SECURITY AND PRIVACY IN THE INTERNET OF THINGS: CHALLENGES AND SOLUTIONS

Ambient Intelligence and Smart Environments

The Ambient Intelligence and Smart Environments (AISE) book series presents the latest research results in the theory and practice, analysis and design, implementation, application and experience of *Ambient Intelligence* (AmI) and *Smart Environments* (SmE).

Volume 27

Recently published in this series

Vol. 26. A. Muñoz, S. Ouhbi, W. Minker, L. Echabbi and M. Navarro-Cía (Eds.), Intelligent Environments 2019 – Workshop Proceedings of the 15th International Conference on Intelligent Environments
Vol. 25. M. Vega-Barbas and F. Seoane (Eds.), Transforming Ergonomics with Personalized Health and Intelligent Workplaces
Vol. 24. A. Muñoz and J. Park (Eds.), Agriculture and Environment Perspectives in Intelligent Systems
Vol. 23. I. Chatzigiannakis, Y. Tobe, P. Novais and O. Amft (Eds.), Intelligent Environments 2018 – Workshop Proceedings of the 14th International Conference on Intelligent Environments
Vol. 22. C. Analide and P. Kim (Eds.), Intelligent Environments 2017 – Workshop Proceedings of the 13th International Conference on Intelligent Environments
Vol. 21. P. Novais and S. Konomi (Eds.), Intelligent Environments 2016 – Workshop Proceedings of the 12th International Conference on Intelligent Environments
Vol. 20. W. Chen et al. (Eds.), Recent Advances in Ambient Assisted Living – Bridging Assistive Technologies, e-Health and Personalized Health Care
Vol. 19. D. Preuveneers (Ed.), Workshop Proceedings of the 11th International Conference on Intelligent Environments
Vol. 18. J.C. Augusto and T. Zhang (Eds.), Workshop Proceedings of the 10th International Conference on Intelligent Environments
Vol. 17. J.A. Botía and D. Charitos (Eds.), Workshop Proceedings of the 9th International Conference on Intelligent Environments

ISSN 1875-4163 (print)
ISSN 1875-4171 (online)

Security and Privacy in the Internet of Things: Challenges and Solutions

Edited by

José Luis Hernández Ramos

European Commission, Joint Research Centre

and

Antonio Skarmeta

University of Murcia, Department of Information and Communications Engineering

IOS Press

Amsterdam • Berlin • Washington, DC

ISBN 978-1-64368-052-1 (print)
ISBN 978-1-64368-053-8 (online)
Library of Congress Control Number: 2020930532
doi: 10.3233/AISE27

Publisher
IOS Press BV
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

For book sales in the USA and Canada:
IOS Press, Inc.
6751 Tepper Drive
Clifton, VA 20124
USA
Tel.: +1 703 830 6300
Fax: +1 703 830 2300
sales@iospress.com

PRINTED IN THE NETHERLANDS

Foreword

Christian Wilk
Research Executive Agency

The roots of the idea of the Internet of Things – even though first references to such an idea already appeared in the 1960s – can be traced back to a vision described by Mark Weiser in the early 1990s in his seminal article 'The Computer for the 21st Century'. In it he described a scenario which he called 'ubiquitous computing' where computers would vanish into the background, becoming so pervasive and unobtrusive that they would basically become invisible and ubiquitous. Such a network of sensors and processors would be permanently aware of the actors in its vicinity, and would react fully context-aware to each need expressed.

Moving from this scenario, which still had the human user and its needs at the center of attention, to a scenario where devices would communicate independently of human intervention, led to the term machine-to-machine communication.

Going even a step further and taking all these devices, independent of their focus on human or machine communication, and connecting them to the internet led to the term as we know it now, the Internet of Things (IoT).

The IoT could be defined as any networked thing equipped with the ability to generate, store, and exchange data, and in some cases as well as to act on data, thus being able to sense, to interact and to change its environment actively. This could be anything from tiny sensors embedded in moving vehicles, voice-activated loudspeakers, wearables, actuators and operational technology in industrial settings, to medical devices and implants.

This new form of seamless connectivity has many applications across various industries such as smart cities, smart grids for energy management, intelligent transportation, environmental monitoring, infrastructure management, and medical and healthcare systems, to building and home automation.

Within a business context where competition is mainly driven by lowering costs, and in combination with several constraints that IoT devices face, such as limited computing power and battery lifetime, security considerations are not the most important design feature for connected devices. And particularly in the industrial sector, legacy devices which may date back from the days when connectivity was very limited, when integrated into larger computer networks, can create risks that the original developers never anticipated.

These potentially severe implications to the security and safety of people makes the security and safety of IoT building blocks a paramount issue. Furthermore, a major barrier to the uptake of IoT on a larger scale is the lack of trust. Building trust into the

IoT based on robust cybersecurity features is a precondition for exploiting its numerous potential benefits and for the realization of Europe's Digital Single Market.

To ensure a minimum level of interoperability, security and assurance, the European Commission issued a Common Cybersecurity Strategy for the European Union in 2013 (JOIN(2013) 1), in which for the first time the term machine-to-machine communication in the context of automated water sprinklers was used to refer to the nascent field of IoT.

The Common Cybersecurity Strategy for the EU kicked off the preparatory work on several EU cybersecurity policies which over the following years became legal acts directly relevant and applicable to the IoT domain:

1. In August 2016 the NIS Directive (2016/1148) entered into force with member states having to transpose it into national law by May 2018. The NIS Directive has three parts:
    a. Capacity building: EU member states must possess minimum capabilities, adopt a cybersecurity strategy, and establish a single point of contact for cybersecurity issues (CSIRT)
    b. Critical Infrastructure: operators of essential services (critical sectors such as energy, transportation, water, healthcare, and finance) have to adopt a culture of risk management and have to comply with security and notification requirements.
    c. Cooperation: in order to build trust and confidence, member states shall collaborate across borders, a mechanism shall be put in place for the exchange of security related information, the sharing of incident information and best practices (CSIRTs network)

    Even though neither the term IoT itself nor its related terms is directly mentioned in the Directive, the Directive directly affects sectors with the highest potential use for (industrial) IoT.
2. The General Data Protection Regulation (GDPR) (2016/679) was released in April 2016, and entered into force on 25 May 2018. The GDPR aims to increase the control of individuals over their personal data and to unify data protection laws across the EU. It introduces limitations to the purpose and scope of personal data collection and processing. It also governs the transfer of personal data outside the EU, and introduces notification requirements in the case of a security breach affecting personal data.
3. The latest addition to the portfolio of EU legislation in the area of cybersecurity was the Cybersecurity Act (2019/881) which entered into force on 27 June 2019 and complements the NIS Directive. It mentions prominently the Internet of Things on several occasions. It consists of two main parts:
    a. Reinforcing the European Union Agency for Cybersecurity (ENISA) by giving it a permanent mandate and strengthening its role
    b. Establishing a European cybersecurity certification framework for ICT products, services and processes

It is against this evolving legal background that research and development projects funded within the EU's Horizon 2020 programme are trying to explore available options and possible approaches to address the security and privacy issues of the Internet of Things.

It is with great pleasure to see such a wide cross-section of projects presented in this book. The spectrum ranges from the secure management of personal data, the specific challenges of IoT with respect to the GDPR, through access control within a highly dynamic IoT environment, increasing trust with distributed ledger technologies, to new cryptographic approaches as a counter-measure for side-channel attacks, and the vulnerabilities of IoT-based ambient assisted living systems.

Security and safety of the Internet of Things will remain high on the agenda of policymakers for the foreseeable future. Even more so when moving towards the internet of nano-things, when things will become literally invisible to the human eye and can penetrate living things unnoticed. Together with the convergence of the physical and biological realm through nanotechnology and synthetic biology this will create an internet of living things which will blur the boundary between biological and cyber risks.

The need for proactive, forward looking policymaking, moving away from the current reactive approach, will therefore become even more important as policy development cycles and technology development cycles will presumably remain as decoupled and out of sync as they have been in the past.

Introduction

Enrico DEL RE[a]
[a] *University of Florence and CNIT, Italy*

In the Information Technology (IT) and in the future Internet of Things (IoT) systems security and privacy, also generally referred to as cybersecurity, play a key role and have to address these six main requirements:

- Authentication: the process of determining whether someone or something is, in fact, who or what it declares to be
- Access control: the procedure to allow an authorized utilization of a resource
- Data integrity: the certification to ensure that the received data are identical to the sent data
- Nonrepudiation: the protection against the possibility that the sender (or the recipient) could deny sending (or receiving) the data
- Availability: the certainty that the desired service must be available when required
- Confidentiality: all the procedures to guarantee that user data must be protected from any unauthorized access and usage

Today in present IT systems all six cybersecurity requirements are implemented by third parties (service providers and/or network operators) by means of suitable procedures (protocols) submitted to the user when requiring a service. Different levels of effectiveness, efficiency and performance have been achieved to fulfill these requirements: the first five have reached an acceptable or sufficient degree of performance (even if not always satisfactory), while recent unauthorized disclosure of user data, in particular by pervasive social networks (but not only by them), has clearly highlighted that the sixth requirement (i.e. confidentiality) need more stringent procedures and, probably, a completely different approach.

The European Union (EU) since 2012 tackled the cybersecurity issues and stated "Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services, including public e-government services. If not addressed, this lack of confidence will continue to slow down the development of innovative uses of new technologies, to act as an obstacle to economic growth and to block the public sector from reaping the potential benefits of digitisation of its services, e.g. in more efficient and less resource-intensive provisions of services. This is why data protection plays a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 Strategy"[1], and "by design new systems must include as initial requirements:

- The right of deletion
- The right to be forgotten
- Data portability
- Privacy and data protection principles

[1] *European Commission, 25.01.2012, SEC(2012)72 final, page 4.*

taking into account two general principles:

- The IoT shall not violate human identity, human integrity, human rights, privacy or individual or public liberties
- Individuals shall remain in control of their personal data generated or processed within the IoT, except where this would conflict with the previous principle."[2]

Following these general and challenging statements, in spite of heavy attempts to defeat any rule, the EU issued the so-called GDPR (General Data Protection Regulation) that entered into force in all Member States on 25 May 2018. This complex regulatory document deals with all cybersecurity requirements related to personal data and, particularly, to the confidentiality and privacy of data anyhow referred to the user (defined data subject in the GDPR terminology).

Basic principles and guidelines of GDPR, when someone or something is collecting, processing and storing personal data, are lawfulness, fairness, transparency, minimization, purpose limitation, security, accuracy and integrity. Another key and distinguishing feature is that the service providers must ask data subject for consent defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Consent is not given once and forever, but must be renewed whenever personal data are used for purposes other than those initially authorized. Heavy penalties are imposed on service providers who do not comply with the GDPR rules. It is a significant step forward for user security and privacy protection, as demonstrated by the worldwide acceptance of its principles, that have gained consensus outside Europe (California, Japan, Brasil, Singapore, New Zealand, and others).

Indeed services currently offered, while slowly trying to comply with GDPR rules, miss almost completely the fulfillment of the security and privacy requirements 'by initial design', as stated by the EU principles.

Moreover, in spite of its fundamental milestone on user security and privacy, does GDPR fully comply with the stated EU principle "Individuals shall remain in control of their personal data generated or processed within the IoT"?

The situation will become even more critical in scenarios foreseen for the future, where the high-speed, ultra-reliable, massive and always available connectivity at the global scale provided by the 5G mobile networks, the billions of (more or less) smart objects and sensors always connected in the IoT and the Artificial Intelligence (AI) innovative and powerful processing capabilities will realize the possibility to obtain, to store, to process, to deliver diversified and high volume data (Big Data). Most of these data will refer to human sensitive information and could be acquired even without the awareness of the interested subjects. For example, this is particularly realistic when automatic profiling (i.e. profiling without any human intervention) of the data subject personal data and automatic facial recognition are put in place. This scenario looks like an ever present distributed and global computer dealing with personal data without the awareness of their

---

[2] *European Commission, 2013, IoT Privacy, Data Protection, Information Security. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753*

owner and suggests a much worse scenario than the famous Big Brother described in Orwell's 1984, with the concrete risk of violation of the fundamental human rights and of people becoming the new future digital slaves of a few big players.

Of course, 5G, AI and IoT can provide breakthroughs and enormous benefits to society and individuals (e.g. for e-health applications and services to disabled and elderly people, environment control and security, smart energy production and utilization, smart mobility management, industry efficiency, smart cities, smart buildings, media and entertainment, e-government,…) and it is a vital interest of the entire human society to preserve the benefits while reducing to the minimum the associated risks of personal security and privacy.

While GDPR is a fundamental step to tackle these contrasting issues, however some possible realistic breaches are evident, in addition to noncompliance of service providers, e.g. by the mentioned automatic profiling and facial recognition.

The implementation of the six cybersecurity main requirements, including the last one of confidentiality and privacy, even after GDPR, is in charge of service providers that should guarantee their fulfillment. The heavy penalties in case of noncompliance should convince service providers to conform and to implement all the necessary tools and actions, but we all know that this is not always the case.

Actually, for the first five requirements the solution provided by third parties is an inevitable and proper approach. However, the control of the data subject of the authorized or unauthorized use of her/his personal data at most can be verified only a posteriori, e.g. accessing to a database of all data transactions certified by a Distributed Ledger Technology.

To avoid, perhaps definitively, the violation of our fundamental rights, we need the new paradigm of "a priori data usage control", meaning that "except in cases of force majeure or emergency, the use in any form and for any purpose of personal data must be authorized in advance and explicitly by its owner, correctly informed of the purpose of use". To meet this highly challenging objective, we need to synergize the innovative and revolutionary GDPR directives and new efficient technological tools dealing specifically with direct control by data subject of her/his data. Indeed, in the future IoT scenarios, the new technological solutions are needed for all the six requirements of security and privacy, as present tools and procedures can be no longer adequate.

The EU played a proactive role to search for the technological solutions to direct data subject control and, more in general, to all aspects of the security and privacy in the IoT, by funding specific researches in the framework of HORIZON 2020 and CHIST-ERA programmes. Doing this, EU put itself on the international forefront of advanced research on these technological challenging issues.

Of course, these research activities are ongoing, but some already achieved results are well encouraging towards possible practical solutions to the problems of the security and privacy in the IoT. The ten chapters of this book give an overview of some relevant preliminary results obtained by projects funded by EU in recent years and generally still ongoing. The readers are faced with the worldwide forefront of the more advanced

researches on the security and privacy techniques for future IoT scenarios, with many examples of specific case use applications.

The chapter **USEIT project: Empowering the users to protect their data** proposes a solution of the security and privacy in a smart building use case involving directly user action through the interaction with intermediate functional entities that analyses the data sent from different sensors in the building to implement the security measures.
The chapter "**Privacy awareness for IoT platforms: BRIAN-IoT approach**" addresses the challenges of privacy control and impact assessment for IoT platform by leveraging GDPR core principles and ISO/IEC standards.
The chapter "**UPRISE-IoT: User-centric Privacy & Security in the IoT**" manages the user awareness and control of privacy risks of a mobile app and the informed consent/deny of the service.
The chapter "**Making the Internet of Things More Reliable Thanks to Dynamic Access Control**" proposes new approaches of context-aware and distributed dynamic access control mechanisms.
The chapter "**The SOFIE Approach to Address the Security and Privacy of IoT using Interledger Technologies**" investigates the application of distributed multiple inter-ledger technologies for implementing authentication, access, nonrepudiation and privacy issues, applied to the four cases of food supply chain, electricity grid load balancing, context-aware mobile gaming, and smart meter data exchange.
The chapter "**Assessing Vulnerabilities in IoT-based Ambient Assisted Living systems**" proposes a framework to model, understand and analyze the security risks in possible attacks related to authorization and access by unauthorized entities to data referred to humans with special needs.
The two related chapters "**Construction of Efficient Codes for High-Order Direct Sum Masking** and **Direct Sum Masking as a Countermeasure to Side-Channel and Fault Injection Attacks**" describe new approaches of direct sum masking to data cryptography to provide countermeasures to the combination of side-channel and fault injection attacks.
The chapter "**A Framework for Security and Privacy for the Internet of Things (SPIRIT)**" addresses the authentication, access, integrity and privacy issues by extraction and classification of the document content and by encryption tools.
The chapter "**IoTCrawler. Managing security and privacy for IoT**" proposes a search engine for IoT information addressing authentication, authorization, confidentiality of exchanged data by encryption techniques and distributed ledger technologies for IoT inter-domain relations.
The following table proposes a concise synopsis of the distribution of the main contents of each chapter versus the six cybersecurity requirements. Foe each project the table points out the approach to address the headed requirement or, alternatively, when specific use cases are considered, what corresponding requirement they try to solve. Hopefully, it will help the reader to navigate around the book.

Table 1. Synopsis of the contents of the book chapters versus cybersecurity requirements

	Authentication	*Access control*	*Integrity*	*Nonrepudiation*	*Availability*	*Confidentiality*
USEIT project: Empowering the users to protect their data	Authentication, Identity management	Authorization	Key cryptographic exchange		Trust and Reputation	
Privacy awareness for IoT platforms: BRIAN-IoT approach						Privacy control based on GDPR and ISO/IEC
UPRISE-IoT: User-centric Privacy & Security in the IoT		Informed consent/deny				Privacy management in mobile apps
Making the Internet of Things More Reliable Thanks to Dynamic Access Control		Context-aware and distributed dynamic access				
The SOFIE Approach to Address the Security and Privacy of IoT using Interledger Technologies	4 cases: food chain, electricity load balancing, mobile gaming, smart meter	4 cases: food chain, electricity load balancing, mobile gaming, smart meter		4 cases: food chain, electricity load balancing, mobile gaming, smart meter		4 cases: food chain, electricity load balancing, mobile gaming, smart meter
Assessing Vulnerabilities in IoT-based Ambient Assisted Living systems	For humans of special needs	For humans of special needs				
Construction of Efficient Codes for High-Order Direct Sum Masking	Cryptography to provide countermeasures to the combination of side-channel and fault injection attacks					

	Authentication	*Access control*	*Integrity*	*Nonrepudiation*	*Availability*	*Confidentiality*
SPIRIT Project	Extraction and classification of the document content	Extraction and classification of the document content	Extraction and classification of the document content and encryption			Extraction and classification of the document content
Direct Sum Masking as a Countermeasure to Side-Channel and Fault Injection Attacks	Cryptography to provide countermeasures to the combination of side-channel and fault injection attacks					
IoTCrawler. Managing security and privacy for IoT	Encryption techniques and distributed ledger technologies	Encryption techniques and distributed ledger technologies				Encryption techniques and distributed ledger technologies

This work has been partially sponsored by the USEIT project (CHIST-ERA PCIN-2016-010) as well as the EU H2020 projects OLYMPUS (Grant agreement ID: 786725) and SerIoT (Grant agreement ID: 780139)

Contents