Internet of Things

Sébastien Ziegler *Editor*

Internet of Things Security and Data Protection

Springer

Internet of Things

Technology, Communications and Computing

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

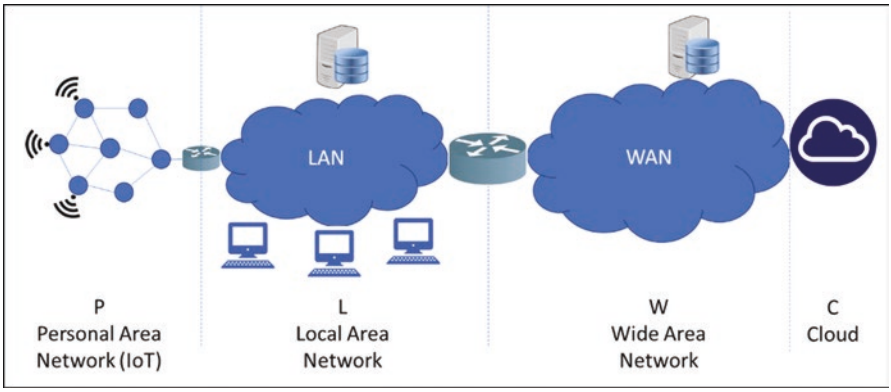

Fig. 1.1 Network segmentation

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.

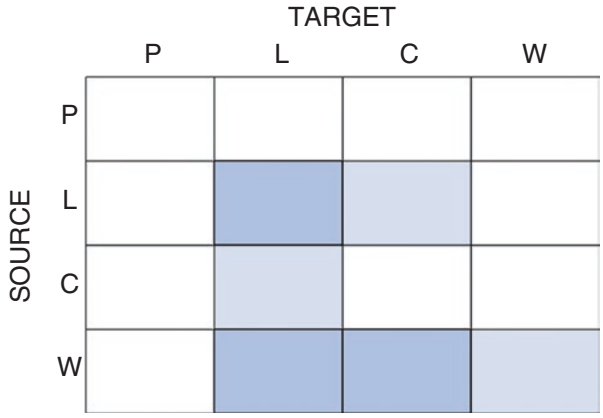

Fig. 1.2 Traditional cybersecurity threat matrix

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

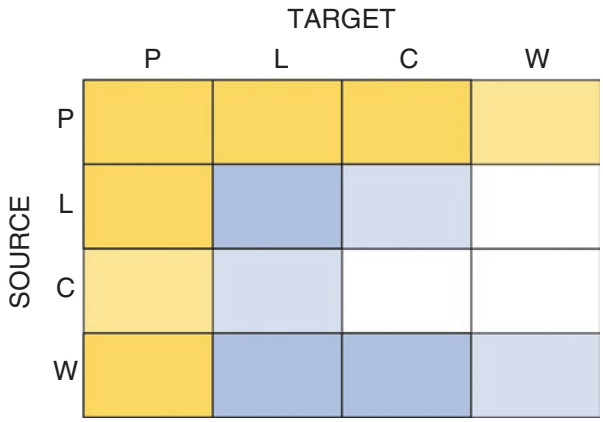

Fig. 1.3 Cybersecurity threat matrix: evolution with the Internet of Things

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

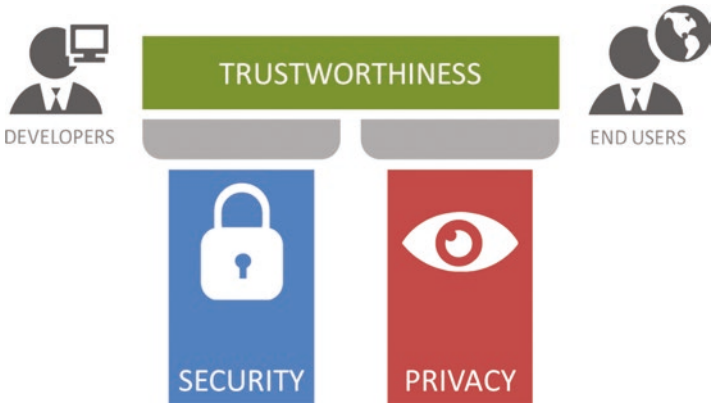

Fig. 2.1 Trustworthiness, security and privacy

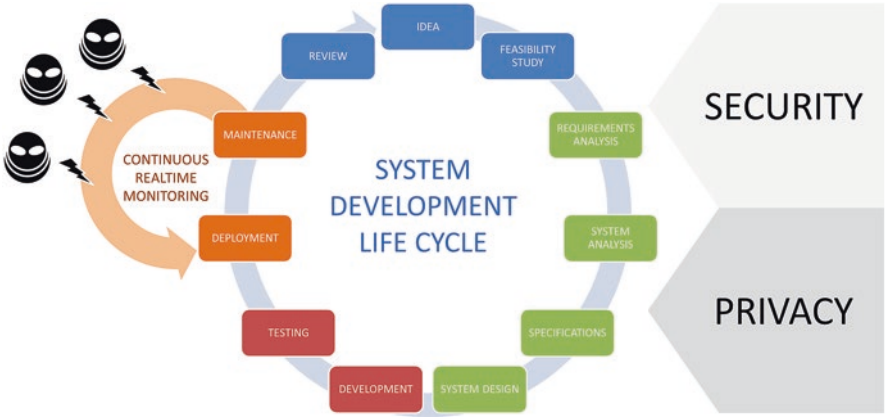

Fig. 2.2 Pervasiveness of security and privacy within the system development life cycle

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.