ("the Board") in the framework of the consistency mechanism envisaged by Article 63; this mechanism is—in summary—a device for institutional cooperation and dispute resolution amongst DPAs in cases of issues having cross-border nature. For the certifications, it means that when the criteria for certifications are approved by the Board, and are adhered to by organisations established in the EU, they may result in a common certification, the European Data Protection Seal.

In order to be valid under the GDPR, certifications must be issued by CBs which are accredited by:

- The competent DPA (Article 43.1.a)
- The national accreditation body named in accordance with Regulation (EC) No 765/2008 in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority (43.1.b.)
- The Board itself (Article 70.1.o)

As may be seen from the discussion above, a double set of criteria is to be developed by the DPAs for the proper working of the certification machinery established by the GDPR:

- Criteria related to the certification mechanisms
- Criteria related to the accreditation of the CBs

On top of these, a set of additional requirements—again approved by the DPAs—is mentioned in relation to the accreditation of CBs carried out by the National Accreditation Authority named in accordance with Regulation (EC) No 765/2008.

It is to be noted that the GDPR-related certification complements, but does not substitute to, cybersecurity certifications. The IoT value chain, which is in itself stretched and complex in terms of personal data protection roles, shall have to cope with the GDPR framework above described as well as with the European Commission proposal for a “Cybersecurity Act”,[8] whose aim is to introduce a “European cybersecurity certification scheme” that shall attest that the ICT products and services that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist at a given level of assurance.

As clarified by the European Commission in the assessment accompanying the proposal, the cybersecurity certification scheme “is without prejudice to the certification of data processing operations, including when such operations are embedded in products and services, under the GDPR”.[9] This gives us the opportunity to highlight the distinction between both certifications. The GDPR certification goes far beyond the duty to secure processed data; it requires to address the whole set of GDPR obligations, including the effective implementation of data subject rights.

9.2.1 Electronic Certificates as Trust Services Regulated by the eIDAS Regulation

The GDPR certification model is somehow mirrored in another relevant source of EU law, namely, Regulation EU 910/2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter “eIDAS Regulation”),[10] which sets forth rules for the provision of trust services in Europe and the recognition thereof in all the member states.

According to the eIDAS Regulation, a trust service (hereinafter “eTS”) is:

> “an electronic service normally provided for remuneration which consists of:
>
> (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
>
> (…)
>
> (c) the preservation of electronic signatures, seals or certificates related to those services;”

[8] See the “Cybersecurity Package” proposed by the European Commission, https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en.

[9] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”), COM(2017) 477 final, 2017/0225 (COD), p. 13.

[10] Regulation 910/2014, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN.

Table 9.1 Landscape of tools and roles regulated by the eIDAS Regulation

Landscape of tools/roles in the eIDAS Regulation	Definition
Electronic trust service ("eTS")	An electronic service normally provided for remuneration (e.g. an electronic signature or an electronic seal)
Qualified trust service ("QTS")	An electronic service which meets the requirements laid down by the eIDAS Regulation
Trust service provider ("TSP")	A natural or a legal person who provides one or more trust services
Qualified trust service provider ("QTSP")	A trust provider which is accredited by the national supervisory authority and provides one or more QTS

The reason this is relevant for the discussion on how to make IoT trustworthy is that the models envisaged by the eIDAS Regulation—which in itself does not apply to any of the IoT deployments—and the one provided for by the GDPR, combined together, could serve the purpose of the automated certification of the IoT and lead to the creation of an IoT Trusted Label[11] or to an enhanced Dynamic Security and Privacy Seal for IoT.[12]

The eIDAS Regulation aims at creating a European internal market for eTS—namely, electronic signatures, electronic seals, timestamp, electronic delivery service and website authentication—by ensuring that they will work across borders and have the same legal status as traditional paper-based processes.

The architecture designed by the Regulation entails that the mentioned services are provided for by a "trust service provider" (hereinafter "TSP"), defined as a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider; in order to be qualified, a TSP shall be granted such a status by the supervisory authority named in accordance with the eIDAS Regulation and provide one or more eTS which are, in turn, "qualified", because they meet the requirements laid down by the Regulation (Table 9.1).

Amongst the eTS disciplined by the eIDAS Regulation, we shall focus specifically on the "electronic seal" (hereinafter also "ES") and the certificate which renders it a "qualified" electronic seal, because the model it is based upon can be conceptually extended, by analogy, to the certification of the IoT and result into the attribution of a Trusted IoT Label (or Seal) or a Dynamic Security and Privacy Seal.

Under the eIDAS Regulation, the electronic seal is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. The ES can be further specified and become:

[11] This subject is at the core of the research in the project Create-IoT, which has partly funded the research for this article. Create-IoT is funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation, under Grant Agreement N° 732929.

[12] This subject is at the core of the research in the project ANASTACIA, which has partly funded the research for this article. ANASTACIA is funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation, under Grant Agreement N° 731558.

(a) "Advanced electronic seal", meaning an electronic seal, which meets the requirements set out in Article 36
(b) "Qualified electronic seal", meaning an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal

The following table summarises the types of seals foreseen by the eIDAS Regulation and their legal value (Table 9.2).

Once described the legal framework underpinning the eTS, it may be argued the convergence of the certification model foreseen by the GDPR towards the one established by the eIDAS.

In this sense, the certification bodies to which the GDPR entrusts the issuance of valid data protection certification could be considered as TSPs, more specifically as QSTPs, given the fact that under both sources of law, they would be accredited by a supervisory authority. In that capacity, they could issue electronic seals, with the following possible deployments, amongst the many:

Table 9.2 Types of seals foreseen by EIDAS Regulation

Type of seal	Requirements	Legal value	Other relevant elements
Electronic seal ("ES")	It is provided by a TSP	(a) It ensures data's origin and integrity (b) It may be recognised legal effect and admissibility as evidence in legal proceedings	—
Advanced electronic seal ("AES")	(a) It is uniquely linked to the creator of the seal (b) It is capable of identifying the creator of the seal (c) It is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation (d) It is linked to the data to which it relates in such a way that any subsequent change in the data is detectable	(a) It ensures data's origin and integrity (b) It shall be recognised legal effect and admissibility as evidence in legal proceedings	—
Qualified electronic seal ("QES")	All requirements listed above from (a) to (d) + (a) Created by a qualified electronic seal creation device (b) Based on a qualified certificate for electronic seal	(a), (b) Above + (c) It shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which it is linked	"Certificate for electronic seal" means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person

- Trusted IoT Label (or Seal)
- Dynamic Security and Privacy Seal

Based on a combined reading of the attributes envisaged by both the GDPR and the eIDAS Regulation, such a seal would have the following characteristics:

(a) Be uniquely linked to the creator of the seal (e.g. the platform provider in a IoT deployment, or the manufacturer of the smart devices connected to the Internet in a certain IoT ecosystem, etc.).
(b) Be capable of identifying the creator of the seal (e.g. the platform provider in a IoT deployment, or the manufacturer of the smart devices connected to the Internet in a certain IoT ecosystem, etc.).
(c) Be created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation.
(d) Be linked to the (personal) data to which it relates in such a way that any subsequent change in the (personal) data is detectable.
(e) Enjoy the presumption of integrity of the personal data and of correctness of the origin of that data to which it is linked (this only in case of such a seal meets the requirements of a “qualified” Trusted IoT Label or Seal).

Clearly, the most advanced version of such a seal, namely, the QES, would derive its legal value from adherence to a certificate which, in turn, should meet the requirements set forth by ANNEX III to the eIDAS Regulation.

Qualified certificates for electronic seals shall contain:

(a) An indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal
(b) A set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the member state in which that provider is established and:
    - For a legal person: the name and, where applicable, registration number as stated in the official records
    - For a natural person: the person’s name
(c) At least the name of the creator of the seal and, where applicable, registration number as stated in the official records
(d) Electronic seal validation data, which corresponds to the electronic seal creation data
(e) Details of the beginning and end of the certificate’s period of validity
(f) The certificate identity code, which must be unique for the qualified trust service provider
(g) The advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider
(h) The location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge

(i) The location of the services that can be used to enquire as to the validity status of the qualified certificate
(j) Where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing

Further to that, the certificate should also contain an engineered version of privacy policies against which the actual processing of personal data should be regularly tested, in order to ensure that the Seal (or Label) actually portrays a truthful status of data protection compliance over the time, while being breached every time there is a departure from the predefined privacy policy objectives.

The model sketched in this section resembles the more traditional certification mechanisms used by certification bodies on the basis of approved standards, in that it similarly relies on third parties which perform checks against a predefined set of values (standards), yet it does so in automated fashion which seems, in principle, more adaptive to the context of the digital environment.

In the next section, the traditional approach to certification will be presented, in order to discuss the advantages and the criticalities of both models in Sect. 9.5. However, it is clear that its practical functioning heavily depends on the technical possibility to embed policy values into the seal and, once this issue is solved, into the explicit legal recognition of such a possibility by means of an amendment to the GDPR which should contemplate the possibility to issue certifications also in the forms envisaged by the eIDAS Regulation, mutatis mutandis.

9.3 Conventional Approach to Certification

The conventional model of certification is a human-based activity; it usually targets a product, a service, a system or a combination thereof, in order to assert their conformity to a predefined set of standards. This exercise is carried out by a party (third party) which is external and independent from the one who seeks the certification.

Therefore, the main components of the traditional model for certification are:

- A product or a service undergoing the procedure, usually defined as Target of Evaluation (or “ToE”)
- An entity performing the certification (“certification body” or “CB”)
- Auditors entrusted by the CB to run the assessment which precedes the certification
- A set of standards against which the assessment is performed and upon which the certification is eventually issued

The procedure for certification is usually triggered by the product or service provider that wish to obtain a certification either to increase the reliability of the ToE or because it is mandated to do so by law.

The certification request is made to a certification body, which can then start a conformity assessment; such assessment involves a set of processes that show the ToE meets the requirements of a standard.

Undergoing the conformity assessment process has a number of benefits:

- It provides consumers and other stakeholders with added confidence.
- It gives the certified company a competitive edge.
- It helps regulators ensure that health, safety or environmental conditions are met.

One of the main forms of conformity assessment is certification, defined as the provision by an independent body of written assurance (a certificate) that the ToE in question meets specific requirements.

In some instances, such as the one regulated by the GDPR and described above, a CB shall be accredited to be able to perform certification activities, meaning that it must be formally recognised by an independent body, generally known as an accreditation body, which guarantees that the CB operates according to international standards.

Another fundamental piece of the certification processes are standards, namely, the rules used to certify a ToE.

Under EU law,[13] "standard" means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, and which is one of the following:

(a) "International standard" means a standard adopted by an international standardisation body.[14]
(b) "European standard" means a standard adopted by a European standardisation organisation.
(c) "Harmonised standard" means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation.
(d) "National standard" means a standard adopted by a national standardisation body.

The standard making process is regulated, in Europe, by Regulation (EU) No 1025/2012 on European standardisation, according to which the European Commission can make a request to the European Standards Organisations ("ESO") to adopt a "harmonised standard" in the meaning of Article 2 (1) (c) therein, namely, a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation.

This framework has been used, for example, to develop the standards necessary to implement the eIDAS Regulation. In fact, to support this new regulation in Europe as well as the needs of the international community to provide trust and confidence in electronic transactions, ETSI's Technical Committee on Electronic

[13] Regulation (EU) No 1025/2012 on European standardisation, Article 2 (1). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF.

[14] Such as the famous ISO.

Signatures and Infrastructures (TC ESI) has published a set of standards for trust services providers (TSP), electronic signatures, electronic seals and electronic timestamps. The set includes a total of 19 European Standards along with guidance documents and test specifications.[15]

The same framework is referred to by the GDPR, whereby it is stipulated that:

"The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2)".[16]

Besides, standards may also be adopted by standardisation bodies independently from a request from the European Commission.

Be that as it may, eIDAS and GDPR standards will be used by traditional certification bodies to carry out conformity assessments of ToEs and issue privacy certifications.

This will require an important effort by individual auditors, whose length will vary depending on the complexity of the ToE, and result in a certification that will only be able to take a "picture" of a given ToE's conformity to standards at a given moment. The challenge is therefore to reconcile this fix model with the dynamicity of the IoT landscape, where devices, platforms, processes and providers may vary quickly in over short time frames.

9.4 Electronic Privacy Certification

As previously mentioned, traditional models of certification can be costly and lengthy in nature and may inadequately fit with the main features of IoT. In the context of security certification of IoT, it was already pointed out by some distinguished researchers[17] that "two challenges have a higher priority for a trusted deployment of IoT. The first is the uncertainty and dynamic environment of IoT. Uncertainty is intrinsic in IoT Systems due to novel interactions of embedded systems, networking equipment, smart sensors, cloud infrastructures, and humans. With respect to Security and Trust aspects, this uncertainty is a major potential cause of security breaches. While monitoring or misbehaviour detection systems

[15] For a complete list of ETSI's eIDAS standards, see https://portal.etsi.org//TBSiteMap/ESI/ESIActivities.aspx.

[16] See Article 43 (8) and (9) of the GDPR.

[17] *See* G. Baldini, A. Skarmeta, E. Fourneret, R. Neisse, B. Legeard and F. Le Gall, "Security certification and labelling in Internet of Things," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 627–632. doi: 10.1109/WF-IoT.2016.784551.

can be used to identify potential security breaches, a testing and certification phase with adequate coverage and linked to the main known security vulnerabilities can mitigate this uncertainty. The second challenge is the scale and heterogeneity of future IoT systems with different security standards, which may also change their configurations in time".

Mutatis mutandis, what holds true for security, holds true for privacy certification too. The question is therefore whether it is possible to retrieve in the Trusted IoT Seal (or Label) and Dynamic Privacy and Security Seal a suitable mechanism for IoT certification, in the light of the shortcomings of the traditional model of certification.

Traditional certification models require time and may cause delay in the commercialisation of products and services, with the risk that they remain behind the curve of the state-of-the-art. In addition, the evaluation has to be performed by bodies that deploy a variable amount of human resources and time which is costly, and the cost must be absorbed by the vendors, thus becoming a serious hurdle for commercialisation (especially in IoT). Another issue is the management of changes in the IoT certified product. As already mentioned previously, traditional certification frameworks certificate a specific ToE in given configuration. As a consequence, any changes to the configuration or any updates to the product that affect the ToE, which is the part of the product that is evaluated, may invalidate the certification. This brings us back to the need to address dynamic changes which are consubstantial to IoT products and services.

A model based on electronic certificates could tackle several issues surrounding the privacy and security certification of the IoT, namely:

- The need to ensure that personal data's integrity is not compromised
- The implementation of the principle of accountability, because the electronic seal would always certify the identity of its creators, which are those who participate to personal data processing as controllers or processors
- The need to ensure that personal data are processed in accordance with a given policy embedded into the seal itself
- The need to certify any deviation from the predefined policy, by means of a breach of the seal

However, fundamental challenges remain. It may be difficult to translate GDPR obligations into technical monitoring. For instance, how to technically monitor the principle of purpose limitation or the principle of data subject rights compliance, and how to apply it to the IoT devices themselves. The complexity of IoT deployments and the heterogeneity of potential legal grounds for data collection tend to require a human intervention in assessing the compliance with the GDPR.

9.5 Dynamic Security and Privacy Seal (DSPS)

ANASTACIA is a European research project, which is precisely researching and exploring hybrid models that combine human-based certification with real-time and automated monitoring. In ANASTACIA, three research partners (Archimede

Solutions, Mandat International and Device Gateway SA) are researching and developing a Dynamic Security and Privacy Seal (DSPS). This DSPS has been specifically designed for IoT deployments.

ANASTACIA developed a comprehensive framework that monitors, detects and counters any identified threats or attacks against an IoT deployment. The ANASTACIA framework provides technical enablers that can monitor complete IoT deployments, including rather large-scale ones. The DSPS model has been developed on top of this core monitoring framework. It takes advantage of the artificial intelligence of the system.

The DSPS has been implemented as a highly secured and authenticated dynamic seal located on an independent server. It provides real-time information in terms of security and data protection status of the monitored IoT deployments.

An important characteristic of the DSPS is its ability to overcome two major hiatuses:

A. The DSPS combines cybersecurity monitoring with personal data protection monitoring. It brings under a common seal the conventional cybersecurity evaluation together with GDPR obligations monitoring. Such approach requires to overcome the usual gap between both sets of requirements.
B. The DSPS combines real-time monitoring technologies with ISO standards and requirements that are designed for conventional human-based audits and assessments. It intends to provide a bridge between both worlds. It complements the work of the auditor and ensures a continuity of monitoring between two audits.

The DSPS is being implemented as a service and is formalised and specified as would be an ISO standard. It has been designed to ease its integration with third-party solutions through open standards and APIs.

9.6 EuroPrivacy Certification Synthesis

The DSPS alone cannot comply with the GDPR requirements. However, its inclusion in formal certification processes is achievable. The EuroPrivacy certification scheme has been designed to overcome most barriers and challenges identified in IoT-related certifications.

9.6.1 Overcoming Cybersecurity: Data Protection Hiatus

EuroPrivacy has been initially developed to address the GDPR requirements. However, through its development, EuroPrivacy has been optimised to work in close complementarity with information security standards such as ISO/IEC 27001.

9.6.2 Addressing IoT Technology Requirements

EuroPrivacy has been specifically developed to enable certification of emerging technologies, including IoT deployments, big data and smart cities. Its architecture enables to customise and adapt the checks and controls to be applied by the auditors. The specific checks and controls for the IoT deployments have been elaborated by group of experts combining data protection and IoT expertise.

9.6.3 Enabling Real-Time Surveillance Integration

EuroPrivacy has been structured to enable real-time monitoring and surveillance integration. While EuroPrivacy complies with the regular ISO requirements, its structure enables a direct integration of real-time monitoring solutions such as the previously described DSP.

9.7 Conclusion

The adoption of the GDPR has deeply triggered the need to develop and provide new certification schemes that can assess the compliance of data protection obligations in the context of IoT deployments. The emergence of real-time monitoring solutions, such as DSSPS, offers encouraging perspectives. However, it appears clearly that simple electronic monitoring alone will not be sufficient to be endorsed by Article 42 of the GDPR. A combination of both formal certification and technology-enabled surveillance seems to constitute the most promising way to move forward.

Coherently with the mentioned research activities, other initiatives have been launched, such as the creation of a European Center for Certification and Privacy (ECCP) based in Luxembourg that is supported by several European partners and is in the process of applying for the accreditation by the local competent supervisory authority, to turn it into an officially accredited certification body qualified for certifying IoT deployments throughout Europe.

Acknowledgments This chapter includes results shared by the European research project ANASTACIA (Grant Agreement N° 731558), which has received funding from the European Union’s Horizon 2020 Research and Innovation Programme and the Swiss State Secretariat for Education, Research and Innovation.

Chapter 10
Voluntary Compliance Commitment Tool for European General Data Protection Regulation

Luca Bolognini, Camilla Bistolfi, and Sébastien Ziegler

10.1 European Data Protection Framework

10.1.1 Data Protection Obligations' Evolution Towards GDPR

When the Privacy Flag project was drafted, in 2014, the General Data Protection Regulation 2016/679 (hereinafter, "GDPR" or "the Regulation")[1] was a mere ongoing proposal of the European Commission, which has been approved in 2016. Organisations and companies located within the EU territory are bound by the European norms and standards, which was not the case for entities based outside of Europe during the effectiveness of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, "the Directive").[2] Following Article 4 of the Directive, there was a concrete risk of gap in terms of privacy protection according to the geographic location of the entity:

> National law applicable
>
> 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>   (a) The processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

[1] http://eur-lex.europa.eu.

[2] Ibid.

L. Bolognini (✉) · C. Bistolfi
Istituto Italiano per la Privacy, Rome, Italy
e-mail: l.bolognini@istitutoprivacy.it

S. Ziegler
Mandat International, Geneva, Switzerland

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_10

(b) The controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law.
(c) The controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

Excluding the case of a European establishment of the controller (Art. 4.1a), this set of provisions demonstrates that only international public law or the location of the equipment would have influenced the applicability of the Directive for non-EU controllers (Arts. 4.1b and 4.1c). European citizens risked to not benefit from a full protection if the company was located outside the EU.

In order to address the complex and sensitive question of personal data transfers outside the EU, complementary rules and mechanisms have been adopted:

- The "Safe Harbour" (now, "Privacy Shield") with the USA.
- The Commission decisions on the adequacy of the protection of personal data in third countries.
- The Binding Corporate Rules ("BCR") adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection.
- The "model clauses", a standard contractual clauses defined by the European Commission in order to offer sufficient safeguards in case of transfers from data controllers to data controllers established outside the EU/EEA and processors established outside the EU/EEA.

GDPR Obligations

Recently, with the GDPR adoption, these conditions have changed though. Article 3 of the Regulation extends the territorial scope of the European data protection norms:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or,
   (b) The monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Even if Articles 3.1 and 3.3 substantially recall the contents of Article 4 of the Directive, following Article 3.2 of the GDPR, it is clear that the conditions for the application of European data protection norms to controllers or processors *not established in the Union* have changed.

The GDPR has extended the geographical scope of personal data protection law to non-EU controllers/processors by focusing on processing activities which involves *the offering of goods or services to data subjects in the Union and/or the monitoring of their behaviour as far as their behaviour takes* place within the Union.

10.1.2 Impact on IoT Data Processors and Controllers

It is to be noted that the European Union has adopted an extensive definition of personal data. For instance, Internet Protocol addresses and MAC addresses are considered as personal data as soon as they are linked to a personal device. In other words, any identifier of an IoT device on the EU territory falls under the authority of the GDPR as soon as it can be attached to a natural person.

Article 28 of the GDPR entails two fundamental obligations:

A. (Art 28.1) "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."
B. (Art 28.3) "Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:…".

This directly impacts IoT service providers who remotely deliver cloud-based services to European customers. This is particularly critical in the eHealth and wearable domain, as well as for connected vehicles. It may also be relevant for manufacturer of IoT devices.

The above-mentioned obligations may lead to limiting the access to the European market for companies that do not comply with them. Moreover, considering the legal and financial risk for companies which would breach the GDPR obligation, all data controllers and data processors have a strong incentive to comply with the regulation. As it was largely publicised, Article 83, paragraph 5 of the GDPR, states that infringements of the core GDPR are subject "to administrative fines up to 2000000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:…"

10.2 Voluntary Compliance Commitment Tool

As explained, with the GDPR, any European data controller must ensure that all its data processors located outside of Europe commit to respect the GDPR provisions before sharing personal data with them. The absence of such demonstration is likely to exclude non-European data processors from an easy access to the European market. The default GDPR framework requires rather complex processes for non-EU-based companies to demonstrate that they will comply with the GDPR.

In order to mitigate this negative effect, Privacy Flag researched and developed a voluntary compliance commitment tool (hereinafter, “VCT”), a mechanism enabling any legal entities located outside the EU, in countries such as Korea, Japan, China and the USA, to voluntarily (and legally) commit to abide to the GDPR obligations regardless of their location.

The VCT aims at providing a voluntary legal binding mechanism for companies located outside of Europe in order for them to signify their legal abidance to the European GDPR obligations regardless of their location. By completing an online process, the VCT enables foreign companies to voluntarily and contractually commit to respect the GDPR obligations. It takes into account the diversity of legal systems regarding the binding value of online contractual process and requirements related to contracts concluded with foreign entities, including US, Japanese, Korean and Chinese ones. The aim was to deliver a mechanism that turns this voluntary commitment effectively binding by giving the contract a legal form that would enable third parties to refer to it in case of non-compliance.

The VCT targets more specifically the data transfer between data controllers and processors based on the EU territory with data processors located outside the EU territory. It leverages sets of standard contractual clauses issued by the European Commission for transfers from data controllers/processors to data controllers/processors established outside the EU/EEA. Moreover, considering the possibility for foreign companies to establish a sub-company inside the EU, the VCT has been defined following the Binding Corporate Rules (BCR) model, intended as a solution for multinational companies which export personal data from the European Economic Area to other group entities located in third countries which do not ensure an adequate level of protection.

The VCT does not constitute a certification in the reading of Article 42 of the GDPR or ISO standards: there is no independent assessment of the compliance of a product, a service or a company with the GDPPR obligations. Nevertheless, it constitutes a relevant and useful complementary data protection mechanism. It demonstrates the will and commitment of a data processor, the contracting party, to abide with the European regulation regardless of its geographic location and main jurisdiction.

The VCT taking into account the content of the model clauses and in accordance with them ensures that the data controller (the company which signs the contract) is committed to a series of obligations that apply also in favour of data subjects. The formal VCT contractual clauses (hereafter, the “Pact”) take over all the basic principles of European personal data protection legislation such as the principle of fairness and lawfulness of the processing, purpose, necessity and proportionality of the personal data, the obligation of the data controller to provide the information, the notification of the data breach, etc.

The tool has been implemented and made available as an online contractual platform at www.privacypact.com. The platform publishes the list of organisations that electronically signed the online VCT contract (the Pact) with legal effects. It includes the details of organisations that signed the Pact, in order to make them visible to the public and recognizable for the subject whose data are processed.

By digitally signing the contract, the Pact is effective for a period of 12 months. The company may renew the Pact after the 12-month period has expired, upon the payment of a small renewal fee. Clearly, in any moment the company can withdraw the contract and it will be removed from the public list.

Additionally, by signing the Pact, the VCT generates a VCT label that can be iFramed in the applicants' websites. The label demonstrates the contractually and legally binding commitment made by the corresponding company.

10.3 Legal Foundation and Impact of the VCT

The VCT constitutes a unilateral commitment that has a valid and binding effect from an international law perspective. It was conceived on the basis of the jurisprudency of the International Court of Justice in the "1974 Nuclear Test" cases. This jurisprudency enshrined in international law the validity of unilateral commitment as a source of obligations towards third parties. In other words, unilateral commitment can generate legally binding rights for third parties that were not part to the declaration.

The VCT leverages the GDPR provisions. Article 40 of the GDPR explicitly allows "controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations" to "make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects" (GDPR Art. 40.3). Article 42 of GDPR states that controllers or processors transferring personal data to third countries can "make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects". The VCT provides a tailored tool to support the implementation of both articles. It constitutes a valid accountability mechanism for supporting and demonstrating an adequate level of data protection provided by controllers or processors for demonstrating compliance with data processing principles.[3]

It is to be noticed that VCT has some similarities with the Privacy Shield system. The EU-US Privacy Shield applies both to data controllers and data processors and is based on a self-certification system by which the US organisation is committed to respect a series of principles in line with European privacy legislation. Interested companies must first sign up to this framework with the US Department of

[3] Article 5.2, GDPR.

Commerce that is responsible for managing and administering the Privacy Shield and companies ensuring that they live up to their commitments. The Privacy Shield system has some similarities with the VCT. Both mechanisms are based on the same logic of voluntary accession by organisations to a disciplinary system of privacy protection based on core of principles drawn from GDPR to provide EU citizens an appropriate level of guarantees. However, the Privacy Shield is based on a bilateral agreement between the European Union and the USA, which provides a sort of "self-certification scheme" that is overviewed by the Department of Commerce. The VCT relies on unilateral commitment by which the entity assumes real legal obligations even if the contract is based on a self-declaration.

An important element is the territorial effect of the VCT. By voluntarily committing to abide to the GDPR principle, a contracting company commits to respect these principles regardless of the location of the data subjects. It can generate additional contractual obligations towards non-European residents, who can refer to the VCT commitment as part of their consent in their local jurisdiction. As the VCT tool keeps a public list of contracting companies, it enables direct identification of entities adhering to the Pact. The VCT has set up a specific body to handle complaints. It hence contributes to establish a trust environment for the European market.

10.4 Conclusion

The two main barriers to IoT market are the technical interoperability and the adopter confidence. The VCT constitutes an innovative approach to extend the applicability of the GDPR principles beyond the EU territory. It enables non-European companies, on a voluntary basis, to commit to comply with the European data protection rules, regardless of their location. In a globalised world, it enables companies to abide to the higher standards in order to avoid any market barrier.

Nowadays, being privacy friendly means increasing the value of a company business. By joining the commitment and signing the Pact, the company demonstrates the attention, awareness and sensitivity to fundamental freedoms and rights concerning the data protection. The tool can contribute to establish a trust environment for non-EU companies in the European market and beyond. It may bring a competitive advantage by increasing the customers' confidence and improving the company reputation. Internally, it can also contribute to increase employee's confidence in company values and missions. The VCT brings benefits to the customers and data subjects. It communicates relevant information to the data subjects on the level of care given to data protection by the data controllers and processors.

More generally, the VCT enables to leverage the data protection level to a high standard that prevent any weak point in globally interconnected IoT deployments.

Chapter 11
IoT Privacy and Security in Smart Cities

Sébastien Ziegler, Mythili Menon, and Pasquale Annichino

11.1 Introduction

While the term "smart city" burst into the scene towards the end of the twentieth century, the technological developments in the IoT domain are accelerating the evolution and development of smart city projects. There is a considerable impetus from national governments and other stakeholders to integrate the latest forms of technologies into the existing urban operations in order to boost their economic, environmental and political development trajectory. Smart cities are expected to improve the overall urban quality of life, to reduce maintenance costs, while creating new job opportunities and a greener economy preserving the environment.

As cities continue to grow inexorably, they need to renew and reinvigorate their core systems including energy, water, construction and environmental sustainability, to meet the rapidly escalating demands of the growing population. By applying information and communication technologies (ICTs) for urban planning, upgrading and operating the city's infrastructure, smart cities have been hailed as an urban development vision capable of integrating ICT solutions to improve the quality of life and enhance urban service efficiency and the overall socio-economic value of the urban ecosystem. The increasing number of IoT products, applications and networks within the smart city domain has propelled the development of standards, APIs and protocols.

In the midst of such momentous development, concerns persist regarding the interoperability and security and privacy associated with sharing of data across existing IoT devices and networks. These issues remain challenging aspects of smart city deployments given the highly fragmented efforts taken thus far in the

S. Ziegler (✉) · M. Menon · P. Annichino
Mandat International, Geneva, Switzerland
e-mail: sziegler@mandint.org

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_11

standardisation arena for smart cities. Moreover, most cities need to cope with their legacy infrastructure. Distinct systems were developed as autonomous silos, using different technologies, guidelines and standards. Thus, despite efforts to develop and deploy integrated solutions, many IoT deployments in smart cities are characterised by a high level of fragmentation within cities themselves. A similar fragmentation and lack of interoperability tend to emerge among cities, which opens the IoT domain to a variety of threats which endanger privacy and security of the data streams.

Considering the above, IoT deployments in smart cities constitute a specific case and are usually characterised by:

- Large-scale and pervasive deployments of IoT devices.
- Use of public space, with physical access to deployed IoT devices by potential hackers.
- Interaction with a large number of individuals, including underage persons, who did not consent to share their personal data.
- Use of legacy communication protocols.
- Fragmentation and lack of interoperability among IoT standards.
- A specific political risk for the democratically elected authorities, which would appear as not respecting the privacy of their citizens.

In such a context, IoT deployments in smart cities must adopt specific strategies to better integrate and secure their heterogeneous IoT deployments, as well as to preserve the privacy and trust of their inhabitants.

11.1.1 Large-Scale Pilot on IoT Deployment for Smart Cities

In order to address these specific requirements, the European Commission has launched and financed a Large-Scale Pilot (LSP) on IoT in smart cities, developed through the Horizon 2020 European research programme. This LSP, named SynchroniCity, is researching and demonstrating the ability of smart cities to better integrate their IoT deployments and to turn their IoT data interoperable for data and application sharing. It has been designed to support and pave the way to a digital single market for IoT-enabled urban services, in Europe and beyond.

SynchroniCity involves 33 partners and 8 core cities in Europe, including Helsinki, Manchester, Milan, Antwerp, Carouge, Eindhoven, Porto and Santander. The project also includes other cities in Mexico, South Korea, the USA and Brazil. It is further supported by the Open and Agile Smart Cities Alliance, which gathers more than a hundred cities.

SynchroniCity has been designed for addressing how to incentivise and build trust for stakeholders (including citizens) to actively participate in the smart city establishment process and deliver common, cocreated IoT-enabled urban services that meet citizen needs in a global market.

Table 11.1 Desirable properties in IoT-enabled smart city services

Properties
Property 1: Interoperability provides cities with the freedom to choose interoperable solutions from multiple vendors that supply the necessary enabling technology layer for smart city operations. This makes use of the new European Interoperability Framework (EIF) and its recommendations as a reference
Property 2: Free competition of vendors and solution providers enables free and thriving competitions among vendors and providers of interoperable IoT infrastructure components within the context of a common reference architecture across different city environments
Property 3: Common service environments promote frictionless portability of IoT-enabled smart city services from one city to another as part of the digital single market. This includes minimising overhead to adapt APIs and to obtain access to equivalent data sources
Property 4: IoT infrastructure reuse could facilitate the easy reutilisation of deployed IoT infrastructures for different IoT services—making multitenancy of IoT devices the norm, not the exception
Property 5: Trusted participation of IoT data providers and consumers ensures that data consumers can trust IoT data providers serving in the different reference zones and vice versa. This includes ways to enforce service agreements between both parties and enable corrective actions if violations occur
Property 6: Incentivise data sharing provides a free market in the different reference zones that offers revenue opportunities for providers of IoT data streams and other urban data sources
Property 7: Common legal foundations provide a common legal environment that provides participating stakeholders with a level playing field across all participating reference zones
Property 8: Increase of competitiveness boosts local economy by creating or maintaining jobs in Europe and participating cities
Property 9: Frictionless innovation lowers barriers for companies to build new and innovative solutions for citizens, organisations and companies within the cities. The DSM should enable and speed up the creation of innovative solutions

SynchroniCity laid the foundation of a reference architecture for IoT in smart cities with identified interoperability points and interfaces and data models. This includes tools for co-creation and integration of legacy platforms and IoT devices for urban services and enablers for data discovery, access and licensing lowering the barriers for participation in the market. The experience derived from SynchroniCity is expected to create an environment of evidence-based solutions that can be easily replicated in other regions of the world.

In line with its aim to create a digital single market for IoT-enabled smart city services, SynchroniCity has identified the following desired properties (Table 11.1).

11.2 IoT Interoperability for Smart Cities

Over the years, the potential success of smart city projects has been inevitably linked to collection and processing of large volumes of data. With the emergence of open data platforms, the establishment of new business models has been triggered to deal with a variety of open challenges and the vast diversity of data sources, including of course IoT data. While aspiring smart cities are a far cry from facing data scarcity, the lack of a common approach and analytical tools to assess the relevance of data still haunts urban stakeholders and deters them from achieving their smart city goals.

SynchroniCity is fostering the adoption of interoperability models by and for smart cities. This strategy is structured around several axes:

(a) Mutualising the experience needs and requirements of partner smart cities

By working on the integration of several smart cities' IoT deployments, SynchroniCity serves as a cornerstone to standardise and structure an open and interoperable data model and API, using the reference architecture being developed within the project. SynchroniCity is expected to assist in the development of a model which not only determines the availability of data but also highlights the criteria that data streams should satisfy to be considered usable.

(b) Leveraging on Open and Agile Smart Cities Alliance (OASC)

The Open and Agile Smart Cities Alliance (OASC) is a city-centric nonprofit organisation, founded in January 2015, with over 114 cities involved. It serves as one of the leading partners of SynchroniCity. The main objective of OASC is to create an open smart city market based on the needs of citizens. As an able stakeholder of SynchroniCity, OASC is also actively involved in developing guidelines for urban systems to make them interoperable between multiple cities and deploy required services. Additionally, OASC provides a platform for cities all over the world to share best practices and experiences while avoiding vendor (and city) lock-in and endorsing the implementation of voluntary international and effective de facto standards. OASC enabled to interact with a larger number of cities to test and validate the model developed by the project.

(c) Developing an open and interoperable API for smart cities

SynchroniCity actively contributed to standardisation effort to create a global standard for IoT in smart cities. It more specifically contributed to the International Telecommunication Union (ITU) work through two channels:

Study Group 20 on Internet of Things and Smart Cities.

Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities.

11.2.1 Open API for IoT in Smart Cities

As the urban ecosystem begins to converge, it requires equally interconnected software applications. In this regard, the use of application programming interfaces (APIs) has largely replaced technologies such as electronic data interchange and custom-written integration programmes for development of new system interactions. Accordingly, APIs have become the "de facto" standard for integrating data and functionality across diverse application ecosystems.

It should be noted that there are two sides to APIs, providing and consuming APIs. Growing numbers of companies consume APIs to access data and functionality exposed by other entities and organisations. A large number of companies are acting as API providers, exposing their systems to those of customers, partners and suppliers. Most participants in the API economy are doing both. Some are also monetising access to data or internal systems as part of revenue generation.

The speed and breadth with which standard-based APIs have proliferated are impacting application performance management (APM) in a big way. Applications relying on APIs to provide data or functions necessary to complete a transaction—an Internet sale, for example—can be slowed or stalled by many of the same factors as tiered, distributed transactions. At the same time, however, APIs are supported by new protocols, connection methodologies and architectures that are largely unsupported by many traditional APM solutions.

Therefore, while APIs are the new standard of B2B and B2C interchange, they also introduce new management challenges that many companies are not equipped to address.

In view of the above and in keeping with the work conducted within SynchroniCity, a work item to develop and standardise an ITU-T Recommendation (international standard) on "API for IoT Open Data in Smart Cities" has been initiated within ITU-T Study Group 20 on IoT and Smart Cities and Communities.

11.3 Reference Architecture for IoT in Smart Cities

The ITU is working on a new reference architecture on IoT for smart cities, which was actively supported and developed by SynchroniCity. This model has been specified by the ITU Focus Group as "Data Processing and Management Functional Architecture".

The reference architecture is simultaneously supporting IoT interoperability as swell as openness and flexibility to prevent technological lock-in situations for smart cities. Recognised frameworks such as FIWARE, UDG and EIP-SCC have been integrated together with the architecture while letting smart cities which one to choose. A common API based on the OASC data model has been adopted and standardised through the ITU. The API provides less complex means to gather, publish, query and subscribe to in-time context information describing what is going on in a city. The information derived through this channel can be updated or accessed by as required for the management of city services. In cases of public availability of information, it can also be collected from third-party applications. The integration with those systems and third-party applications is low cost and is not intrusive. The SynchroniCity API is agnostic to IoT technology used in the smart city and is fully portable and interoperable.

11.3.1 Snapshot of SynchroniCity Architecture: Gateway to the Future of Internet of Things

Setting the Context

An effective smart city architectural framework is an indispensable tool, which can interweave information security and adequate governance processes and ensure the implementation of standards for interoperability. Such a framework will also boost a service-oriented ecosystem within the urban domain. A series of leading smart city projects including Smart Dubai and Smart Nation Singapore have mushroomed across the globe. Even developing countries like India[1] and Sri Lanka have also announced their respective national smart city plans. What plagues majority of the existing smart city ventures is the lack of a credible architecture model which overcomes the burdens of limited interoperability and data management while working on and monitoring set short-term and long-term goals.

As such majority of smart city architectural frameworks exist solely on paper without the scope for their large-scale implementation. The EU Horizon 2020 project SynchroniCity provides the much-required guidance in this realm by creating and proposing a smart city architectural framework which is currently being implemented in various cities across Europe.

A Sneak Peak of SynchroniCity

The SynchroniCity architecture is based on an analysis of the different use cases encountered on the SynchroniCity platform, on the compliance of the reference zones (as known as smart cities), on the reuse of existent approaches in the domains of IoT and smart cities and, finally, on the Open and Agile Smart Cities (OASC) principles. The current architecture of SynchroniCity is as depicted in Fig. 11.1.

What sets SynchroniCity apart from other chain smart city projects is the vision for a single framework for IoT-enabled urban services by overcoming existing technological and socio-economic barriers. Through the project, stakeholders have also been able to derive best practices and recommendations for designing and integrating IoT into existing urban services while encompassing a defined governance metamodel which supports the implementation of such an architecture.

The main components of the SynchroniCity architecture are the following:

- Context data management.
- IoT management.
- Data storage management.
- Marketplace and asset management.
- Security, privacy and governance.
- Monitoring and platform management services.

[1] Smart City Mission-launched under the Ministry of Urban Development, India.

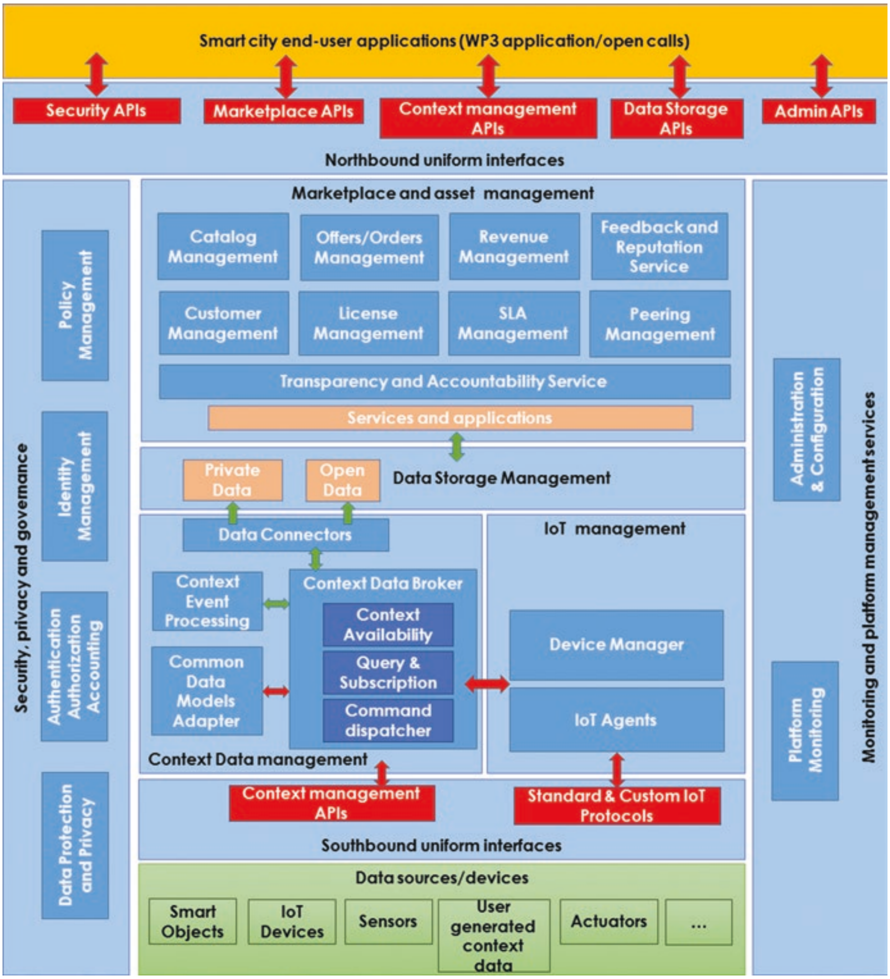


Fig. 11.1 SynchroniCity architecture

The context data management is a kind of middleware handling the information provided by different sources like IoT devices, public resources and private resources. The context data management is composed by several modules: the context data broker, the context event processing, the common data models adapter and the data connector.

The goal of the context data broker is to discover, to collect and to publish information through a standardised interface. The context event processing is able to handle a large number of events, to analyse them and to answer to them. The common data model adapter is responsible for the interoperability by mapping heterogeneous data to a specific well-defined data model. Finally, the data connector enables the storage of the historic data.

The IoT management is composed of different sub-modules presented in this document. First of all, the IoT agent permits to the IoT devices to send their data to the context data broker using their own protocols. Then, the device management is able to configure each IoT agent to ensure a good connection to the IoT devices.

The data storage management is the third main component and enables the storage of all sorts of data (open data, private data and commercial) on different supports (local storage, cloud platforms and databases). Of course, the stored data concern the IoT systems encountered in the smart cities.

The marketplace and asset management are providing goods and services to the smart cities. This module has nine functional sub-modules ensuring the needs of the customers: the catalogue management, the order management, the peering management, the revenue management, the feedback and reputation service, the customer management, the license management, the service-level agreement (SLA) management and, at the end, the transparency and accountability service.

The peering management permits different marketplaces to communicate between each other and so to provide more offers to the customers. The SLA management handles the digital services provided by the marketplace in function of different parameters like the response time and the data loss rate. Afterwards, the transparency and accountability service is responsible of the enforcement of the customer's preferences, notably for the customer's personal data. This service publishes the purposes and the restrictions concerning the collection of IoT data.

The security, the privacy and the governance are managed by the following component. A set of several sub-modules is responsible to ensure the good implementation of different aspects linked to the security and the privacy. The first sub-module is called data protection and privacy; its goal is to guarantee the confidentiality, the integrity and the immutability of the data, notably through data encryption. The second sub-module is in charge of the identity and authentication management. The next one is handling the authorisation and the accounting across the SynchroniCity platform. Finally, the last module called policy management defines the policies used through the SynchroniCity platform.

The last main component is the monitoring and platform management service which ensures the good administration and configuration of the entire platform. Another sub-module is the platform monitoring which permits to observe the SynchroniCity platform through several logs.

In the context of the main components (described above) and in line with the mandate of the SynchroniCity project, stakeholders have envisioned the following key characteristics for an architectural framework such that it helps cities move towards a service-oriented ecosystem using IoT-enabled devices:

- High level of interoperability for existing ICT infrastructures, services and applications.
- Free competition between vendors for application and service provision (thereby creating a digital single market for IoT services).
- IoT infrastructure reuse and common service environments with trusted participation of all parties.

- Sustained and secured data sharing.
- Existence of an adequate legal framework for the deployment of smart city architectures.

The main key elements of the reference architecture utilised within SynchroniCity are common north- and southbound interfaces:

- Northbound alignment: involves a simple, operational and de facto standard pathway for accessing, exchanging and using data streams. This helps create a network of multiple cities with an interoperable framework for information management and processing.
- Southbound alignment: involves the provision of enablers for integrating heterogeneous IoT constituents in the cities participating in SynchroniCity. This alignment also includes the deployment/integration of compliant IoT services, applications and solutions, which helps simplify their adoption.

11.4 Ensuring IoT Data Protection in Smart Cities

With the adoption of the General Data Protection Regulation (GDPR) by the European Union, the data protection became a priority concern. It is not anymore an ethical requirement, but also a source of legal, financial, political and reputational risks.

As in other domains, IoT-related, security and privacy concerns must be addressed by smart cities. They have to integrate and manage diverse IoT deployments and applications while developing adequate strategies to manage the constant flux of innovation and risks brought by IoT solutions. Cities are encouraged to ease the use of collected data through open standards and open data access. This context leads to a certain tension between the two distinct objectives: promoting open access and reuse of data collected by the smart city, while protecting citizens and preventing any leak of personal data. This dual approach has been at the core of the SynchroniCity project.

A data protection policy has been established at the project level in order to:

- Ensure full compliance with the obligations and requirements of the European General Data Protection Regulation (GDPR).
- Proactively protect the data subjects' rights by addressing any identified risk in order to protect and preserve the rights and freedoms of citizens.
- Coordinate the application of key principles, such as personal data minimisation, and privacy by design and by default.
- Research and develop innovative approaches to enhance data protection in smart cities.

The data protection strategy has been structured around three axes:

(a) A dual data protection officer (DPO) organisation and strategy.
(b) A specific data protection impact assessment (DPIA) tool for smart cities.
(c) A privacy application.

11.4.1 Data Protection Officer

The GDPR has forged a new function: the data protection officer (DPO). It is a person designated by a data controller to manage and monitor its compliance with the applicable data protection regulation. Under Article 37 of the GDPR, all public authorities will be required to designate a data protection officer. Moreover, on December 16, 2016, Article 29 WP has published its draft guidelines clarifying the extent to which this role of DPO is connected to the complete implementation of the principle of "accountability".

In SynchroniCity, DPOs play an important role. They are responsible to overview the effective implementation of the data protection regulations. They monitor the collection of data and ensure adherence to relevant and applicable law and data protection standards. In this context, the clarification of the data protection roles and responsibilities, as well as the identification of clear DPOs, is essential.

11.4.2 Dual Data Protection Officer Organisation

SynchroniCity involves several cities, which are free to determine what data should be collected and how they should be processed. Each city is de facto a data controller and must have its own DPO. As a consequence, SynchroniCity had to deal with several city DPOs.

The functions and responsibilities of the city DPOs included inter alia:

- Monitoring GDPR compliance in their city.
- Overviewing personal data collection and processing.
- Performing the data protection impact assessment (DPIA).

In parallel, a certain level of coordination was required at project level. Moreover, the project had to be in a position to answer questions from third parties related to its data protection policy. As a direct consequence, SynchroniCity has also appointed at the project level a Project DPO Coordinator (DPOC) in charge of overviewing and coordinating the work of the various city DPOs.

The coordination was achieved through a Data Protection Committee (DPC) that gathered all the local city DPOs to meet on a regular basis under the chairmanship of the DPOC. The DPC was in charge of:

- Defining the data protection policy at the project level.
- Facilitating the coordination among the different DPOs.
- Serving as a public information and contact point on data protection for the project.
- Handling and reporting any personal data protection issues at project level.

This dual architecture has been a key enabler in developing and adopting collective measures, such as the DPIA and the Privacy Application.

11.5 Data Protection Impact Assessment for Smart Cities

The Article 35 of the GDPR requires that a data protection impact assessment (DPIA) be performed by data controllers in several cases, before collecting any data. The DPIA is compulsory for instance when the data controller intends to adopt new technologies and/or if it intends to monitor large areas of public spaces. In other words, a prior DPIA is compulsory by default for all smart cities located on the EU territory.

The objective of this paragraph is to provide an overview of the DPIA for smart cities that was developed in the context of SynchroniCity. The DPIA has been specifically designed and tailored by the DPCOC (Mandat International) to address the specific needs and potential risks related to IoT deployment in urban environment. The DPIA served as the cornerstone of the privacy by design approach guiding the data controllers' actions.

A DPIA always refers to a formal process established for identifying and evaluating privacy risks, checking privacy legislation and finding solutions to avoid or mitigate these risks. Wright and De Hert [1] defined a DPIA as: "a privacy impact assessment is a methodology for assessing the impacts on privacy of project, policy, program, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts" [1].

11.5.1 DPIA Characteristics

A DPIA process complies with several characteristics that are summarised below:

- **A Privacy by Design Safeguard**
  DPIA has to be intended as a step "to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects", as enshrined by Article 25 of the GPDR on privacy by design and by default. DPIA is therefore a crucial moment to understand data protection implications of the processes, single out risks and identify remedies.
- **A Preliminary and Continuous Process**
  A DPIA should be carried out before any data collection and should be repeated according to the evolution of the IoT deployment. It is a continuous process that should be repeated as often as required. It should start early and continue throughout the development processes.
- **Scalability**
  A DPIA should be scalable enough to encompass the size of the system to be assessed. Every organisation and project is different and has different experience in dealing with privacy. Smart cities usually imply quite large deployments. The scale and scope of the DPIA should thus be appropriate to these circumstances.
- **Accountability**

The ability to demonstrate that a DPIA has been carried out adequately by adopting and implementing the appropriate measures and demonstrating that these measures have been implemented.

- **Transparency and End-User Engagement**
  A minimum level of transparency and objectivity should be ensured by, for example, involving stakeholders, publishing the results, etc. The GDPR formally requires to involve, where applicable, end-users (or entities representatives the end-users) in the DPIA process.

11.5.2 Applicability and Benefits of a DPIA for a Smart City Project

It may be tempting for a smart city to claim that a DPIA is not required when it considers that no personal data are processed. At SynchroniCity project level it was agreed that the implicit aim of the DPIA as specified by the GDPR; the duty to document the data protection measures; and the principle of precaution; all command to check and demonstrate that no personal data are processed and that data subject rights are not at risk. In this context, it was agreed that all cities involved in the project had to perform a DPIA in order to protect the project and the respective local authorities.

There are a number of important benefits when performing a DPIA, namely:

- Preventing costly adjustments in processes or system redesign by mitigating privacy and data protection risks.
- Prevention of discontinuation of a project by early understanding of the major risks.
- Reducing the impact of law enforcement and oversight involvement.
- Improving the quality of personal data (minimisation, accuracy).
- Improving service and operation processes.
- Improving decision-making regarding data protection.
- Raising privacy awareness within the organisation.
- Improving the feasibility of a project.
- Strengthening confidence of consumers, employees or citizens in the way which personal data are processed and privacy is respected.
- Improving communication about privacy and the protection of personal data.

This approach is endorsed by the WP29, which states that "*In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers comply with data protection law*".

For those interested in a more detailed analysis on how DPIA applicability shall be determined, we provide complementary and more detailed information on DPIA applicability at the end of this chapter.

11.5.3 DPIA Methodology and Target of Evaluation

In order to perform a DPIA, some preliminary issues should be tackled. The first one is to understand and describe the target of evaluation of the DPIA. This activity should be carried out by the city's DPO in cooperation with the DPOC and DPC. The DPO should define the objects, services or processes which may need to be assessed, and the DPOC should validate it.

The target of evaluation (ToE) specifies the scope of the evaluation from a data protection standpoint. It may include one or several components of a smart city, like an app, a system of sensors, cameras, an interface, a database, etc. The same applies to smart cities' services, such as a service offered to citizens in the context of an efficient traffic management. As the WP29 points out in the *Guidelines on Data Protection Impact Assessment* (hereinafter "DPIA Guidelines"), "*a single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing*".[2] For example, a group of municipal authorities setting up a similar network of sensors used to monitor the noise on the streets could carry out a single DPIA covering the processing by these separate controllers.

An accurate specification of the ToE is of fundamental importance for the performance of a DPIA, as it is the object thereof. At the beginning of the DPIA report, the person in charge of the DPIA shall accurately determine the ToE and its area of application. This requires to identify, clarify and analyse the data flows. It will usually require to have at least one or several drawings to visualise and analyse all the data flows. On that basis, the legal provisions applicable for the processing of personal data will be determined.[3]

The following relevant questions should be answered for each envisaged ToE:

- Does the ToE qualify as an IT product, an IT-based service or processing operation?
- If the ToE is an IT-based product: Does the product manufacturer qualify as a controller ("controller") or as a processor ("processor") in terms of EU data protection law?
- If the ToE is an IT-based service: Does the service provider qualify as a controller ("controller") or as a processor ("processor") in terms of EU data protection law?
- If the ToE is a set of processing operations: Do these operations present similar risks? Can they be covered by the same DPIA?
- What precisely is the target of evaluation?

[2] Article 29 Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679" p. 6.

[3] EuroPriSe "Criteria for the certification of IT products and IT-based services" [Online]. Available: https://www.european-privacy-seal.eu/EPS-en/Home.

Table 11.2 WP29 DPIA elements

(a)	A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller
(b)	An assessment of the necessity and proportionality of the processing operations in relation to the purposes
(c)	An assessment of the risks to the rights and freedoms of data subjects
(d)	The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the applicable data protection law taking into account the rights and legitimate interests of data subjects and other persons concerned

- What types of personal data are processed when the product or service is used or when the processing operations take place?
- Which groups of data subjects are concerned when the product or service is used (e.g. consumers, citizens, travellers, drivers and employees of the service provider)?
- What data flows occur when the product or service is used?

The DPIA must be led by the respective DPO of each city. The DPO shall have an adequate understanding of the GDPR and data protection law.

Any DPIA process must encompass at least the following four elements (Table 11.2).

SynchroniCity developed a tailored DPIA tool to address the specific needs and risks related to data processing in smart cities. The tool has been made available to the participating cities and iteratively improved and will be made available as a service at the end of the project through a dedicated website (www.dpiaservice.com).

11.5.4 Stakeholders in a Smart City DPIA

When performing a DPIA, it is important to identify all relevant stakeholders that may access and exploit personal data. The following list of stakeholders may be considered when performing a DPIA for a smart city scenario:

- **Cities**: The cities are represented by the governmental body, which is the effective overarching control on the smart city policy in a given city. They control the general purposes and means of data collection, and decide if a smart city will be implemented or abandoned. From a data protection viewpoint, they shall be considered by default as the prime data controllers of personal data processed by the smart city. Yet even when they do not practically process personal data, their role in data protection is critical because they are in the position to determine purposes and means which are later on pursued by the other stakeholders.
- **Citizens**: From a data protection perspective, they are the main data subjects. This category may be further split into two, in order to distinguish between active

citizens (participating in the smart city initiative) and inactive citizens (whose personal data are accidentally or systematically collected by sensors or other data captors without their active engagement).

- **Urban utilities**: Companies providing public services in the cities are key players in making the cities more efficient and sustainable. Either outsourced (public procurement) or just public (belonging to the municipalities), they tend to integrate IoT technology for improving service performance. As such, they become natural data generators (collecting data), data consumers (interacting with other public services in the cities aiming at improving the whole ecosystem) and data providers to third parties. Last but not least, they are also technology consumers.
- **LPWAN operators and service providers**: Operators and service providers play a central role in either generating, collecting and providing data linked to the information interchange (operators) and service provision.
- **Universities**: Academic institutions are often associated with smart cities' projects with various roles, e.g. as scientific coordinators, testbeds managers, etc.
- **App developers**: Users of smart cities' services often have to install third-party applications which enable them to access their data, as stored by the device manufacturer. Installing these applications often consists in providing the app developer with an access to the data through the API.
- **Marketing research and customer segmentation companies**: The great amount of information generated in the context of a smart city may turn very useful for stakeholders specialised in customers' behavioural analysis and segmentation. This can lead to the setting up of databases containing profiled information on data subjects which, in turn, are very useful to derive business intelligence insights. Such information may be collected through smart cities' deployments and processed in an anonymous fashion (e.g. as aggregated data) or in clear mode; in the latter case, personal data protection issues arise and need to be tackled (Fig. 11.2).

With the exclusion of the citizens, from a data protection viewpoint, all the stakeholders listed above may bear the role of data controllers or data processors, depending on what they do with personal data and with what is their degree of autonomy and control over personal data processing.

As requested by the GDPR, all city DPOs were invited by the DPOC to associate and consult citizens (or independent representatives of citizens) when applying the DPIA process.

More specifically, and where applicable, the DPIA should be led by the DPO and involve the strategic functions, such as:

- Project coordinator(s).
- Legal/compliance officers and other DPOs.
- ICT security officers.
- ICT engineers involved in the design of the smart city solutions to be assessed.
- Procurement staff.
- Senior management of the entities associated with the project.

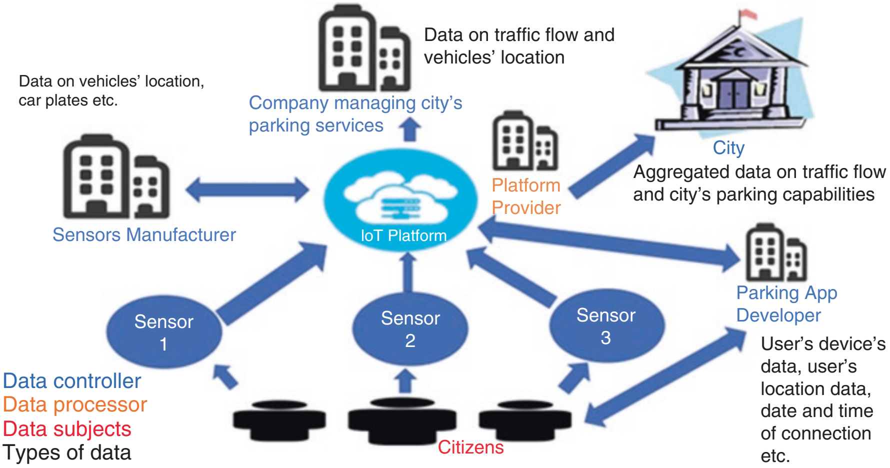

Data on traffic flow and vehicles' location
Company managing city's parking services
Data on vehicles' location, car plates etc.
Sensors Manufacturer
IoT Platform
Platform Provider
City
Aggregated data on traffic flow and city's parking capabilities
Parking App Developer
Sensor 1
Sensor 2
Sensor 3
User's device's data, user's location data, date and time of connection etc.
Data controller
Data processor
Data subjects
Types of data
Citizens

Fig. 11.2 Smart city stakeholders

In order to ensure uniformity to the DPIA process, all the activities of the involved stakeholders should be coordinated by the smart city DPO who should lead the process and take into account all the stakeholders involved in the data processing of the smart cities.

It should also involve the DPOs of each of the entities acting as data processors (or co-controllers) in the smart city project. Any third party that is expected to have access to personal data linked to the ToE should have an appointed DPO. If not, the smart city should ensure that no personal data are shared with such entity.

11.5.5 Outcome of the DPIA

Once the risks and the possible countermeasures to them are identified, the data controller should draw a conclusion and choose one of the following possibilities:

1. *Option 1*: The DPIA results conclude that the risk for data subject is minor and deemed acceptable. An action plan shall be established with attribution of resources, deadlines and responsibilities to the functions called to implement the countermeasures and keep control on the DPIA adequacy over time.
2. *Option 2*: The DPIA results are not deemed acceptable: Whenever the data controller cannot find sufficient measures (i.e. when the residual risks are still high), the DPO shall suspend the project and consult the supervisory authority, as requested by Article 36 GDPR.

It shall be noticed that the DPO will also have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5) GDPR).

Regardless of the output of the DPIA, the DPO must retain a record of the DPIA and will have to update and reiterate the DPIA whenever required by the circumstances. It is recommended to reiterate the DPIA on a yearly basis.

11.6 Privacy App

It is unlikely to easily get a prior informed consent of citizens to get personal data collected in an urban environment. As a consequence, the lawfulness of personal data collection in smart cities usually relies on the public interest and a legal basis. Despite the ability of smart cities to avoid the prior informed consent process, Article 12 of the GDPR requires that data controllers "*take appropriate measures to provide any information (...) relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form*".

Smart cities are particularly complex environments for GDPR implementation, where multiple stakeholders interact and can deploy IoT solutions. Information such as the purpose for data collection and the identity of the data controllers are not easily identifiable. Moreover, the inherent large-scale nature of IoT deployment and public space monitoring is a source of additional risks and obligations.

Beyond the difficulty in acquiring prior informed consent from data subjects in the context of IoT deployments, there are additional key obligations that a data controller should respect. Among those obligations, it is essential to mention not only the obligation to inform data subjects about any personal data processing but also the obligation for the data controllers to ease the exercise of data subject rights.

In this context, SynchroniCity designed and developed a dedicated smart phone application to support GDPR implementation and compliance in the context of smart cities. This application has been named Privacy App[4] and is freely available for both Android and iPhone smart phones in several languages.

The application enables smart cities to share information on all deployed IoT devices. The information is accessible through an interactive map that displays the location of each deployed IoT device. It enables smart cities to inform citizens on each and every IoT device deployed in their city. By simply clicking on one of the IoT icons on the map, citizens access to detailed information, including on the purpose of data collection, the data retention period, the data controller, who can access the data, etc. It also enables data subjects to directly contact the data protection officer of the corresponding data controller.

In parallel, the developed application enables citizens to identify any IoT devices that are not yet listed on the map. The citizen can take a picture and tag any IoT device.

[4] https://www.privacyapp.info/.

A moderator, in principle linked to the municipality, is then invited to complement the information.

Such bidirectional model contributes to empowering and engaging with citizens for the collective control of IoT deployments in public space. Furthermore, it enables municipalities to benefit from a crowdsourcing mechanism to identify any illicit IoT deployment in the public space.

11.7 Conclusion

IoT deployments in smart cities require of course to be secured. Beyond the usual security requirements, the GDPR requires that smart cities apply innovative and adequate measures to comply with the applicable data protection regulations. In the context of SynchroniCity, these requirements have been met by combining three sets of measures:

1. An ad hoc structure bringing together the city DPOs with the DPOC in a DPC in order to coordinate the data protection policy, control and monitoring.
2. A tailored DPIA for smart cities, in order to identify and mitigate any potential risk for data subjects' rights.
3. A dedicated Privacy application for smartphones to inform citizens on the smart city IoT deployment and data processing.

11.8 Complementary Consideration on the Applicability of a DPIA

According to Article 35(1) of the GDPR, "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks". Further in the Article (paragraph 3, letter c), it can be read that "a data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of (…) a systematic monitoring of a publicly accessible area on a large scale".

IoT deployment is based on emerging technologies and usually entails a systematic monitoring of publicly accessible area on a large scale by means of sensors, cameras and other objects. As a consequence, it can be reasonably assumed that DPIA are required by most IoT deployments in smart cities and should be performed before deploying the solution.

The following diagram explains a standard process determining if a DPIA is required (Fig. 11.3).

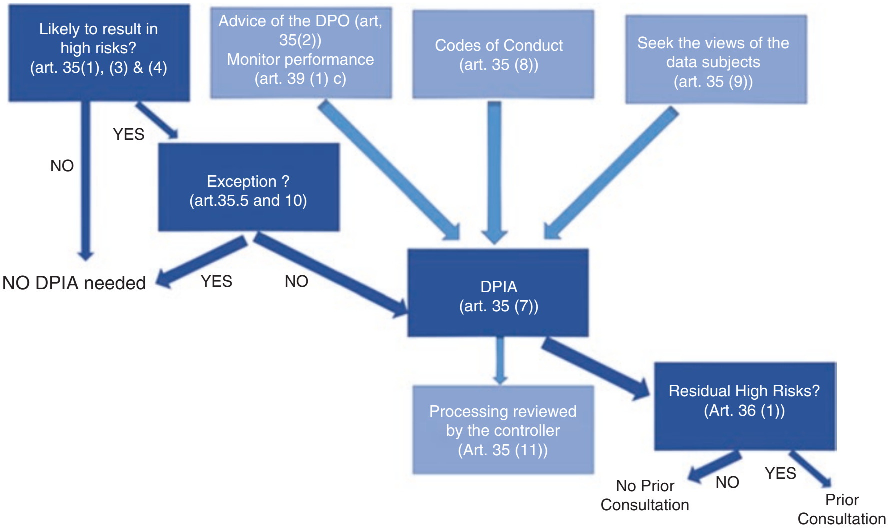

Likely to result in high risks? (art. 35(1), (3) & (4)
Advice of the DPO (art, 35(2)) Monitor performance (art. 39 (1) c)
Codes of Conduct (art. 35 (8))
Seek the views of the data subjects (art. 35 (9))
YES
NO
Exception ? (art.35.5 and 10)
NO DPIA needed
YES
NO
DPIA (art. 35 (7))
Processing reviewed by the controller (Art. 35 (11))
Residual High Risks? (Art. 36 (1))
No Prior Consultation
NO
YES
Prior Consultation

Fig. 11.3 DPIA Diagram, WP29, DPIA Guidelines

11.8.1 Key Criteria in Determining DPIA Applicability

Further to the criterion of a systematic monitoring of a publicly accessible area on a large scale explained above, in appraising whether a DPIA is necessary, the following additional criteria should be considered, as indicated by the WP29.

1. Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" (Recitals 71 and 91 GDPR). Examples of this could include a bank that screens its customers against a credit reference database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.
2. Automated decision-making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion.
3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area" (Article 35(3)(c))13. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects

may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s).

4. Sensitive data: this includes special categories of data as defined in Article 9 (e.g. information about individuals' political opinions), as well as personal data relating to criminal convictions or offences. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data and financial data (that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by a natural person in the course of purely personal or household activity (such as cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be perceived as very intrusive.
5. Data processed on a large scale: the GDPR does not define what constitutes large scale, though Recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

   (a) The number of data subjects concerned, either as a specific number or as a proportion of the relevant population.
   (b) The volume of data and/or the range of different data items being processed.
   (c) The duration, or permanence, of the data processing activity.
   (d) The geographical extent of the processing activity.

6. Datasets that have been matched or combined, for example, originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
7. Data concerning vulnerable data subjects (Recital 75 GDPR): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. For example, employees would often meet serious difficulties to oppose to the processing performed by their employer, when it is linked to human resource management. Similarly, children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns more vulnerable segment of the population requiring special protection, such as the

mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

8. Innovative use or applying technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and Recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy and therefore require a DPIA.
9. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and Recital 91 GDPR). This includes processings performed in a public area that people passing by cannot avoid or processings that aim at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.
10. The WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects and therefore to require a DPIA. As a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA due to the lower level of risk, and processing operations which meet at least two of these criteria will require a DPIA.

11.8.2 Exemptions to the DPIA Obligation

Two main exceptions to the obligation to conduct a DPIA can be identified:

1. The first of these is set forth by Article 35(5), whereby it is stated that "The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board". It shall be therefore checked whether the personal data processing (or sets of processing) entailed by the smart city is covered by one of these lists, once they are drawn up and published. So far, the DPAs of the European Member States have not exercised this prerogative yet.
2. The second exception is likely more relevant for smart cities; it stems from Article 35(10) GDPR which lifts data controllers from the obligation to carry out a DPIA when "the processing has a legal basis in Union law or in the law of the

> Member State to which the controller is subject, and that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis".

Smart cities are very often the result and/or the objective of public policies which may have their foundations in formal acts of legal nature adopted by local, national or European public authorities. When this is the case, the following two conditions must be met in order for the exception to the DPIA to apply:

1. The legal basis for a certain smart city initiative must be provided for by Union or Member State law.
2. The law has been adopted after a data protection impact assessment, as part of a general impact assessment.

This triggers two complementary questions:

A. What Kinds of Acts Can Be Considered Union or Member State Law?
The notion of law must be interpreted widely; it encompasses written and unwritten legal rules which are applicable in a given system (Union or Member State) according to its own constitutional criteria on the production and hierarchy of norms.

As a result, not only legislative acts adopted pursuant to the ordinary or special legislative procedures provided for by the Treaty on the Functioning of the EU ("TFEU") are to be considered Union law but also secondary acts, such as European Commission's delegated or implementing acts can amount to Union law in the reading of Article 35 GDPR.

Similarly, Member State law not only encompasses legislative acts adopted at national level but also secondary laws or administrative rules, such as regulations, circulars, city councils' resolutions as well as regional laws, depending on the definition of law provided for by the domestic legal order. Another factor to be considered is that, pursuant to Recital 45 of the GPDR, "the Regulation does not require a specific law for each individual processing", and therefore one law may contain the legal basis for several data processing.

It shall be verified whether the personal data processing takes place on the basis of a law adopted by the competent Union or Member State authority; the concept of law should be widely interpreted, so as to encompass any enforceable source of rules adopted pursuant to the constitutional framework of the legal system under consideration (i.e. the EU treaties, legislative and non-legislative acts for Union law, national constitutions, ordinary and secondary laws for Member States' law).

B. What Is a General Impact Assessment? And When a Data Protection Impact Assessment Can Be Deemed Performed in the Adoption of a Legal Basis?
An example of what is a general impact assessment for envisaged legislation can be found in the procedure usually followed by the European Commission when appraising the policy options before presenting a legislative proposal. In its impact assessments, the European Commission usually identifies the objectives of the envisaged reform, the issues to be tackled to improve the existing regula-

tory framework and the best policy approach to be undertaken, in the light of the issues to be solved and of the objectives to be achieved.

A data protection impact assessment may be particularly relevant for those legal instruments that set up systems, databases, complex initiatives or procedures which rely on personal data processing. An example thereof is the commission's proposal to revise the EURODAC system database5 which, according to the European Data Protection Supervisor ("EDPS"), should require a prior data protection impact assessment.

From a general reading of the GDPR, it can be inferred that such an assessment, performed at the early stage of the legislative process, is functional to the adoption of rules that embed those data protection elements and safeguards foreseen by Recital 45 of the GDPR, whereby it is set out that "(…) A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association".

This recital is a short manual of privacy-by-designed lawmaking, which presupposes a DPIA beforehand.

In conclusion, it must be ascertained if, in the adoption of Union or Member State law, the competent rule-maker has carried out a data protection impact assessment of that legal basis, also as part of a general impact assessment of the same kind of the ones usually performed by the European Commission. However, even when such assessment is performed while making the law, it is likely to require a review before the entry into operations, as the adopted legal basis may differ from the proposal in ways that affect the impact on privacy and data protection (WP29, DPIA Guidelines).

Reference

1. D. Wright, P. De Hert Privacy Impact Assessment, Volume 6 of Law, Governance and Technology Series, P.523, Springer Science & Business Media, ISBN 9400725434, 9789400725430 (2012)

Chapter 12
End-User Engagement, Protection and Education

Adrian Quesada Rodriguez, Sébastien Ziegler, Christopher Hemmens, Ana Maria Pacheco Huamani, Cesco Reale, Nathalie Stembert, Drew Hemment, Rob Heyman, Jonas Breuer, and Dejan Drajic

12.1 Introduction

In this book, we have discussed many of the technical, technological and legal aspects of protecting ourselves and others from attacks and other illegal activity through interconnected devices and services in the IoT. It's all very well making ourselves the arbiters of best practices when it comes to IoT security, but if we want to accomplish a truly secure IoT network—one that will facilitate new and meaningful interactions across all modern social and economic frameworks—then it is vital that we communicate our findings with society at large and reinforce the importance of the topics already discussed in this book.

Two projects funded by the EU's Horizon 2020 programme have set out to do exactly that. The first is U4IoT, which has brought together experts from across the end-user engagement spectrum and compiled a set of resources complete with workshop templates, crowdsourcing tools, information repositories and an expert pool, among others, that specifically set out to help the people building the next

A. Quesada Rodriguez (✉) · S. Ziegler · C. Hemmens
Mandat International, Geneva, Switzerland
e-mail: aquesada@mandint.org

A. M. Pacheco Huamani · C. Reale
Archimede Solutions, Geneva, Switzerland

N. Stembert
University of Applied Science Rotterdam, Rotterdam, Netherlands

D. Hemment
FutureEverything, Manchester, UK

R. Heyman · J. Breuer
IMEC, Amsterdam, Netherlands

D. Drajic
DunavNET, Novi Sad, Serbia

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_12

generation of IoT technologies to work seamlessly and meaningfully with the people who will ultimately use their products and services. These experts' contribution to this book will hinge directly on their knowledge of end-user engagement and what lengths need to be taken in order to ensure that the topics in the rest of this book regarding security and privacy are adequately communicated to everyday users and citizens.

The second project covered in this chapter, CREATE-IoT, which also supports a number of central EU-funded IoT projects, is more administrative; however, it does include a component directly designed to leverage artwork and artists in engaging society and communities in IoT technology. This aspect highlights ways in which art and artists offer a novel set of strategies and resources to address social and ethical factors of security and privacy in the IoT. CREATE-IoT sets out a framework, tools and resources that others can use in order to facilitate their engagement with artists and communities. The art produced will tend to be more prescriptive and unique to the artists producing the work. These works will communicate the ideas that are central to this book in such a way that individuals will intuitively understand why these topics are so important and why they themselves need to engage with them. We will see that such art interventions can stimulate innovation in IoT technology and also build literacy, attention and, ultimately, trust and acceptance.

This chapter will investigate both the engagement toolkit developed by the U4IoT project and the goal that CREATE-IoT's artwork will ultimately achieve. It will look at what these elements are, how they will be constructed, how they will be used and what the intended result of them will be. Finally, we will look beyond what these aspects are and focus more on what they mean for concepts like ethics and the environment, which are also incredibly important as this new technology finds its way into more homes, workplaces and shared public spaces.

12.2 Methods of Engagement

12.2.1 Online Resources and Toolkits

One of the U4IoT's central goals is to develop and publish a series of online tools that the large-scale pilots of the Horizon 2020 programme will use to involve and engage with the end-users who will ultimately use the services being built by the pilots. These include driverless cars, smart cities, improved healthcare for the elderly and more. To achieve these goals, not only do the tools have to allow someone who is not an expert in end-user engagement to do just that but also have to abide by EU rules on security and privacy. This applies to the entire lifecycle of the pilots, from idea to market.

U4IoT's approach is to develop these tools in direct collaboration with the pilots helping them to build something that will have both broad and specific applications across the IoT spectrum. By undergoing a cocreative process in this way, U4IoT is gaining an invaluable understanding as to what challenges and obstacles we will face as more and more people become exposed to the world of IoT in ways that were unthinkable even 5 years ago. The tools will build upon this information and these experiences to provide a range of nuanced and accessible approaches and methodologies that theoretically anybody working in IoT would be able to take advantage of.

For example, e-courses are a simple and direct way of helping the IoT practitioner to learn about end-user engagement methods and how to (1) define objectives; (2) plan and prepare materials; (3) select, locate and invite participants to workshops or test sessions; (4) select a location/context/platform; (5) monitor, analyse and document results; (6) implement results; and (7) debrief and disseminate results.

End-user engagement strategies can get much deeper including cocreation workshops, living labs, crowdsourcing and other types of meet-up. The U4IoT training programme covers all of these, and their list of methodologies, guidelines and materials can be found on their website.[1]

Although U4IoT is primarily concerned with making sure that the large-scale pilots of the Horizon 2020 programme are best equipped to interact with their end-users, these tools have general use and can be applied in many fields including privacy and security. Given the number of options available, U4IoT designed and published an *interactive flow diagram*. This flow diagram asks a series of questions about where you are in the lifecycle of your project, as well as, for example, what resources you have available, what type of feedback you want (qualitative/quantitative), etc., and provides its best guess at the strategy or methodology that is best suited to your situation; this flow diagram is also available on the U4IoT website.

U4IoT will culminate in the development of an online knowledge base on lessons learned, solutions and user feedback, which will be hosted, along with all the methodologies and strategies listed above, by the IoT Forum, who will also update and maintain it.[2] We will now go into more detail regarding different aspects of the toolkit.

12.3 Crowdsourcing

The *Wisdom of Crowds* has its roots in a 1907 paper by Francis Galton in which, at a fair in the early twentieth century where attendees were invited to guess the weight of an ox, the average of all the attendees' guesses was an accurate estimate for the weight of the ox.[3] This story opened a 2005 book by James Surowiecki in which the author sets out the case that crowds can reach optimal solutions more accurately than a few individuals, no matter their expertise.[4]

[1] http://u4iot.eu.

[2] http://iotforum.org.

[3] Galton, Francis (1907-03-07). "Vox Populi" (PDF). Nature. https://doi.org/10.1038/075450a0. The middlemost estimate expresses the vox populi".

[4] Surowiecki, James. 2005. *The wisdom of crowds*. New York: Anchor Books.

U4IoT is developing a crowdsourcing application for smartphones that will allow the large-scale pilots of the Horizon 2020 programme to tap into this "wisdom" across demographics and locations, combined into single studies using something that most people in the developed world now interact with on a daily basis. Originally created by Mandat International as part of IoT lab, researchers can set up experiments on the crowdsourcing platform; these will then run in the smartphone app, and, when the duration of the experiment is over, the researchers can use the data gathered at their discretion.

It's possible to generate data directly from the phone's sensors, including location, movement and intensity of light, but it's also possible to send willing participants surveys whenever the researcher needs additional information. This is an ideal way to generate feedback from a large and diverse set of individuals, and, because of the restrictions set in place by the EU's GDPR, it is fully compliant with privacy and data protection regulations.[5]

The application runs on iOS, Android and Windows Phone and can be downloaded directly to phones from the relevant stores. Researchers can register on the IoT lab website and control the parameters of the experiment from there.[6]

12.4 Workshops

Traditionally, user-centred design practices were conducted from an "expert perspective". This approach where the user is seen as a "subject" is slowly evolving in an approach in which the user is becoming an expert of his own experiences.[7] Cocreation practices and tools enable end-users to participate as experts and become cocreators of their own solutions.[8]

U4IoT consortium partner, Stembert Design, has developed a Co-Creative Workshop Methodology especially designed for IoT-related contexts. The goal of the methodology is to bring together multidisciplinary participants, e.g. experts, stakeholders and end-users, to cocreate solutions in a couple of hours, with the aim to enable experts to empathise with the needs of stakeholders and end-users, eventually leading to more meaningful IoT-based solutions. Within U4IoT, the Co-Creative Workshop Methodology has been customised to support the large-scale pilots participating in the Horizon 2020 programme.

[5] The EU's General Data Protection Regulation (GDPR) is a sweeping change to privacy and data protection in Europe and is explained in detail in a later section of this chapter.

[6] http://www.iotlab.eu.

[7] Sanders & Stappers, "Co-creation and the new landscapes of design", 2008, CoDesign: International Journal of CoCreation in Design and the Arts, Vol. 4 No. 1, Taylor and Francis.

[8] Sleeswijk Visser, Stappers, Van der Lugt & Sanders, "Contextmapping: experiences from practice", 2005, CoDesign: International Journal of CoCreation in Design and the Arts, Vol. 1 No. 2, Taylor and Francis.

This third iteration of the Co-Creative Workshop Methodology contains materials for five topics corresponding to the context of the pilots: smart cities, smart farming, smart events, smart cars and smart health. The methodology is accompanied by a handbook and the cocreative toolkit, which consists of guidelines, templates, picture cards, actors, objects and sensors. Partners of the pilot projects are enabled to organise, facilitate, analyse and document a Co-Creative Workshop. The handbook describes the guidelines for a cocreative cycle of four phases, co-analysis, codesign, co-evaluation and co-implementation, and includes practical tips on how to organise and run a Co-Creative Workshop.

Particularly in the co-evaluation phase, participants are encouraged to reflect on the cocreated solution based on their own values. Sometimes internal (within the interest of one stakeholder) and/or external (between different stakeholders) value conflicts arise, e.g. between security and privacy.[9] Such conflicts make conscious trade-offs necessary, and discussions among participants can help provide deeper insights and understanding of their views on these matters.

The Co-Creative Workshop Methodology, handbook and toolkit provide all the materials required to create rich, multifaceted and workable solutions to a vast range of complicated problems associated around IoT including those related to security and privacy. During the process of cocreation, needs can be identified from appended explanations, and views can be heard from a diverse range of people.

12.5 Privacy Game

Serious games are being used more and more by companies, institutions and organisations as an excellent tool for raising awareness about important topics. They are used to encourage reflection on a wide range of different subjects such as ecology, migration, racism, homophobia, democracy and others. There is now a vast literature on serious games including a paper offering a precise classification of the medium.[10] The learning objectives are integrated into the games, so the players can learn during the ludic experience.

A serious game about privacy is being developed as part of U4IoT, by Archimede Solutions, and intends to support end-user engagement for the large-scale pilots of the Horizon 2020 programme. The aim is to allow the pilots to learn and understand the key concepts of data protection in the EU, mainly in regard to the GDPR.[11] The game also aims to raise awareness of privacy risks, explain complex legal concepts in simpler terms and increase compliance of the pilots with data protection norms.

[9] Friedman, Batya, et al. "Value sensitive design and information systems." Early engagement and new technologies: Opening up the laboratory. Springer Netherlands, 55–95.

[10] Djaouti, Damien; Alvarez, Julian; Jessel, Jean-Pierre. "Classifying Serious Games: the G/P/S model" (2015).

[11] The details of the GDPR are covered later in this chapter.

Although the initial target users are primarily the large-scale pilots, the game is also suitable for general public and will be made available for general use at the end of the project. The game is conceived to be easily understandable and playable, enjoyable, flexible in its duration from a few minutes to 1 h, playable by a few or many players, playable in teams, cost-reasonable and covering the main aspects of the GDPR and particularly the main concepts of data protection as it applies to the domains of the large-scale pilots.

The main concepts communicated through this game are the key definitions and principles of the GDPR, the main privacy risks for the LSPs and the difference between the different categories of data. In order to create a game that takes into account the described objectives, target users, requirements and key concepts to be communicated, it was decided to create a game involving questions featuring six sections: a general section on EU data protection in the GDPR and one section each on the five pilot projects—smart cities, smart farming, smart events, smart cars and smart health.

The game will allow the players to learn some important concepts about privacy in an easy and funny way and provides a template for other IoT professionals who would be interested in replicating this method for engaging people on topics of IoT.

12.6 Art, Creativity and Public Participation

Although not part of the U4IoT toolkit, art has an important part to play in building engagement around privacy and security. CREATE-IoT, the other CSA in the Horizon 2020 programme, is looking at how art can engage both public and stakeholders alike in IoT innovation.

Art and artists can play a role in bridging the space between technology and society and contributing to technology innovation. There is a history of art and technology innovation coming together going back to the late 1960s and 1970s. Innovation culture in Silicon Valley was shaped by the fusion of arts and engineering, as occurred in artist residencies at Palo Alto Research Centre, Xerox Parc, in the 1970s, with mutual benefits of cultural and technological exchange [1]. There has been a trend since then for organisations to look to artists for new methods of stimulating innovative thinking in product development and institutional practices [02]. Today, the digital or new media art field is represented by organisations and festivals such as Ars Electronica, eyeBeam, FutureEverything, Waag Society, MIT and NTT ICC. In the IoT domain, one of the earliest generalised IoT data platforms, Pachube, was developed by an artist and architect, Usman Haque.

Art interventions can address the challenge of demystifying IoT and build trust in IoT systems. Due to the complexity and novelty of next-generation IoT capabilities, the awareness and acceptance of both stakeholders and the broader public can be low. For acceptance and uptake, the technological capability needs to be expressed in a way that is meaningful to the stakeholder, which is often dependent on the expertise of specialists. The unique skills of artists can make users and the general public more aware of what the IoT is, what it means for them and how it works and can help to identify which technology capabilities are useful for cocreation.

The "art" considered here is not typically paintings on walls. It more commonly takes the form of interactions, interfaces or experiences, often characterised by creative experimentation with data and technology and by an attention to ethical and social consequences of emerging technologies. Every Thing Every Time creates a novel interface to city data, through digital poetry generated in real time from publicly available data and displayed on flipdot displays around a city. A tailor-made data platform gathers various data streams from sensors and data sources. As Manchester's citizens interact with the city, these data streams are turned into an ephemeral, poetic narrative that gives a glimpse into the ubiquity of technology in the urban space.

The creative capacity of artists to give voice to difficult questions, to explore ethical and social implications and to manifest these through public facing artworks means that artists are well equipped to address privacy and security issues. By way of illustration, chattr [03] was an art installation in which spoken conversations which occur in public spaces are recorded, transcribed and published as indelible text on the Internet. The project highlights the gap between attitudes to privacy in digital and physical spaces. It investigates whether a Data Use Policy can be acceptable in exchange for real-world social settings and records the attitudes of people as their spoken word becomes a shareable, mineable dataset uniquely identified as a URL. This work was presented at the FutureEverything and TodaysArt art festivals, creating a highly visible and public debate on privacy and security in IoT and building on methods from art and HCI to generate insights to feed into the development of IoT systems.

12.6.1 Art and Creativity in the European IoT Large-Scale Pilots

The European Commission is promoting the combination of art and ICT as an approach to stimulate innovation and acceptance through STARTS, the Digital Agenda for Europe Initiative for Science, Technology and the Arts (an initiative of DG Connect).

CREATE-IoT is coordinating and supporting the introduction of art and artists in the European IoT large-scale pilots. Central to this is an art/science cluster, made up of artists, projects and intermediary organisations working in the IoT. In CREATE-IoT, two cultural organisations, FutureEverything and Art Share, will work with IoT pilots to support experiments and experiences that can engage large numbers of users and consumers, cocreation workshops for citizens facilitated by artists in real-life consumer environments and participatory demos in a "festival as lab" to explore privacy and security concerns that affect users' experience.

Table 12.1 Open Prototyping framework process model

Stage	Attributes	Value to stakeholders
Scope	Artistic imagination	Domain and problem characterisation
Connect	Connections and exchange	Community links and creative talent
Play	Creative experiments	Creative experiments and artistic user testing
Produce	New IoT interfaces	New expressions, interfaces and experiences
Display	Participation and literacy	Visibility, attention and participation
Interpret	Transparency and trust	Build trust and elicit requirements

CREATE-IoT is promoting artistic practices in IoT pilots and also supporting these by presenting methods that can be used to inject activities involving arts in technology innovation. CREATE-IoT sets out a horizontal cocreation framework for combining art and ICT—the Open Prototyping framework—and makes available tools, resources and artistic works organisations can use to facilitate these art-technology collaborations.

The Open Prototyping framework has been developed by FutureEverything and builds on two decades of research and development in the field. It consists in a six-stage process model, with attributes and common benefits to stakeholders described for each stage (Table 12.1).

12.7 Privacy and Social Care

Naturally, engaging with the public on the subject of IoT does not come down simply to education, instruction and art; indeed, it is also important that the public can trust that this new technology isn't going to infringe upon their right to privacy. By ensuring that these rights are respected, it's possible to gain the trust that will be required to see this new technology rolled out and implemented into everyday society.

In this section, we outline some of the rules and regulations that have been put into force regarding EU citizens' rights to privacy and some of the tools and considerations that come in parallel with that.

12.8 The General Framework: EU GDPR and ePrivacy Directive/Regulation

Personal Data Protection (PDP) has been enshrined in the normative framework of the European Union by a substantial amount of treaties, regulations and directives which have clearly developed its status as a human right for residents of the Union. Among these, two sources are of the highest relevance for the protection of end-users: the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Directive (ePrivacy Directive).

The GDPR: Designed to update the dispositions of the Data Protection Directive (95/46/EC) and to harmonise the approaches to PDP across Europe, the GDPR was adopted in 2016 to be enforceable on 25 May 2018. Among its key features, the GDPR enshrines a number of guiding principles and dispositions that are to be implemented whenever personal data is compiled, stored, processed, disclosed or otherwise handled. Namely, the regulation builds upon the principles of:

- Lawfulness: Processing should take place in the context of express consent by the data subject (or one of the necessity scenarios found in Article 6 of the GDPR).
- Fairness: Processing must account for the protection of children and other vulnerable individuals.
- Transparency: Any information and communication relating to the processing of personal data should be easily accessible, easy to understand and presented using clear and plain language.
- Purpose limitation: Personal data should be collected for specified, explicit and legitimate purposes and not subjected to further processing incompatible with those purposes.
- Data minimisation: Collected data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy: Data are to be kept up to date, and reasonable steps should be taken to ensure the erasure or rectification of inaccurate data.
- Storage limitation: Data must be stored in manners which permit the identification of data subjects only for the minimum necessary timeframes to perform the purposes of collection/processing (longer periods are sometimes possible according to Article 5 of the GDPR).
- Integrity: Technical and organisational measures must be implemented to prevent unauthorised or accidental modification and erasure of personal data.
- Confidentiality: Technical and organisational measures should be implemented to prevent unauthorised or accidental access and disclosure of personal data.
- Accountability: Compliance with these principles and in general with the normative framework that surrounds personal data is the responsibility of the controller, as is the burden to demonstrate compliance.

Based on these principles, the regulation details several elements of key importance to end-users of information society services and, of course, to the potential end-users of the engagement tools and mechanisms addressed by previous sections of this chapter. Chief among these elements are:

- Requirements for consent (Art. 7), protection of underage persons (Art. 8) and processing of special categories of data (Art. 9): The GDPR provides special protections to prevent those situations which might put data subjects (especially vulnerable data subjects, such as minors) at risk in the context of large-scale IoT deployments.[12]

- Facilitation of exercise of the data subject's rights of information (Arts. 13 and 14), access to personal data (Art. 15), rectification (Art. 16) and erasure (Art. 17): The GDPR further strengthens the dispositions of Directive 95/46/EC to require transparent information and communication towards data subjects. This is particularly relevant for IoT deployments for which novel transparency and communication mechanisms must be developed and deployed[13] to ensure all of the end-user's rights are respected by the data controller and processor.
- Regulation of data portability (Art. 20): The increasing popularity of wearable IoT brings forward a giant wave of personal data which is generated at every passing second. Under the GDPR, data subjects are able to request that this data is submitted[14] from one controller to another in an effort to maximise competition and enable user choice.
- Protection of the individual vis-à-vis automated decision-making mechanisms (Art. 22): Potential applications of automated decision-making[15] ranging from the fields of medicine, autonomous vehicles and smart homes showcase how the increasing integration of machine learning and AI with IoT devices also leads to potential breaches of data subjects' rights. The GDPR aims to prevent these clashes by granting data subjects the right to not be subject to decisions which might produce legal effects or similarly affectations unless explicit consent has

[12] Take, for example, the deployment of a smart grid system or the introduction of smart traffic cameras by a city. The GDPR prevents the possibility of inferring racial or ethnic origin, religious beliefs, trade union membership and health/sexual information by cross-referencing the data obtained from traffic cameras with geographical information and expressly prohibits such activities unless express consent has been obtained by the data subject. A similar point could be made from an intrusive deployment of a smart grid, from which religious beliefs and health data could be inferred by examining a household's energy consumption in time vs. the average or (if available) examining the room-by-room energy usage. This problem grows exponentially with big data analytics and the increasing introduction of AI-enabled chips in IoT devices.

[13] Current efforts to maximise communication and transparency between IoT devices and end-users range from the inclusion of printed notices next to the devices to the inclusion of smart tags and Bluetooth beacons to point end-user's smart devices towards relevant websites and even efforts to deploy massive, geo-aware augmented reality solutions by which the end-user will be able to immediately contact the data controller and processors.

[14] The exact way this will be implemented is yet unclear, as the immense range of datasets to be shared and the wide variety of standards (both open and closed) that could be used have slowed down the necessary coordination among the industry sectors. On this point it is important to remember that security considerations are also of key importance, as the GDPR requires that all possible risks and affectations to personal data are considered both when data is at rest and when it is being transferred. Finally, cross-border data transfers might raise the difficulty of any data portability request by the end-user if no equivalent protection is given by local legislation and no agreements have been made by the relevant controllers.

[15] See, for example, http://ieeexplore.ieee.org/document/7733572/ and Arun, Thangavelu & Venkatesan; Cognitive Computing for Big Data Systems Over IoT: Frameworks, Tools and Applications; *Volume 14 of Lecture Notes on Data Engineering and Communications Technologies; Springer, 2017*.

been obtained, and it is necessary for the performance of a contract between the data subject and the data subject; or such decision is authorised by law, and sufficient safeguards have been set in place to protect the data subject's rights freedoms and legitimate interests.

- Adoption of data protection by design and by default and requirements to guide data controllers and processors (Arts. 24–31): One of the most significative changes in the GDPR towards ensuring the protection of the data subject is the introduction of privacy and security considerations to the very design of the systems that generate or process personal data (and to require such safeguards to be enabled by default). The adoption of this approach by the companies that design, sell and implement these devices should come as a welcome effort towards ensuring the safety and privacy of the IoT systems which are used by the data subject.[16] This approach should guide the way controllers and processors carry out the specific requirements set by the GDPR, ensuring that organisational and technical mechanisms are in place to guarantee the legality and proportionality of processing activities and ultimately enriching the security and privacy provided by the IoT ecosystem.
- Further regulation of transfers of data to countries outside the European Union and those countries which do not ensure equivalent levels of protection to personal information (Arts. 44–50): IoT devices are usually built and/or maintained by companies located outside the European Union. Furthermore, the data and metadata they generate will often be processed not by a device in direct control of the end-user but by cloud-based middleware or other kinds of remote server which will require cross-border transfer of personal data to perform its functions. The GDPR (and the ePrivacy Regulation, as will be examined below) aims to address this problem by introducing stronger requirements to such data transfers.

While most of these requirements are fundamentally organisational in nature (as they pertain chiefly to the organisational structure and data management capabilities of personal data controllers and processors), they are intrinsically related (and sometimes explicitly so, as in the case of Articles 24–31) to the introduction of strong security measures. In this regard, the GDPR closes the traditional divide between privacy and security and serves to enhance user's rights through the incorporation of not only a privacy and privacy by design and by default approach but also by expressly introducing some security considerations and practices to the legal framework of personal data protection and, most importantly, to the rights available to the end-user.

[16] For an example on how the privacy by design approach should be considered by IoT applications, see the case of smart health in https://www.sciencedirect.com/science/article/pii/S1877050917317398.

12.8.1 The ePrivacy Directive and the Upcoming ePrivacy Regulation

Best known for expressly regulating the use of Cookies and other tracking devices[17] in IT systems, the ePrivacy Directive [05] complimented Directive 95/46/EC as it was aimed fundamentally at maximising the protection of the rights of end-users of the electronic communication sector. As such, it included express dispositions on the security requirements to be implemented from a technical and organisational point of view by providers of publicly available electronic communications services; confidentiality of communications[18]; protection of traffic data; billing, call identification and restriction; protection of location data; subscriber directories; and unsolicited communications.

The dispositions made by the ePrivacy Directive are currently being reviewed as it will soon be replaced by a new ePrivacy Regulation. The latest proposal version available to the public shows that the new Regulation will be aimed towards particularising and complimenting the dispositions of the GDPR: "the e-Privacy proposal is a lex specialis to the GDPR as regards electronic communications data that are personal data. The e-privacy also seeks to ensure and protect the right to the confidentiality of communications enshrined in Article 7 of the Charter and Article 8 of the European Convention of Human Rights" ([04], p. 91).

The regulation presents significant updates vis-à-vis the ePrivacy Directive and reflects not only the many ways in which technology has evolved but also to respond flexibly to the needs of the industry while safeguarding end-user rights. For IoT end-users,[19] the Regulation will ultimately grant a more granular level of control over

[17] As it declares, starting from its Recital 24 that "Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users" (European Parliament & European Council 2009) and require that any programme installed on such equipment to be based on legitimate purposes. This is further expanded by Recital 25, which states that these legitimate purposes include the provision of information society services, and as such "their use should be allowed on condition that users are provided with clear and precise information (…) so as to ensure that users are made aware of information being placed on the terminal equipment they are using" (European Parliament & European Council 2009). Additionally, the recital requires that the user is given the right to refuse and that any information is provided in a user-friendly manner. The contents of these recitals are synthetised and further clarified by Article 5.3 of the directive, which formally introduces these limitations to the applicable body of law of the European Union (in direct connection to the dispositions mentioned in infra note 18).

[18] Confidentiality of the communications was protected by the Directive's Article 5, which required member states to introduce safeguards on their national legislation to "prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned (…) this paragraph shall not prevent technical storage which is necessary for the conveyance of a communication (…)" (European Parliament & European Council 2009).

[19] The ePrivacy Regulation addresses IoT directly. Recital 12 of the latest draft notes that "The use of machine -to-machine services, that is to say services involving an automated transfer of data and information between devices or software- based applications with limited or no human interaction,

their personal data by setting higher conditions to the processing of electronic communications data (Article 6); the storage and erasure of data and metadata (Article 7); the protection of information stored in terminal equipment of end-users and related to or processed by or emitted by such equipment (Article 8); and the information and options for privacy settings to be provided to the end-user (Article 10).

The potential for synergies between the protection granted by the GDPR and the ePrivacy Regulation will lead to exciting developments in the near future. Companies which aim to sell their products and services in the European market will need to better understand these new obligations and interiorise risks to personal data in their management practices. This must ultimately lead to an increase in end-user engagement: they must be made aware of both the possibilities and risks of IoT in order to become empowered in the protection of their rights as envisioned by these new legal frameworks.

12.8.2 Data Protection Impact Assessments

With the General Data Protection Regulation (GDPR) entering into force, new actions will be required by data controllers. These include the creation of data registers and in some cases Data Protection Impact Assessment (DPIA). Both of these require the data controller to understand what is happening to the data. In this context, two issues have surfaced that need to be addressed: a need for more awareness about the regulation itself and awareness about the data that is being processed by the data controller.

To help data controllers understand what is required of them to comply with the regulation, imec-SMIT (a partner in the U4IoT consortium) proposes two successive tools. The first tool is a privacy literacy survey. This is a method to generate knowledge and skills, which enable data controllers to assess the applicability of the regulation to a case and to identify basic challenges. The second is an interdisciplinary mapping tool, which allows to identify issues and to prepare for a DPIA by making the mapping of a system possible that overarches multiple disciplines,

is emerging. While the services provided at the application -layer of such services do normally not qualify as an electronic communications service as defined in the [Directive establishing the European Electronic Communications Code], the transmission services used for the provision of machine -to-machine communications services regularly involves the conveyance of signals via an electronic communications network and, hence, normally constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation, in particular the requirement s relating to the confidentiality of communications, should apply to the transmission of machine- to-machine electronic communications where carried out via an electronic communications service". In accordance with this approach, Article 5(2) of the proposed regulation recognises that "Confidentiality of electronic communications data shall apply to the transmission of machine-to-machine electronic communications where carried out via an electronic communications service".

actors and organisations. As a result, the barriers of those with little GDPR awareness are lowered, without losing an overview of the data itself.

These tools address new technologies and have been developed to deal with abstract systems that are still evolving. Representations of these systems are made tangible enough for actors with different backgrounds (disciplines and expert knowledge) to understand them. They are also easy enough to use for those that are not experts in DPIA or the GDPR. They are highly applicable to the IoT ecosystem, where everyone that collects GDPR-relevant data (both innovators and traditional stakeholders) can benefit. This is the case because firstly, the ecosystem is all about data flows between diverse devices and actors, entailing data collection by default and often as a passive background process that is invisible to end-users; secondly, IoT is a relatively new and immature technology and business ecosystem; thirdly, it is characterised by a diversity of connected objects with little standardisation and organisations and companies with different levels of data protection; fourthly, established underlying structures and governance still lack; and lastly, IoT has massive data flows at the core of its value promise, and leveraging this data will generate the main revenues.

Privacy literacy survey and manual: This tool serves not only to ask multiple choice questions to monitor the knowledge of a data controller or processor as. It also functions as a feedback mechanism for the participant by indicating false and correct answers and explanations of each concept. As such, it serves as a first manual for GDPR dummies to understand basic concepts. It is also helpful in identifying who in an organisation needs to further his or her understanding of the GDPR, also if they are not the data protection officer but still someone with responsibilities related personal data.

At the time of writing, one general GDPR survey[20] was created, and following interim conclusions can be offered. Users find the questions too difficult, which is either seen as frustrating or a good reason to invite experts. Many respondents started reusing the survey as a manual, which signals the demand to have a repository of answers and questions. Those who contributed also suggested we tie the concepts more specifically to the areas they work in. The survey will therefore be extended as questionnaire and manual. A method to adopt the survey to specific domains is being developed. Ideally, a code of conduct will be the result, which becomes tacit in the form of a FAQ (frequently asked questions).[21] Sharing knowledge as a FAQ would also increase the creation of best practices in sectors but also decrease the amount of work each separate organisation has to do.

A method for mapping data flows: This tool relies on a Post-it method that allows people, who may not necessarily understand all GDPR concepts, to map an envisioned or existing system's data flows. It consists of easy-to-follow steps to describe an entire process. Post-its are easy to change and to manipulate visualisa-

[20] $n = 50$ and consisting of civil servants working on smart city projects in European cities as partners of the CITADEL Project. The surveys are ongoingly collected from May 2017 until the time of writing.

[21] In case of X, it is best to do Y according to article Q of the GDPR and our code of conduct.

tions. They decrease the threshold for different parties to contribute to one shared representation of all data flows. This can be challenging when multiple actors work together. The method thus allows to make hidden assumptions and data practices explicit. It is composed of three building blocks: data points describe where data is stored; transmissions describe data that moves between data points, including the medium, how much data is carried over (all, some) and what kind of encryption is used; and data registers are used to provide a more detailed description of each data point, including, for example, nature, owner, location and volume of information of the data holding (e.g. human resources data), format and use of the information (paper or electronic? structured or unstructured?), data elements (e.g. name, physical address, email address), and where it is stored and accessed (in/from which country/countries). Through the application of the method, we have learned that system administrators or technology-minded participants neglect to look at local, analogue or physical copies if we refer to databases instead of data points and that it is safer to refer to data instead of personal data, to ensure that participants include all information regardless of their own definition of personal data.

At the time of writing, this method has been implemented with startups, IoT developers and two smart city projects. We have found that it work best if multiple experts with a responsibility for a part of the system are present, to making simplified assumptions about other parts of the system, covering up important or risky challenges. The mappings were difficult to complete for participants because many held discussions assessing a part of the system from their area of expertise. The mapping is interesting beyond its application as a privacy by design tool. It also works as an object to start discussion of ownership, as an input for privacy statements and as a visualisation or transparency tool for data subjects. Future work is required to further define the fields of different Post-its in a more standardised format.

12.9 Ethics

Whenever the move is made to change or nudge the behaviour of individuals, one must always be careful not to do it in such a way that undermines the interests of said individuals. Within the EU at least, it is widely accepted that high levels of security and privacy are important to citizens, but one cannot simply assume this is the case and thereby force these measures on individuals, even if it is ostensibly for their own benefit.

This is why education is such an important part of introducing new technologies to the population and why everything mentioned in this chapter is important for everything else mentioned in this book. By equipping citizens with the knowledge we think they need to make what we believe are the right measures for protecting themselves as the technology moves forward, we also give them the freedom to evaluate the information on their own terms and make the decisions that best suit their way of life.

Unfortunately, this is not the end of the story. If poor decision-making in regard to security and privacy is taken by certain individuals, this may impinge on the protection of others in society. In such a case, is it more important to dictate what citizens may or may not do on this topic than give them the freedom to make these decisions for themselves? The use of educational tools and resources should theoretically make these problems easier to solve and hopefully lead to new solutions presenting themselves.

On a related subject, it is in all of our interests to ensure that the technology is deployed sustainability and with due respect to the environment. This has less to do with education and more to do with how the technology is deployed; however, it is still in the interest of the citizens to know about and understand the issues that the technology raises and how they can interact with it in order to make sure that the lives of individuals are improved by IoT as much as possible, whether due to the decisions they make themselves or by those made on their behalf, and, in the latter case, that people are sufficiently informed as to why such decisions have been made and what their consequences are.

12.10 Conclusion

Great technology is meaningless unless it is used effectively. IoT's greatest impact will only become manifest if the people who will ultimately be using it—in theory, the world's entire population—know what the technology is, what it's capable of and how to protect themselves when using it.

Proper end-user education is imperative. This chapter has outlined several ways in which this is possible and also discussed issues that come about when dealing directly with large groups of individuals. We have examined diverse options come to generate successful end-user engagement, including straightforward options such as webinars and e-courses, to more interactive options such as games and the use of art. The options explored in this book are but a handful of possibilities; however they demonstrate how engagement can be achieved and what the relevant situations and approaches are when conducting this work. Anyone who wishes to work with large population groups should seriously consider the best ways to communicate and engage with their target audience, including the options presented throughout this chapter.

End-user engagement is a vital aspect of integrating IoT successfully into modern-day societies, and as such, it should not be ignored. When dealing with citizens and non-experts, we cannot assume that what we're doing is the right thing to do without considering the ethics of the technology. IoT is, by design, a pervasive and complex technology. This chapter has addressed ways to introduce technological advancements to diverse audiences while enhancing interactions and meeting acceptable ethical standards. Consideration for the environment and the knock-on effects endemic to the choices that certain individuals make within the IoT ecosystem are also of great relevance to these exercises.

Acknowledgments This chapter includes results shared by the European research project U4IoT (Grant Agreement N° 732078); project CreateIoT (Grant Agreement N° 732929), which has received funding from the European Union's Horizon 2020 Research and Innovation Programme and the Swiss State Secretariat for Education, Research and Innovation.

References

1. Harris, C. (1999). *In Search of Innovation*. Cambridge, MA: MIT Press. ISBN:978-0262082754
2. P.S. Adler, Beyond hacker idiocy: a new community in software development, in *The Firm as a Collaborative Community: Reconstructing Trust in the Knowledge Economy*, ed. by C. Heckscher, P. S. Adler, (Oxford University Press, New York, NY, 2006), pp. 198–259
3. B. Dalton et al., Chatter [art prototype]. FutureEverything 2013 and The Creative Exchange, Manchester, 21–24 March 2003
4. European Parliament & European Council, Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJL 337, 18 Dec 2009, p. 11
5. M. Lauristin, Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010–C8-0009/2017–2017/0003(COD)) Committee on Civil Liberties, Justice and Home Affairs, European Parliament (2017)

Chapter 13
User-Centric Privacy

Antonio Skarmeta, José L. Hernández-Ramos, and Juan A. Martinez

13.1 Introduction

The realisation and deployment of IoT scenarios promises a cross revolution to all areas of our everyday lives. However, the pervasive and ubiquitous nature of the IoT requires multidisciplinary approaches in order to agree on a common understanding of its implications. Specifically, there is a real need to identify the risks associated to a hyperconnected world in terms of security and privacy, since IoT stakeholders will only accept such ecosystem if it is based on secure, trustworthy and privacy-preserving infrastructures [1].

The IoT promotes global interconnectivity through the application of recent wireless communication technologies and pervasive computing, turning things into real smart objects [2]. Therefore, traditional security and privacy enterprise-centric approaches need to be moved to a *user-centric* view, in which people are empowered to govern the disclosure of their devices' data. IoT security and privacy concerns demand for cross and multidisciplinary approaches, which require efforts from different areas in order to bring citizens into the loop. From the security point of view, smart objects will be often deployed in uncontrolled environments where basic security properties must be still ensured. This circumstance requires the adaptation of current security protocols and technologies to operate on devices and networks with resource constraints that can operate in critical scenarios, such as roads or energy infrastructure. From the privacy point of view, the enforcement of data minimisation and purpose limitation is challenging due the scale and nature of IoT scenarios. Indeed, the further application of aggregation and correlation techniques over massive amounts of data will exacerbate this

A. Skarmeta (✉) · J. L. Hernández-Ramos
Universidad de Murcia, Murcia, Spain
e-mail: skarmeta@um.es

J. A. Martinez
Odin Solutions, Murcia, Spain

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3_13

concern, facilitating profiling and tracking tasks. These needs require that security and privacy concerns in IoT are to be addressed by cross and multidisciplinary approaches by taking into account not only technical and technological challenges.

Indeed, from a legal point of view, the IoT requires approaches covering security and privacy needs from different perspectives under the integration of a legal framework to support them. This process is essential in order to introduce citizens in the IoT ecosystem, while their security and privacy are not compromised. Indeed, this has led to the conception of the “Opinion 8/2014 on the Recent Developments on the Internet of Things”,[1] based on the “Data Protection Directive 95/46/EC”,[2] which has regulated the processing of personal data within the EU until the adoption of a new legal framework for data protection, the *General Data Protection Regulation* (GDPR),[3] introduced with the aim to strengthen citizens’ privacy rights, and whose full applicability is scheduled for 2018 (although already in force). Moreover, the *Directive on security of network and information systems* (the NIS Directive, adopted in July 2016[4]) provides legal measures in order to boost the overall level of cybersecurity in the EU. In addition, the Directive 2002/58/EC[5] is intended to regulate privacy aspect in the electronic communications. Such initiatives represent some of the most significant efforts in Europe to enforce basic privacy principles of citizens.

From a technical point of view, the IoT requires holistic security and privacy approaches with a high degree of flexibility to support scenarios with heterogeneous devices (sensors, actuators, gateways or backend servers) interacting among each other, facing the inherent requirements regarding scalability, interoperability and usability throughout the life cycle of the smart object. In this sense, the *Internet Engineering Task Force* (IETF) has established specific working groups (WGs) intended to accommodate widely deployed security and privacy technologies and protocols to the requirements of IoT scenarios. In particular, the *DTLS In Constrained Environments* (DICE) WG[6] was focused on supporting the use of the Datagram Transport Layer Security (DTLS) [3] in environments with constrained devices and networks. Furthermore, the *Authentication and Authorisation for Constrained Environments* (ACE) WG [4] aims to develop authentication and authorisation mechanisms to be integrated on IoT devices. While these initiatives represent a step forward in order to achieve a secure and privacy-aware IoT, it still arises the need to consider comprehensive approaches addressing security and privacy requirements of smart objects under architectural efforts to be independent regarding the underlying technologies.

[1] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/_les/2014/wp223 en.pdf.

[2] http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46 part1 en.pdf.

[3] http://ec.europa.eu/justice/data-protection/reform/index en.htm.

[4] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[5] https://ec.europa.eu/digital-single-market/en/news/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector.

[6] https://datatracker.ietf.org/wg/dice/about/.

This chapter describes part of the work carried out during the *Secure and sMArter ciTIes data management* (SMARTIE) EU project [5], which was focused on creating a distributed framework enabling the sharing of heterogeneous information for the use in smart city applications based on end-to-end security and data owner's privacy requirements. SMARTIE represented an ambitious effort to realise a more secure and privacy-preserving IoT ecosystem, and it complemented the work from other initiatives, such as the *Reliable Smart Secure Internet Of Things For Smart Cities* (ALMANAC) [6], *Resilient and secUre IoT for sMart city applications* (RERUM) [7] and SOCIOTAL EU projects [8]. The SMARTIE framework represents a user-centric IoT platform, which has been conceived to foster secure data sharing among different IoT entities while ensuring citizens' privacy. This platform's architecture is based on the reference architecture (RA) from the IoT-A EU project [9]. From this RA, the SMARTIE's security and privacy requirements for the IoT ecosystem are addressed, through the design and development of an attribute-based access control infrastructure, which integrates a policy-based authorisation approach with the use of advanced cryptographic schemes. Next sections provide a description of some of these user-centric technologies for IoT security and privacy, as well as their integration on the SMARTIE platform as result of the architecture instantiation.

13.2 Mechanisms and Technologies to Empower Users' Consent in the IoT

The realisation of many IoT use cases is based on sharing huge amounts of data that are sent to central data platforms for making decisions accordingly. In this context, empowering users to control how their data are disclosed is a crucial aspect to ensure the deployment of IoT at a broad scale. This is particularly challenging, especially when this information is outsourced, combined with each other, correlated and stored over long periods of time. This section provides a brief description of some of the technologies that have been used for user-centric privacy for IoT last years. In particular, some of them represents the basis for the SMARTIE platform, as described in Sects. 13.3 and 13.4.

13.3 MyData Model

The use of personal data has become a worldwide mainstream business activity in the last years. Its value is such that according to The World Economic Forum, "Personal data is becoming a new economic asset class, a valuable resource for the twenty-first century that will touch all aspect of society" [10]. As a matter of fact, in a survey provided by Accenture where nearly 600 businesses around the world were responding, 79% of them affirmed to collect data directly from individuals (thanks to the customer account, for instance), as well as from connected devices and third-party data suppliers. By contrast, such businesses are usually accompanied with a control loss by the individuals which have little or no knowledge over how data about them and their activities is created or used. In fact, nowadays, individuals grant legal consent to organisations and software applications for the collection and use of their personal data by accepting the terms of the service they use without understanding them or even without reading them due to their length and complexity.

As in real life, in our digital life, individuals should have legal rights and technical tools to manage personal data collected about them. This is an extension to the freedom of thought and expression that we all have as citizens. Moreover, the current protection regulations prevent companies to create innovative services around personal data so they resort to ways to bypass them. In order to solve this situation MyData initiative has been proposed [11], encompassing a framework, principles and a model for a human-centric approach to empower individuals about their personal data management and processing.

The fundamental principles on which the MyData initiative is based are as follows:

1. **Human-centric control and privacy**: Individuals are no longer passive targets, but empowered actors in the management of their personal lives both online and offline.
2. **Usable data**: It is essential that personal data is technically easy to access and use—it is accessible in machine-readable open formats via secure, standardised APIs (application programming interfaces).
3. **Open business environment**: A shared MyData infrastructure enables decentralised management of personal data, improves interoperability, makes it easier for companies to comply with tightening data protection regulations and allows individuals to change service providers without proprietary data lock-ins.

MyData is a progressive approach to personal data management that combines digital human rights and industry need to have access to data. This approach benefits both sides: individuals and companies. For individuals, it provides easy-to-use and comprehensive tools for personal data management and transparency mechanisms that openly show how organisations use their data. For companies, it opens opportunities for new kinds of data-based businesses by facilitating the legal and technical access to pre-existing personal datasets when the individual is willing to give his/her consent. And in addition also for the civil society, it creates the necessary structures, processes and policies for protecting the rights of individuals and fostering the use of personal data in the development of innovative services.

The architecture proposed by the MyData initiative is based on interoperable and standardised MyData accounts. The proposed model allows individuals to control their personal data from a single place in an easy way. Such accounts will be provided by organisations that act as MyData operators, giving also the possibility to individuals to host their own accounts.

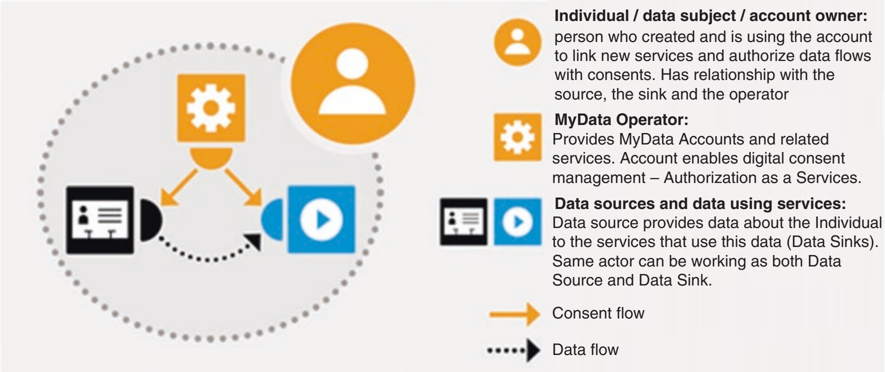

Individual / data subject / account owner:
person who created and is using the account to link new services and authorize data flows with consents. Has relationship with the source, the sink and the operator
MyData Operator:
Provides MyData Accounts and related services. Account enables digital consent management – Authorization as a Services.
Data sources and data using services:
Data source provides data about the Individual to the services that use this data (Data Sinks). Same actor can be working as both Data Source and Data Sink.
Consent flow
Data flow

Fig. 13.1 MyData architecture [11]

The data flows from a data source to a service or application that uses the data. It is worth mentioning that the flow of consents or permissions is separate from the actual flow of data as described in Fig. 13.1. Actually, the primary function of a MyData account is to enable consent management—the data itself is not necessarily streamed through the servers where the MyData account is hosted. Finally, the representation of the consent management can be developed using the open consent meta-format (Kantara Initiative). Such technology offers different advantages for both people and companies, including the following:

1. Knowledge and Control: Consent management (before, during and after).
2. Compliance and Trust: Makes it easy (and cheap) for companies to comply with new laws.
3. Oversight and Management: Provides regulators with flexibility to regulate and enforce regulations according to localised requirements.
4. Improving economic performance of policy solves many issues in identity management.

13.4 eXtensible Access Control Markup Language (XACML)

Over recent decades, a plethora of access control models have been proposed to be used on different Internet scenarios. However, the *role-based access control* (RBAC) [12] and *attribute-based access control* (ABAC) [13] models are probably the most established and deployed. In the case of RBAC, users are associated to roles which, in turn, are bound to specific set of privileges. RBAC also allows users to be members of multiple roles, and consequently, it provides a mapping between users and roles to specify which users are allowed to play which role. Additionally, the flexibility of RBAC allows creating hierarchies of permissions and inheritance, wherein more restrictive permissions override more general permissions. However, several well-known drawbacks have been identified for RBAC model. In particular, mismatches of the set of privileges associated with a role lead to specify more granular roles, which is known as the *role explosion* problem. In order to provide a more fine-grained access mechanism, the ABAC model was proposed in which authorisation decisions are based on attributes that the user has to prove (e.g. age, location, roles, etc.), as well as resources, actions and environmental properties. The main advantage of ABAC is a requesting entity does not need to know a target, providing a higher level of flexibility for open environments. However, while the number of rules can be reduced (compared to RBAC), it leads to more powerful (and complex) rules and more processing and data availability requirements.

RBAC and ABAC are usually deployed by using the *eXtensible Access Control Markup Language* (XACML) [14]. XACML is a standard, declarative and XML-based language to express access control policies, which allows specifying the set of subjects which can perform certain actions on a specific set of resources, based on attributes of them. Under the XACML data model, the definition of access control policies is mainly based on three elements: *PolicySet*, *Policy* and *Rule*. A *PolicySet* may contain other *PolicySets* and *Policies*, whereas a *Policy* includes a set of *Rules*, specifying an *Effect* (*Permit* or *Deny*), as a result of applying that *Rule* for a particular request. The *Target* sections of these elements define the set of attributes from *resources*, *subjects*, *actions* and *environment* to which the *PolicySet*, *Policy* or *Rule* is applicable. Moreover, since different *Rules* might be applicable under a specific request, XACML defines *Combining Algorithms* in order to reconcile multiple decisions. In addition, a set of obligations (*Obligations* class) can be used to notify a set of actions to be performed related to an authorisation decision.

XACML architecture consists mainly of four elements:

- *PEP* (Policy Enforcement Point): it is responsible for performing access control, by making decision requests and enforcing authorisation decisions.
- *PDP* (Policy Decision Point): it evaluates applicable policies and makes authorisation decisions upon receiving access control requests.
- *PAP* (Policy Administration Point): it is used to create a policy or set of policies.
- *PIP* (Policy Information Point): it acts as a source of attribute values.

XACML is a widely used approach for access control and it is an OASIS standard. As described in Sect. 13.3, the main XACML components have been instantiated in the scope of SMARTIE as a main building block for the enforcement of users' privacy preferences.

13.5 Distributed Capability-Based Access Control (DCapBAC)

In IoT, access control has been traditionally proposed through centralised approaches in which a central entity or gateway is responsible for managing the corresponding authorisation mechanisms, allowing or denying requests from external entities. The main motivation behind this approach is alleviate the burden of constrained smart objects, so they delegate security and privacy aspects to more powerful components. However, such solutions come with a cost; the central entity compromises end-to-end security, and it becomes a security and privacy bottleneck for the corresponding scenario. Furthermore, the dynamic nature of IoT scenarios with a potential huge number of devices complicates the trust management with the central entity, affecting scalability. Moreover, access control decisions do not consider contextual conditions which are locally sensed by end devices when access is requested.

In order to address these challenges, the *Distributed Capability-based Access Control* (DCapBAC) [15] represents a lightweight and flexible access control approach to be deployed on IoT environments with heterogeneous devices and networks. DCapBAC is based on SPKI Certificate Theory [16] by linking access privileges to the public key of the smart object or user. The key element of this approach is the concept of capability that represents a "token, ticket, or key that gives the possessor permission to access an entity or object in a computer system". In particular, DCapBAC tokens comprise a set of access rights (as <action, resource> pairs), which are bound to the public key by following a semantics similar to JSON Web Tokens (JWT) [17]. Additionally, the token provides a simple semantics to specify access conditions to be verified locally by the smart object being accessed. These conditions have been used for the specification of a threshold trust value, as part of the IoT trust and reputation model proposed in [18]. Moreover, unlike OAuth that has defined a profile with User-Managed Access (UMA) [19] to specify how resource owners can control the access to their resources, DCapBAC has been integrated with the well-known and established XACML standard (OASIS) for defining access control policies, in order to automate the token generation process. In addition, DCapBAC has been extended for privacy preservation purposes [20] by considering the Identity Mixer (Idemix) technology [21], in order to prove the possession of the DCapBAC token, while privacy can be still preserved.

13.5.1 DCapBAC Basic Scenario

In order to illustrate the use of DCapBAC, Fig. 13.2 shows a basic interaction scenario. In this case, the Resource Owner (RO) delegates her access privileges to a Client (C) entity (acting as a data consumer) to perform an action over a resource being hosted by the Resource Server (RS) (acting as a data producer). It is assumed that the RO already maintains the C's public key, and the RS has the RO's public key. Therefore, the RO issues a DCapBAC token to C in order to delegate her privileges. The token includes time restrictions that specify its validity period, the RO's signature, the C's public key as well as a set of pairs <action, resource> indicating the access rights that are given to the corresponding client.

Then, after receiving the token, C tries to perform a certain action over a specific resource within the RS by using the token. In this case, the RS checks the time restrictions, if the requested action is included in the token, and it validates the RO's signature by using its public key. Furthermore, the RS uses the C's public key

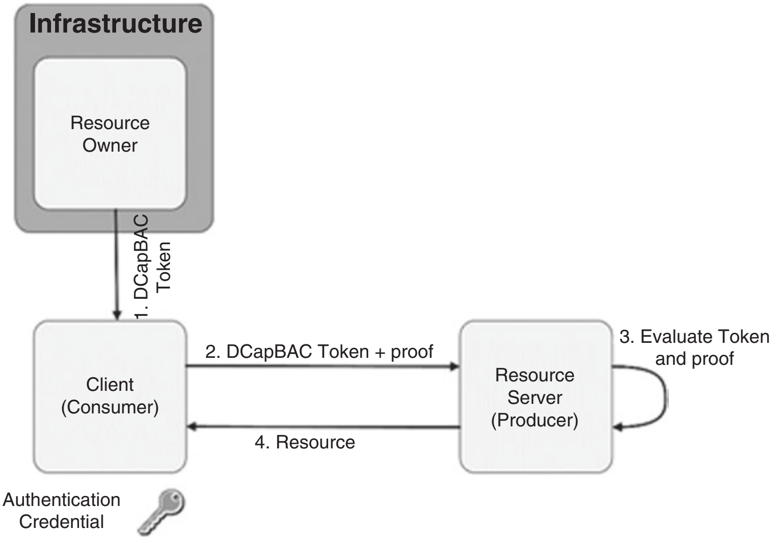


Fig. 13.2 DCapBAC basic scenario

that is included in the token to verify if the requesting entity is the client associated to that token. Towards this end, C makes use of signature algorithms or security protocols such as DTLS in the case of using the Constrained Application Protocol (CoAP) [22].

13.5.2 DCapBAC Extended Scenario

The initial DCapBAC scenario has been extended in the scope of the SMARTIE project with additional infrastructure access control components, in order to automate the token generation process, as part of a so-called entity *Authorisation Service*. This extended scenario is shown in Fig. 13.3.

This way, ROs are enabled to define access control policies through the PAP to govern the generation of DCapBAC tokens, in order to control the access to their resources. In this case, when a client C requests a token to perform a certain action over a resource, it queries the *Capability Manager* entity, which is responsible for generating tokens. Then, this component queries the PDP in order to get an authorisation decision for that request. The PDP uses the policies that were defined by the RO in the PAP, and it evaluates them. In case of a PERMIT result, the Capability Manager generates a DCapBAC token. Upon receiving the token, C can employ the token in the same way as in the previous case.

This extended scenario is used in the SMARTIE approach to enable an attribute-based and lightweight access control solution, and it will be described in next sections.

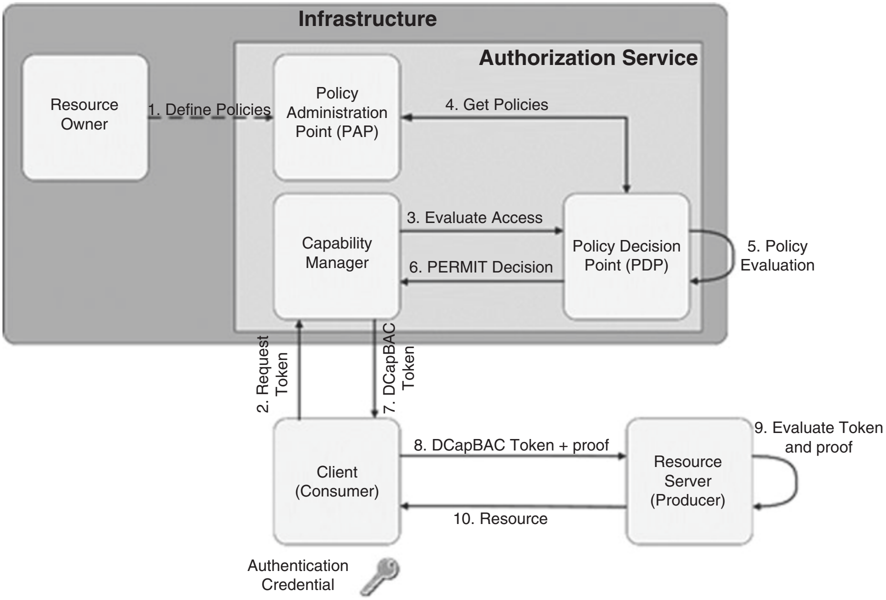


Fig. 13.3 DCapBAC extended scenario

13.6 Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

The requirements presented by common IoT scenarios require more flexible data sharing models between entities, while the privacy of smart objects involved is still preserved. Unlike the current Internet, IoT interaction patterns are often based on short and volatile associations between entities without a previously established trust link. Furthermore, many IoT use cases are based on the sharing huge amounts of data to groups of services and devices through the use of central data management platforms. Indeed, given the scale and dynamism of the envisioned IoT scenarios, it is expected that smart objects often operate as groups of entities, for instance, to accomplish a specific task in a cooperative way. The concept of group is crucial in the IoT to cope with environments with a huge number of smart objects interacting each other, and the application of security mechanisms involving groups of devices with dynamic and ephemeral relationships is a challenging aspect.

Beyond the use of traditional symmetric key cryptography (SKC) and public key cryptography (PKC) approaches as underlying cryptographic schemes, IoT scenarios require more flexible advanced solutions to provide a suitable level of flexibility and scalability. In this direction, *attribute-based encryption* (ABE) [23] represents the generalisation of identity-based encryption, in which the identity of the participants is represented by a set of attributes related to their identity. ABE is gaining attention because of its high level of flexibility and expressiveness, compared to previous schemes. In ABE, a piece of information can be made accessible to a set of entities whose real, probably unknown identity is based on a certain set of attributes. Based on ABE, two alternative approaches were proposed. In the *key-policy attribute-based encryption* (KP-ABE) [24], a ciphertext is encrypted under a set or list of attributes, while private keys of participants are associated with combinations or policies of attributes. In this case, a data producer has limited control over which entities can decrypt the content, being forced to rely on the AA entity issues appropriate keys for getting access to disseminated information. In contrast, in the *ciphertext-policy attribute-based encryption* (CP-ABE) scheme [25], a ciphertext is encrypted under a policy of attributes, while keys of participants are associated with sets of attributes. Thus, only smart objects with a CP-ABE key satisfying such combination will be able to decrypt the information. This cryptographic scheme provides significant features and a noteworthy potential to be exploited in IoT environments. On the one hand, a smart object, acting as a data producer, can decide how its information is disseminated to other entities by encrypting each piece of information with a different combination of identity attributes. Indeed, unlike the use of symmetric key cryptography, in which groups of entities must be preconfigured by delivering the same key, a smart object could encrypt each data under a different combination of attributes, allowing the creation of dynamic groups (or subgroups). For example, a smart object could encrypt information so that only the set of objects from the same manufacturer or the same owner could decrypt the information

13.7 Integrating Contextual Data for Dynamic User Consent

Given the pervasive, distributed and dynamic nature of IoT, context should be a first-class security component in order to drive the behaviour of devices. This would allow smart objects to be enabled with context-aware security solutions, in order to make security decisions adaptive to the context in which transactions are performed. At the same time, context information should be managed by taking into account security and privacy considerations. In particular, current IoT devices (e.g. smartphones) can obtain context information from other entities of their surrounding environment, as well as to provide contextual data to other smart objects. Additionally, trust and reputation mechanisms should be employed to assess the trustworthiness of data being provided by other entities in the environment. In this way, smart objects can discard information that comes from less reliable devices. Moreover, high-level context information can be reasoned and inferred by considering privacy concerns. Thus, a smartphone could be configured to provide information about a person's location with less granularity (e.g. giving the name of the city where he is, but not the GPS coordinates) or every long periods of time in order to avoid that daily habits of a person could be inferred by other entities.

In order to make security adaptive to context, the CPaaS.io project[7] is currently intended to provide a platform to enable users and smart objects to share information by maintaining different interacting entities to be uncoupled. In this sense, the resulting platform will be used for secure exchange of contextual data, so users and smart objects could adapt their security and privacy behaviour according to it. For example, this information could be used by an *identity management* component, which is intended to manage the identities of users and smart objects in an (optionally) privacy-preserving way by disclosing a subset of their identity attributes. Towards this end, a repository of privacy rules can be used to define privacy preferences of users for a proper selection of their partial identities based on their current context conditions (e.g. time, location). An example privacy policy could be "IF contextA=atWork AND contextB=workinghours, THEN partialIdentity=seniorRes earcher", specifying a single attribute to be used for transactions carried out under those context conditions. The evaluation of these rules could be used, in turn, by high-level graphical applications that can facilitate users to manage their partial identities under different contextual conditions. It should be pointed out that privacy policy of a user or smart object could select a different partial identity to the identity that is required by platform services. In order to solve this conflicting situation, an identity negotiation process could be considered, in the case the service requires more identity attributes from the user than he wants to disclose in the current situation. In this regard, a comparison from the service's and user's privacy policy could be used in order to suggest the best partial identity to be adopted.

In addition to identity management, authorisation functionality could be also based on contextual information. Indeed, for a more fine-grained authorisation mechanism in the IoT, contextual information is a key aspect to be considered when making access control decisions. In the same way that contextual information can be considered for partial identities selection, this component is expected to be deployed into services or devices, in order to drive the access control logic to protect resources being accessed. In this way, capability tokens could contain contextual conditions to be enforced by the service being accessed (e.g. related to current time or location). Therefore, when a user tries to get access to a resource being hosted in the service, the token could include restrictions related to the context (e.g. "IF distance < 1 m") to be locally verified when the token is evaluated by the target device.

As already mentioned, in IoT, there will be common situations in which information needs to be outsourced or shared through the use of a central data management platform to groups of smart objects or users. For these scenarios, an approach based on advanced cryptographic schemes, such as CP-ABE, could be key to guarantee security properties when this data needs to be shared with groups entities. In this case, the high-level context information could be used to select a specific CP-ABE policy to encrypt a certain piece of data. In particular, this component could contain a set of *sharing policies* specifying how the information should be disseminated according to contextual data. These policies are intended to be evaluated before information is disseminated by the smart objects. The result of the evaluation of

[7] https://cpaas.bfh.ch/.

these policies could be, in turn, a CP-ABE policy indicating the set of entities which will be enabled to decrypt the information to be shared. An example sharing policy could be "IF contextA=atPub AND data=myLocation, THEN CP-ABE policy=myfriends OR myfamily", specifying the location of a user is shared with friends or family members when he is at a pub. According to it, when a policy is successfully evaluated, the resulting CP-ABE policy is used to encrypt the information to be shared. In the case of two or more sharing policies are successfully evaluated, the most restrictive CP-ABE policy could be selected. After the information is encrypted and disseminated, this component of smart objects receiving such data will try to decrypt it with CP-ABE keys related to its identity attributes. It should be noted that the use of such approach could be integrated into end devices (e.g. smartphones) that will share their data with other users through the platform. At the same time, such approach could be included into the platform, in case other devices (e.g. sensors) are not able to deploy this mechanism.

13.8 SMARTIE: User-Centric Security and Privacy for the IoT

13.8.1 Security and Privacy Requirements for a User-Centric IoT

Under a data-driven IoT, there is a real need for user-centric security and privacy mechanisms that are able to reach consensus among different actors, while the benefits from IoT are still realised. On the one hand, the integration of physical devices into the Internet infrastructure makes them vulnerable to attack and abuse. This is particularly challenging, since these devices will be often physically deployed in uncontrolled environments. On the other hand, the need to manage critical infrastructures and services in smart cities is based on huge amounts of data from individual users, in order to adopt effective decisions to make future cities more efficient and sustainable.

Indeed, for the deployment of innovative and valuable services in smart cities, there is a real need to collect sensitive information from citizens, such as data to help for modelling their daily habits, usual locations (e.g. workplace and home) and scheduled activities. It is also necessary to allow remote control of public infrastructure and even citizens' personal devices. In this "big brother" and automated environment, the risk and impact of security threats can have serious consequences to the community. Data collected in a smart city must be protected in order to reduce the risk of data theft and leakage, which can lead to identity fraud, financial damage and invasion of privacy. The city's infrastructures and IoT devices must also be protected from malicious attacks that may waste the energy resources of the city (e.g. controlling the water and energy management of the city) or even cause physical injuries to citizens by causing accidents (e.g. taking control on the city's lights) or panic (e.g. showing fake alerts about dangerous contamination).

The SMARTIE platform is aimed to ensure security and privacy, which are essential for the success of smart city solutions and for their acceptance by the citizens. As described below, this platform's architecture has been derived from a reference framework. This architecture was designed to ensure fundamental principles of information security such as confidentiality, integrity, access control and availability for the different aspects of a smart city. In particular, confidentiality is needed to protect the privacy of citizens and valuable information of stakeholders in the city, thereby protecting against unauthorised external access. Integrity protects data against modifications that can lead to harmful decisions, and hence it helps on unauthorised device control, hacking and sabotage. Confidentiality and access control are also key aspects for smart cities' platforms to prevent denial of service, man-in-the-middle and intrusion attacks. Data confidentiality in databases by cryptographic means is fundamental to avoid private data disclosure to internal adversaries. Furthermore, guaranteeing data availability and control functionality is also essential, especially in hard situations, such as rescue operations for public safety in which coordination tasks are required.

13.8.2 SMARTIE Architecture

The huge range of IoT application domains has led to the specification of different high-level architectures, which are usually tailored to be deployed on specific scenarios. Furthermore, the current landscape of IoT technologies and protocols is still disharmonised and fragmented. These aspects have been identified as a significant barrier for large-scale IoT deployments and, at the same time, as an incentive for the creation of coordinated efforts. In this sense, IoT-A was a large-scale project focused on the design of an architecture reference model (ARM) to be additionally instantiated by other IoT architectures through a set of specific tools and guidelines. ARM is strongly supported by already mentioned initiatives, such as the IEEE P2413 or the initial definition of HLA provided by AIOTI WG03.

The set of results derived from IoT-A embrace a reference model (RM) to promote common understanding at high abstraction level, a reference architecture (RA) to describe essential building blocks and build compliant IoT architectures and a set of best practices/guidelines to help in developing an architecture based on the RA. In particular, the RA provides several views and perspectives focused on different architectural aspects. Among these views, the functional view describes a set of functional components (FC), which are organised into nine functional groups (FG), as well as their responsibilities and interfaces. In particular, the security FG is composed of five functional components: authentication, authorisation, identity management (IdM), key exchange and management (KEM) and trust and reputation (T&R). According to it, Fig. 13.4 shows a simplified view of the SMARTIE architecture based on such functional view, in which some of mentioned technologies in Sect. 13.2 are included as part of the authorisation FC. Further information of the architecture can be found in [26].

13.8.3 SMARTIE Components for Security and Privacy

The SMARTIE project was focused on the definition of different security and privacy mechanisms for IoT-enabled smart cities, in order to foster and ease the exchange of heterogeneous information, while security and privacy are still ensured. To cope with the main security and privacy needs in the IoE paradigm, SMARTIE's approach is based on the instantiation of the producer/consumer vision for smart objects from [27]. Under such approach, a smart object can play the role of data producer or consumer in any time of its life cycle. Specifically, in a common IoT scenario, a smart object (e.g. a sensor) can be considered as a data producer, which generates raw data. Then, these data are sent to a central data platform for additional processing tasks. Once processed, this information is disseminated to groups of users or services acting as data consumers.

This general IoT scenario raises numerous security and privacy issues, which must be addressed by scalable and flexible mechanisms. From the *producer* perspective, there is a real need to protect the access to the platform, so that only legitimate and authorised entities (e.g. sensors) are able to provide information to the platform. Otherwise, a high degree of reliability on the information that is provided by the platform cannot be guaranteed. Towards this end, as already mentioned, this instantiation of SMARTIE's architecture follows the DCapBAC model, in order to provide an efficient

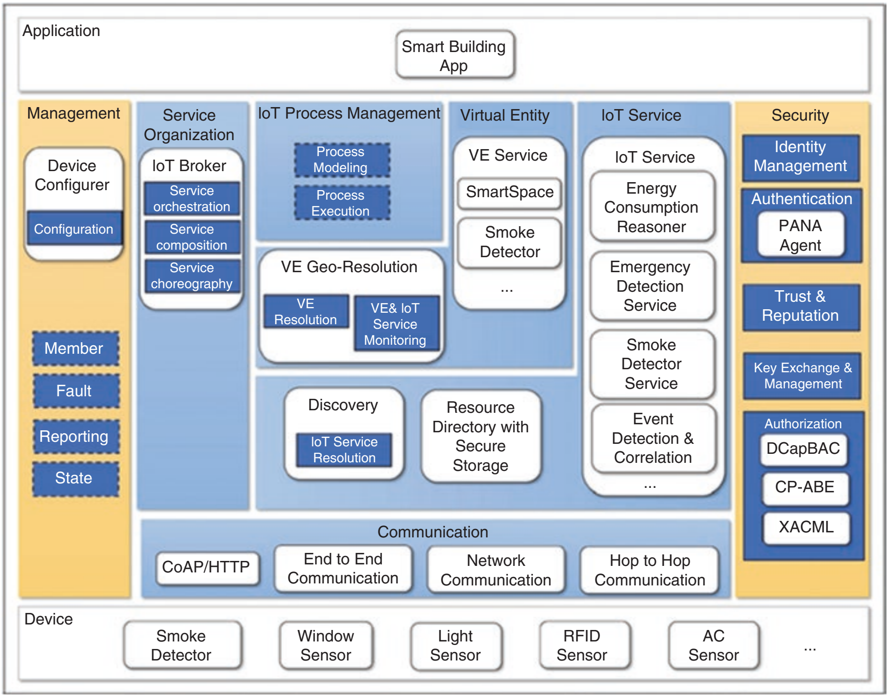


Fig. 13.4 SMARTIE architecture

and lightweight access control mechanism that is used to protect the access to the platform. This technology is based on linking access rights or capabilities to the client's public key. In this way, unlike typical OAuth-based approaches in which the use of a bearer token does not require the bearer to prove that it is actually the entity associated with that token, DCapBAC uses public key cryptography as a proof-of-possession mechanism. Furthermore, it has been integrated with a policy-based access control approach using the XACML standard; so, users or services in charge of the platform are enabled to define proper access control policies for the platform's services. Furthermore, DCapBAC has been integrated with a bootstrapping approach based on the *Protocol for Carrying Authentication for Network Access* (PANA) [28] by defining a simple semantics to provide a mechanism for supporting authorisation credential management procedures [29]. PANA is a protocol widely accepted as a bootstrapping mechanism that is currently used by initiatives, such as ETSI M2M and ZigBee Alliance. In particular, the proposal is based on the extension of the set of PANA AVPs, in order to allow the application and delivery of DCapBAC tokens. For this purpose, two new Action and Resource AVPs have been added to be optionally used by the PANA Client (PaC) to obtain a DCapBAC token. The Resource AVP makes reference to a URI where the resource is hosted (e.g. coap://weatherstation1.umu.es/temperature). Moreover, the Action AVP refers to a possible CoAP method to be performed on that resource (e.g. GET). Therefore, the PANA Agent (PAA) queries the Capability Manager to obtain a capability token for a PaC that is sent within a new AVP called DCapBAC token.

From the *consumer* perspective, there is a real need to ensure only legitimate and authorised users or services are able to access the information provided by smart metres (acting as producers) through the platform. In this sense, SMARTIE makes use of CP-ABE in which each piece of data is encrypted under a certain logical combination (or policy) of identity attributes, whereas a private key is associated with a certain set of attributes. In this way, different services or users will be able to decrypt a certain piece of information sent by a sensor if their key satisfies the policy that was used to encrypt such data. The use of CP-ABE in this case provides two significant advantages. On the one hand, its straightforward application to provide confidentiality in one-to-many configurations, since the group of entities satisfying the policy, will be able to access the information, providing a high level of scalability and adequacy to publish/subscribe scenarios. On the other hand, CP-ABE offers a simplified key management that does not require key refresh or revocation to be able to decrypt data that were encrypted under different policies. Indeed, changing or modifying the CP-ABE policy that is used to encrypt a data does not require new key management tasks.

Below, we provide the description of a specific use case in which these SMARTIE components have been integrated to provide a fine-grained user-managed access control approach.

13.8.4 Applying SMARTIE Components in the Internet of Energy

The considered use case is based on a real scenario at the University of Murcia (UMU) premises. Figure 13.5 shows a high-level diagram representing the scenario. In this case, different sensors, such as luminosity, presence sensors and smoke detectors, are deployed on the building. Furthermore, all the rooms' doors as well as the main entrance door are equipped with RFID readers. The building also has a fire detection system. These devices act as *data producers*, and they are connected to *gateways* by using legacy protocols. Thus, the gateways are in charge of retrieving events from the sensors and communicating with the smart building management service.

As shown in the figure, SMARTIE's components have been instantiated by different deployment elements to realise the described access control functionality into the SMARTIE platform. In this way, according to already mentioned technologies, it should be noted DCapBAC has been enabled through the definition of different components within the SMARTIE platform in order to automate the DCapBAC token generation process. In particular, we have made use of XACML for the implementation of the policy administration point (PAP) and the policy decision point (PDP) components, which have been deployed as web services. In addition, we have added the Capability Manager as the component for generating DCapBAC

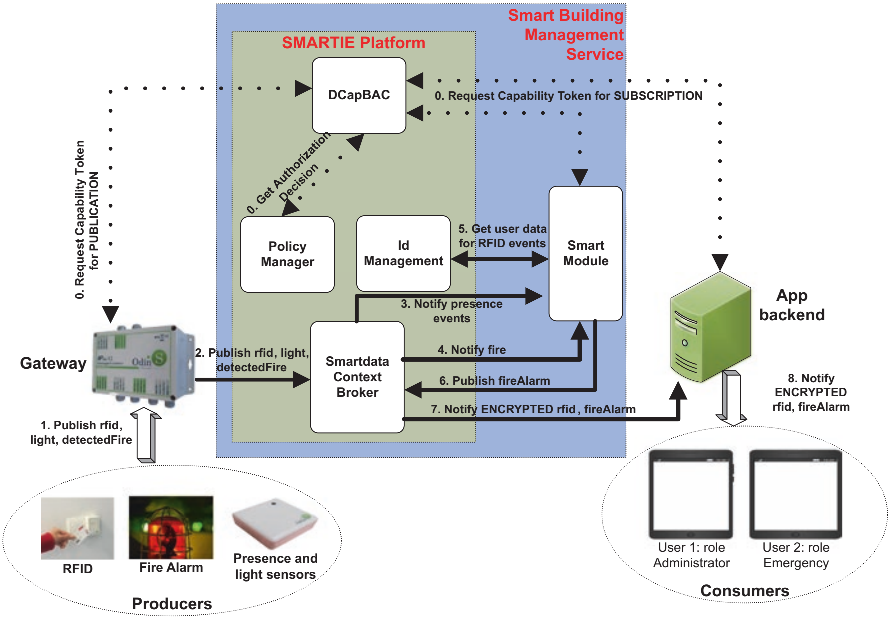

Smart Building Management Service
SMARTIE Platform
DCapBAC
0. Request Capability Token for SUBSCRIPTION
0. Request Capability Token for PUBLICATION
0. Get Authorization Decision
Policy Manager
Id Management
5. Get user data for RFID events
Smart Module
3. Notify presence events
App backend
Gateway
2. Publish rfid, light, detectedFire
Smartdata Context Broker
4. Notify fire
6. Publish fireAlarm
7. Notify ENCRYPTED rfid, fireAlarm
8. Notify ENCRYPTED rfid, fireAlarm
1. Publish rfid, light, detectedFire
RFID
Fire Alarm
Presence and light sensors
Producers
User 1: role Administrator
User 2: role Emergency
Consumers

Fig. 13.5 Instantiation of SMARTIE components in a smart building scenario

tokens in case of receiving affirmative authorisation decisions from the PDP. Furthermore, the IoT broker is intended to provide the functionality of a data broker, in order to allow producers (i.e. sensors and detector) and consumers (i.e. users and applications) to remain decoupled, by following a publish/subscribe communication model. In addition, it has been enriched with CP-ABE functionality, so that received data can be encrypted by using specific CP-ABE policies.

Before describing the main interactions, it should be noted there are different steps that are assumed to be made before the use case. First, we consider a certain empowered user (e.g. the responsible for smart building management service) has already defined a set of access control policies through the PAP, to determine which entities are authorised to publish and subscribe to information on the platform. Second, we assume that CP-ABE policies has been previously defined that will be used to encrypt information from the deployed devices. In addition, it is assumed that users have already obtained the necessary cryptographic material (CP-ABE key and public cryptographic parameters) to try to decrypt the information from the platform.

In this scenario, the building administrator is subscribed to RFID events in order to know this kind of presence in the building. The other user is an emergency manager that is subscribed to fire alarm events. When the user logs in to the mobile application, this application's backend server subscribes to the "fireAlarm" or "RFIDReading" topic at the *Smartdata Context Broker* if the user is emergency manager or building administrator, respectively. For subscriptions and publications in the broker, a DCapBAC token is required from the *Capability Manager* component (which, in turn, queries the *XACML* component) within the SMARTIE platform. Consequently, the gateways obtain a DCapBAC token in order to publish data to the Smartdata Context Broker. When this broker receives an event from these gateways, it notifies the *Smart Module* (that has been previously subscribed to the events associated to the devices). The Smart Module registers all the events that indicate human presence (i.e. luminosity, RFID and presence events) and obtains user information from the *Id Management* in the case of RFID events.

From then on, the backend server will receive notifications related to these two topics and will forward these notifications to the mobile application. When a fire event is detected by the fire detection system, corresponding gateway notifies the Smartdata Context Broker, and the latter sends the notification to the Smart Module. This module generates a fire alarm event that includes the proper location records and posts this event to the Smartdata Context Broker. The broker then forwards the fire alarm event to the user app, which has been previously subscribed to events of this kind. Before forwarding the event, the broker encrypts it based on CP-ABE (the encryption key and attributes for the fire alarm event have been previously configured in an additional entity *Attribute Authority*).

Indeed, the application's users will only be able to decrypt the notifications to which he is authorised because all notifications are encrypted by the CP-ABE component. Thus, the two users will receive information about the above-mentioned topics, that is, "fireAlarm" and "RFIDReading", but they will only be able to access to one kind of notification: "fireAlarm" notifications if the user is an emergency manager and "RFIDReading" if the user is a building manager. This authorisation is implicit, based on attribute-based encryption. The app's backend server is not able to see the notification's data since it cannot decrypt them; it only forwards encrypted notifications to the application. End-to-end confidentiality is therefore ensured between the Smartdata Context Broker and the mobile application.

13.9 Conclusions

Given the scale and ubiquity of the next generation of IoT-enabled scenarios, security and privacy have become a "must". While industry and academia agree on the need of common understanding to cope with these challenges, the fragmented landscape of technologies and protocols make a secure and privacy-aware IoT more difficult to be realised. This chapter has provided insights about some of the most extended technologies that are intended to include the end users and citizens in the loop of IoT security and privacy. Some of these approaches have been proposed in the context of some European IoT initiatives in recent years and integrated with consolidated approaches for access control. While these efforts are focused on some of the main aspects for a more user-centric security and privacy, they are intended to mean a step forward to realise a more trustable IoT ecosystem to be supported by recent legal frameworks in the EU.

Acknowledgment This chapter includes results shared by the European research project CPaaS.io (Grant Agreement N° 723076); IoTCrawler (Grant Agreement N° 779852); and Fed4IoT (Grant Agreement N° 814918), which has received partial funding from the European Commission as well as by the Spanish Ministry of Economy and Competitiveness through the Torres Quevedo program (Grant Agreement N° TQ-15-08073).

References

1. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
2. G. Kortuem, F. Kawsar, V. Sundramoorthy, D. Fitton, Smart objects as building blocks for the internet of things. IEEE Internet Comput. **14**(1), 44–51 (2010)
3. E. Rescorla, N. Modadugu, *Datagram transport layer security version 1.2*. (No. RFC 6347) (2012)
4. L. Seitz, S. Gerdes, G. Selander, M. Mani, S. Kumar, *Use cases for authentication and authorisation in constrained environments* (No. RFC 7744) (2016)
5. J.L. Hernández-Ramos, D.G. Carrillo, A. Skarmeta, F. Gonçalves, L. Cortesão, J.M. Bohli, M. Bauer, SMARTIE: a secure platform for Smart Cities and IoT. Eng. Secure Intern. Things Syst. **2**, 75 (2016)
6. D. Bonino, M.T.D. Alizo, A. Alapetite, T. Gilbert, M. Axling, H. Udsen, et al., Almanac: internet of things for smart cities, in *Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference*, (IEEE, New York, 2015), pp. 309–316
7. H.C. Pöhls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E.Z. Tragos, et al., RERUM: building a reliable IoT upon privacy-and security-enabled smart objects, in *Wireless Communications and Networking Conference Workshops (WCNCW), 2014 IEEE*, (IEEE, New York, 2014), pp. 122–127

8. J.B. Bernabe, I. Elicegui, E. Gandrille, N. Gligoric, A. Gluhak, C. Hennebert, et al., SocIoTal—the development and architecture of a social IoT framework, in *Global internet of things summit (GIoTS), 2017*, (IEEE, New York, 2017), pp. 1–6
9. A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. Van Kranenburg, S. Lange, S. Meissner, *Enabling things to talk* (Springer, Berlin, 2016)
10. T. Cooper, R. LaSalle, Guarding and growing personal data value. *Accenture Institute for High Performance* (2015)
11. A. Poikola, K. Kuikkaniemi, H. Honko, Mydata a nordic model for human-centered personal data management and processing. *Finnish Ministry of Transport and Communications* (2015)
12. D. Ferraiolo, J. Cugini, D.R. Kuhn. Role-based access control (RBAC): features and motivations. In *Proceedings of 11th annual computer security application conference* (1995), pp. 241–248
13. E. Yuan, J. Tong, Attributed based access control (ABAC) for web services, in *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference*, (IEEE, New York, 2005)
14. T. Moses, Extensible access control markup language (xacml) version 2.0. *Oasis Standard, 2005* (2005)
15. J.L. Hernández-Ramos, A.J. Jara, L. Marín, A.F. Skarmeta Gómez, DCapBAC: embedding authorisation logic into smart things through ECC optimisations. Int. J. Comput. Math. **93**(2), 345–366 (2016)
16. C.M. Ellison, B. Frantz, B. Lampson, R. Rivest, B. M. Thomas, T. Ylonen, *SPKI certificate theory* (1999), *RFC2693*
17. M. Jones, J. Bradley, N. Sakimura, *Json web token (jwt)* (No. RFC 7519) (2015)
18. J.B. Bernabe, J.L.H. Ramos, A.F.S. Gomez, TACIoT: multidimensional trust-aware access control system for the Internet of Things. Soft. Comput. **20**(5), 1763–1779 (2016)
19. T. Hardjono, E. Maler, M. Machulak, D. Catalano. User-managed access (uma) profile of oauth 2.0. *Kantara Initiative, Recommendation, 04* (2014)
20. J.L. Hernández-Ramos, J.B. Bernabe, M. Moreno, A.F. Skarmeta, Preserving smart objects privacy through anonymous and accountable access control for a m2m-enabled internet of things. Sensors **15**(7), 15611–15639 (2015)
21. J. Camenisch, E. Van Herreweghen, Design and implementation of the idemix anonymous credential system, in *Proceedings of the 9th ACM conference on Computer and communications security*, (ACM, New York, 2002), pp. 21–30
22. Z. Shelby, K. Hartke, C. Bormann, B. Frank. *The Constrained Application Protocol (CoAP)*(RFC 7252), 2014 (2016)
23. A. Sahai, B. Waters, Fuzzy identity-based encryption. Eur. Secur. **3494**, 457–473 (2005)
24. V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in *Proceedings of the 13th ACM conference on Computer and communications security*, (ACM, New York, 2006), pp. 89–98
25. J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in *Security and Privacy, 2007. SP'07. IEEE Symposium on*, (IEEE, New York, 2007), pp. 321–334
26. SMARTIE. Deliverable 2.3: SMARTIE initial architecture specification, http://www.smartie-project.eu/download/D2.3-Initial%20Architecture%20Specification.pdf
27. J.L. Hernandez-Ramos, J.B. Bernabé, A. Skarmeta, ARMY: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things. IEEE Commun. Mag. **54**(9), 28–35 (2016)
28. D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin. *Protocol for carrying authentication for network access (PANA)* (No. RFC 5191) (2008)
29. J.L. Hernández-Ramos, D.G. Carrillo, R. Marín-López, A.F. Skarmeta, Dynamic security credentials pana-based provisioning for IoT smart objects, in *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum*, (IEEE, New York, 2015), pp. 783–788

Index

S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Internet of Things, https://doi.org/10.1007/978-3-030-04984-3