Consolidating IoT Hardening through a Qualitative and Experimental Approach

Authors
Matthew Cutajar, MSc (Royal Holloway, 2022)
Konstantinos Markantonakis, ISG, Royal Holloway

Abstract

The Internet of Things (IoT) refers to the interconnected network of physical devices, vehicles, buildings, and other objects that are embedded with sensors, software, and connectivity. IoT devices can communicate and interact with the internet as well as other similar devices, to provide valuable insights and services for various industries such as healthcare, transportation, and smart cities. However, as the number of IoT devices increases, so do the potential vulnerabilities and security risks. These vulnerabilities can be caused by a variety of factors, such as weak default passwords, lack of encryption, and outdated software. Hackers can exploit these vulnerabilities to gain access to sensitive information, disrupt operations, or launch attacks on other devices and systems. Data breaches, device or network compromise, privacy violations, downtime and in the case of organisations, business interruption are some of the consequences of an IoT device being hacked. This makes it imperative to secure IoT devices. One of the means to secure IoT devices is hardening procedures, where a set of security measures are implemented to improve the security of IoT devices and systems. This article puts forward an analysis of three hardening procedures published by three reputable organisations within the Cybersecurity field, which can be used by smart home users. Furthermore, this article provides a description and analysis of how a new hardening procedure was recommended.[a]

[a] This article is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.

1 Introduction

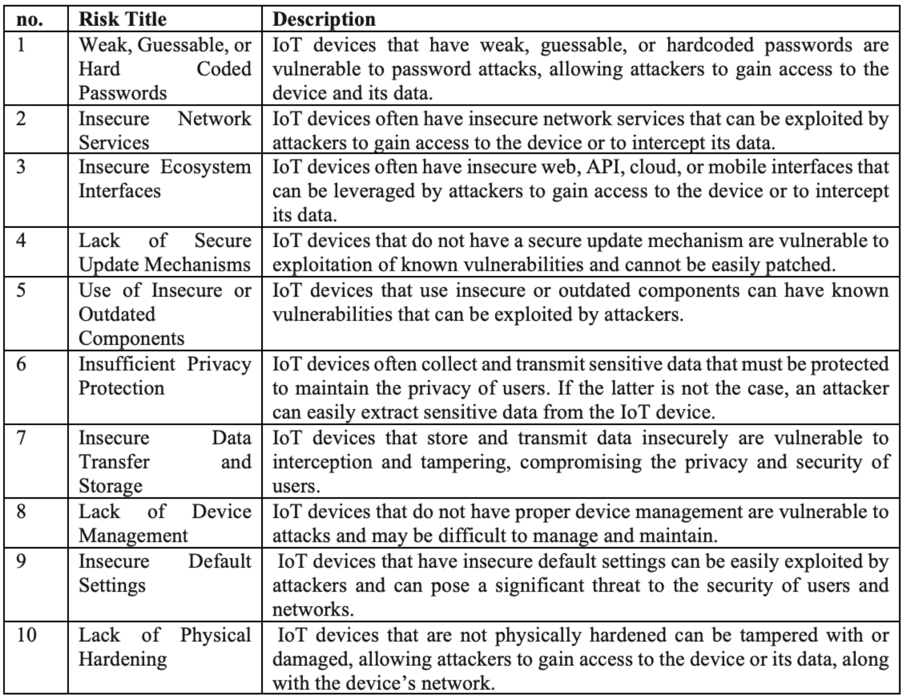
IoT is an emerging technology platform, where different smart devices communicate with each other via sensors. Such devices are also connected to the internet and can make people's lifestyles easier via machine-learning. Nowadays, IoT is also being used within various organisations and is no longer restricted to household items. The goal of IoT is to make everyday objects "smart" by giving them the ability to communicate and interact with each other and with humans. Hence, making our lives more convenient and efficient. IoT technology has the potential to revolutionise many industries, including healthcare, transportation, and home automation. The number of connected IoT devices was expected to reach 20.4 billion by 2020 and will rise to 30.7 billion by 2025 (Gartner, 2017[1]). International Data Corporation (IDC, 2021[2]) predicted that the number of IoT devices is estimated to reach 55.7 billion dollars by 2025. But as the number of IoT devices increase, so do IoT attacks. A study by Zscaler (2020)[3] found that the number of IoT malware samples increased by 700% between 2019 and 2020. IoT attacks are on the rise due to several factors, including the increasing number of connected devices, lack of security measures in many IoT devices, and the valuable data that can be obtained from these devices.

[1] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[2] https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/

[3] https://ir.zscaler.com/news-releases/news-release-details/zscaler-study-confirms-iot-devices-are-major-source-security

Table 1: OWASP IoT Top 10 and the description



no.	Risk Title	Description
1	Weak, Guessable, or Hard Coded Passwords	IoT devices that have weak, guessable, or hardcoded passwords are vulnerable to password attacks, allowing attackers to gain access to the device and its data.
2	Insecure Network Services	IoT devices often have insecure network services that can be exploited by attackers to gain access to the device or to intercept its data.
3	Insecure Ecosystem Interfaces	IoT devices often have insecure web, API, cloud, or mobile interfaces that can be leveraged by attackers to gain access to the device or to intercept its data.
4	Lack of Secure Update Mechanisms	IoT devices that do not have a secure update mechanism are vulnerable to exploitation of known vulnerabilities and cannot be easily patched.
5	Use of Insecure or Outdated Components	IoT devices that use insecure or outdated components can have known vulnerabilities that can be exploited by attackers.
6	Insufficient Privacy Protection	IoT devices often collect and transmit sensitive data that must be protected to maintain the privacy of users. If the latter is not the case, an attacker can easily extract sensitive data from the IoT device.
7	Insecure Data Transfer and Storage	IoT devices that store and transmit data insecurely are vulnerable to interception and tampering, compromising the privacy and security of users.
8	Lack of Device Management	IoT devices that do not have proper device management are vulnerable to attacks and may be difficult to manage and maintain.
9	Insecure Default Settings	IoT devices that have insecure default settings can be easily exploited by attackers and can pose a significant threat to the security of users and networks.
10	Lack of Physical Hardening	IoT devices that are not physically hardened can be tampered with or damaged, allowing attackers to gain access to the device or its data, along with the device’s network.

IoT attacks can take on many forms as will be further discussed below. Additionally, many IoT devices are not designed with security in mind and lack basic security features such as encryption or regular software updates. A successful attack on an IoT device could have serious consequences, including loss of life, financial loss, and disruption of critical services. One way of securing IoT devices against cyber-attacks and protecting sensitive information are hardening procedures. Hardening refers to the process of securing a device by reducing its attack surface and making it more resistant to cyber-attacks. Hardening procedures can help to address IoT attacks by, for example, requiring strong passwords, enabling encryption, and ensuring that software is up to date.

Some examples of **IoT Security Attacks** are:
- Malware attacks;
- Distributed Denial-of-Service (DDoS) attacks;
- Botnet attacks;
- Man-in-the-middle attacks;
- Physical attacks; and
- Credential Stuffing Attacks.

This article will give a brief overview on an experimental and qualitative analysis of three IoT hardening procedure and an analysis of a hardening procedure carried out by the author. The aim of the proposed hardening procedure was to provide smart home users with more controls which if implemented can protect their IoT devices further. Thus, the overall security of IoT devices is increased through the mitigation of threats and vulnerabilities and the reduction of the overall threat landscape of IoT devices.

2 OWASP’s Top 10 Critical IoT Security Risks

As previously outlined, IoT security attacks are malicious activities aimed at exploiting vulnerabilities in IoT devices and systems to gain unauthorised access, steal sensitive information, or disrupt the normal operations of the devices. These attacks pose a significant threat to the security and privacy of IoT users and the integrity of IoT systems.

The Open Web Application Security Project (OWASP) has a list called the ‘OWASP IoT Top 10’[4]

[4] https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

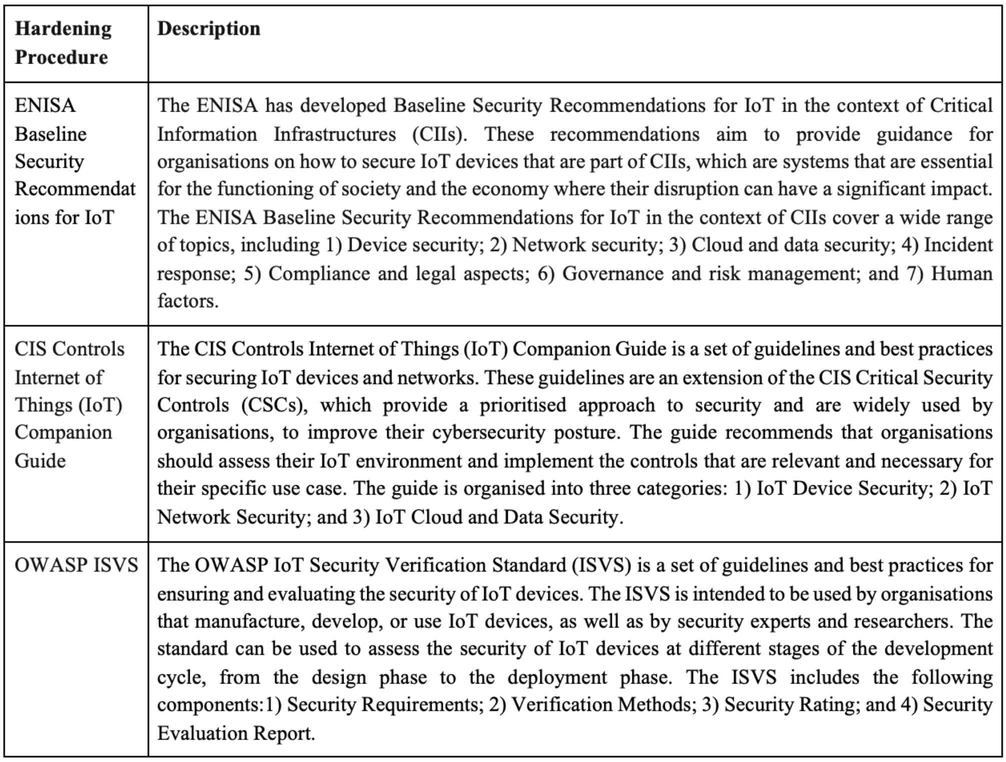
including the most critical security risks identified within IoT devices, developed by the OWASP in 2018. As indicated in Table 1, the list aims to provide a comprehensive overview of the security risks associated with IoT devices, and to provide guidance for organisations on how to mitigate these risks. The latest version of the list was released in 2018. Table 1 presents the OWASP IoT Top 10 and a description provided by the author about each risk.

3 IoT Hardening Procedures

IoT hardening procedures refer to the process of securing IoT devices and systems from potential cyber threats. These procedures involve implementing various security measures, such as access control, data encryption, firmware updates and network segmentation, to strengthen the security of IoT devices and prevent unauthorised access, data breaches, and other security incidents.

Several organisations, such as the European Union Agency for Cybersecurity (ENISA), OWASP, and National Institute of Standards and Technology (NIST), have published guidelines and best practices for IoT hardening. The three hardening procedures used for this research are ENISA's 'Baseline Security Recommendations for IoT' (2017)[5], the CIS 'Controls Internet of Things Companion Guide' (2019[6]) and OWASP IoT 'Security Verification Standard' (2022)[7]. Each of these hardening procedures are briefly described in Table 2 below.

Table 2: Hardening Procedures and their respective description



Hardening Procedure	**Description**
ENISA Baseline Security Recommendations for IoT	The ENISA has developed Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures (CIIs). These recommendations aim to provide guidance for organisations on how to secure IoT devices that are part of CIIs, which are systems that are essential for the functioning of society and the economy where their disruption can have a significant impact. The ENISA Baseline Security Recommendations for IoT in the context of CIIs cover a wide range of topics, including 1) Device security; 2) Network security; 3) Cloud and data security; 4) Incident response; 5) Compliance and legal aspects; 6) Governance and risk management; and 7) Human factors.
CIS Controls Internet of Things (IoT) Companion Guide	The CIS Controls Internet of Things (IoT) Companion Guide is a set of guidelines and best practices for securing IoT devices and networks. These guidelines are an extension of the CIS Critical Security Controls (CSCs), which provide a prioritised approach to security and are widely used by organisations, to improve their cybersecurity posture. The guide recommends that organisations should assess their IoT environment and implement the controls that are relevant and necessary for their specific use case. The guide is organised into three categories: 1) IoT Device Security; 2) IoT Network Security; and 3) IoT Cloud and Data Security.
OWASP ISVS	The OWASP IoT Security Verification Standard (ISVS) is a set of guidelines and best practices for ensuring and evaluating the security of IoT devices. The ISVS is intended to be used by organisations that manufacture, develop, or use IoT devices, as well as by security experts and researchers. The standard can be used to assess the security of IoT devices at different stages of the development cycle, from the design phase to the deployment phase. The ISVS includes the following components:1) Security Requirements; 2) Verification Methods; 3) Security Rating; and 4) Security Evaluation Report.

[5] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[6] https://paperpile.com/b/d4ycgz/FK3c

[7] https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS

4 Methodology

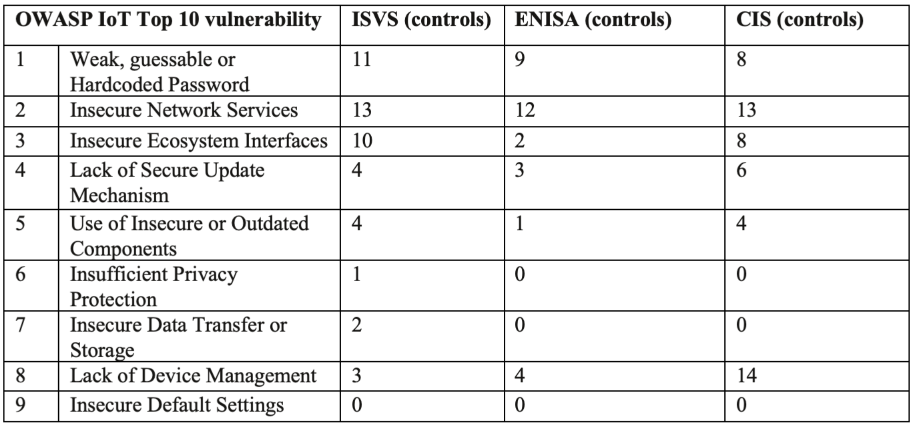
A qualitative and experimental approach was used in order to provide an analysis of the three hardening procedures mentioned above. To gather data through the qualitative approach of this study, for each hardening procedure (ISVS, ENISA and CIS) the below steps where performed:

1. Identification of controls that are applicable and implementable in a smart home environment;

2. Each applicable control was then scored according to which OWASP IoT Top 10 vulnerability it aimed to mitigate. For example, if it solved OWASP IoT Top 10 Risk Number 1 it was assigned 10 points, and for IoT Risk Number 10, 1 point was assigned.

For clarity's sake, ISVS had 11 controls which were applicable and can be attributed to mitigating the OWASP IoT Top 10 vulnerability number 1 (Weak, guessable, or hardcoded Password). ENISA and CIS had 9 and 8 controls which were applicable and mitigating the same control. The findings of the above exercise are summarised in Table 3 below. All the controls which cannot be implemented within a smart home environment are also listed within Table 3, meaning that those controls are primarily intended for Smart Home Developers, Manufacturers or organisations implementing IoT technologies.

Table 3: Hardening Procedure Applicable Controls according OWASP's IoT Top 10 Vulnerability



OWASP IoT Top 10 vulnerability		ISVS (controls)	ENISA (controls)	CIS (controls)
1	Weak, guessable or Hardcoded Password	11	9	8
2	Insecure Network Services	13	12	13
3	Insecure Ecosystem Interfaces	10	2	8
4	Lack of Secure Update Mechanism	4	3	6
5	Use of Insecure or Outdated Components	4	1	4
6	Insufficient Privacy Protection	1	0	0
7	Insecure Data Transfer or Storage	2	0	0
8	Lack of Device Management	3	4	14
9	Insecure Default Settings	0	0	0

Furthermore, to compare the hardening procedures the author sought to identify the percentage of applicable controls that each hardening procedure had. This was calculated using the Formula 1 below. Moreover, to gather additional data, the author summed up all the scores of each hardening procedure and then calculated the average points per control using Formula 2.

Formulas:

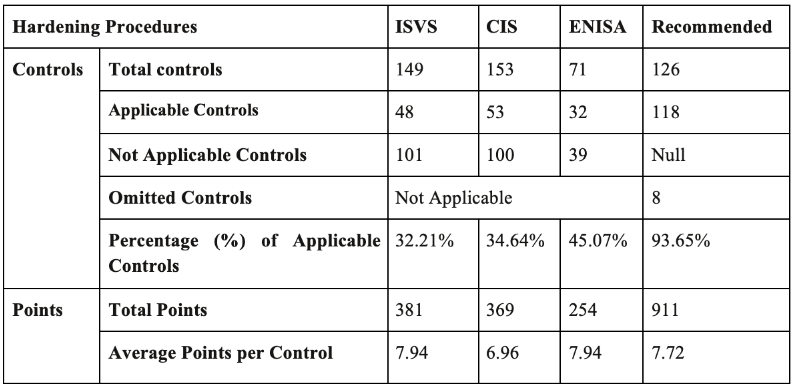
1) Percentage (%) of applicable Controls = (100 ∗ Not Applicable Controls) / Applicable Controls

2) Average Points per question = Total Number of Points / Total Controls

The recommended procedure was set up by joining all the applicable controls from all the three hardening procedures mentioned above into one hardening procedure. It was noted that there was an overlap in controls targeting smart homeowners and thus, those controls which were considered duplicate were omitted. Once all the duplicates were omitted, the remaining controls were sorted according to the OWASP IoT Top 10 score which was assigned to each control (as per the scoring system mentioned above). To perform the qualitative analysis, the recommended procedure was then compared to the three chosen hardening procedures. The findings of the analysis performed above are presented in Table 4.

As can be noted from Table 4, it is evident that the recommended hardening procedure (incorporating the controls of the three hardening procedures) provided more controls than any of the other three hardening procedures used on their own, especially in the Top 3 OWASP IoT Top 10 vulnerabilities.

Table 4: Breakdown of workings including recommended hardening procedure



Hardening Procedures		**ISVS**	**CIS**	**ENISA**	**Recommended**
Controls	**Total controls**	149	153	71	126
	Applicable Controls	48	53	32	118
	Not Applicable Controls	101	100	39	Null
	Omitted Controls	Not Applicable			8
	Percentage (%) of Applicable Controls	32.21%	34.64%	45.07%	93.65%
Points	**Total Points**	381	369	254	911
	Average Points per Control	7.94	6.96	7.94	7.72

This is since the recommended hardening procedure was a merger of all the three hardening procedures established to be used in this study.

5 Experimental Approach

To verify whether the recommended procedure provides any further benefits in a "real-case scenario" when compared to the three other hardening procedures used on their own, testing was carried out under the five Case Scenarios indicated below using the Modified Risk Evaluation Process defined in Figure 1:

1. IoT device is not hardened;
2. IoT device is hardened using OWASP ISVS;
3. IoT device is hardened using CIS Controls;
4. IoT device is hardened using ENISA;
5. IoT device is hardened using the recommended hardening procedure as explained in the qualitative approach.

For each Case Scenario a CVSSv3 Severity Rating was assigned. The severity rating for Case Scenario 1 was a 'High' severity rating outlining several Operating System vulnerabilities. A legacy version of Raspbian (Raspbian Buster) was utilised to mimic a device being introduced in the market without vulnerabilities. Possibly being laden with vulnerabilities once the end-user starts using the device. The start point of the other four Case Scenarios were the non-hardened device with vulnerabilities established in Case Scenario 1. The target CVSSv3 Severity Rating for Case Scenarios 2 to 5 were then considered 'Null'.

The author used a modified risk evaluation process to identify a Common Vulnerability Scoring System Version 3 (CVSSv3) severity rating for each case scenario. The modified risk evaluation process was used to verify whether the proposed hardening procedure has a lower severity rating than the other three procedures. Figure 1 illustrates the modified risk evaluation process proposed by the author.

From the research findings established through the Case Scenarios, the author noted that by implementing minor changes on the device (Raspberry Pi), the security of IoT devices can be increased drastically. Furthermore, results indicated that by implementing the recommended hardening procedure within the same Case Scenario the same CVSSv3 severity score (Null) was achieved. Thus, it can be attested that when exposed to the same attacks on the same device, the recommended hardening procedure rendered the same level of confidence as the three other hardening procedures.

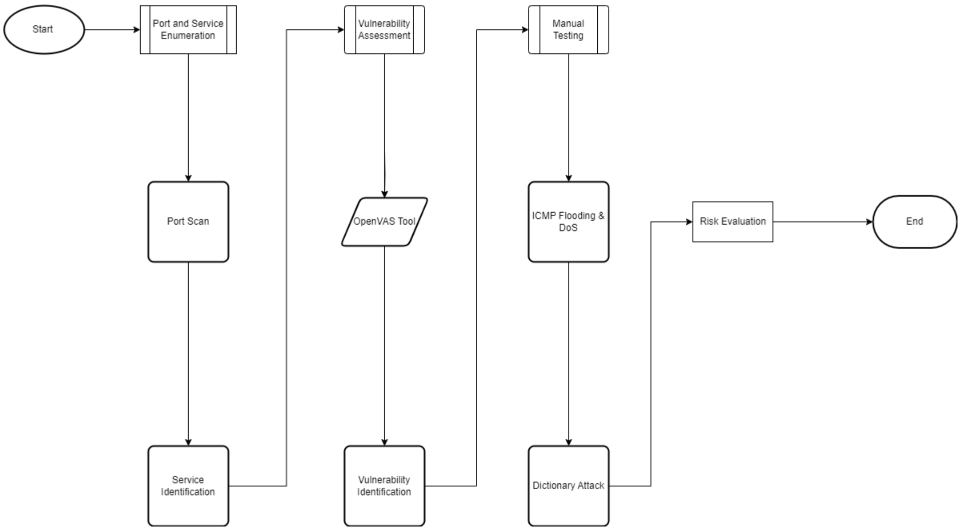


Figure 1: Modified Risk Evaluation Process

6 Conclusions and Recommendations

In concluding it can be attested that to reduce the overall risks in IoT devices, measures should be taken throughout all the points of an IoT product lifecycle starting from design till the device is decommissioned by the smart home users. Thus, it is imperative that reputable organisations such as ENISA, CIS and OWASP continue to publish hardening procedures not just for developers/manufacturers of smart home devices but also hardening procedures targeted at smart home users. Smart homeowners must also be aware that the convenience that these IoT devices offer comes at a price for their privacy and their network security. Thus, the general public must be more aware of IoT risks and implement the necessary hardening procedures to better protect their data.

Manufacturers and developers of smart home devices must establish a support lifecycle for IoT devices. Hence, ensuring continuous software updates mitigating any vulnerabilities which are identified of smart home devices. This will ensure that the risk landscape of their devices is minimal. However, manufacturers can release thousands of software updates but if these aren't downloaded and installed by the IoT devices' owners this is futile. Therefore, smart homeowners must regularly check whether their devices have updates and install them as soon as possible to ensure that they are up-to-date with the latest vulnerability patching. It should also be a common practice for manufacturers to force request smart homeowners to change the devices' default password upon initial configuration. If this is not possible, then smart homeowners should change the default passwords immediately and only enable the necessary services on their IoT devices. This reduces the attack surface and enables everyone to unlock the full potential that IoT has to offer.

Biographies

Matthew Cutajar received his MSc in Information Security from the Royal Holloway, University of London in 2022. He was previously certified by EC-council as a Certified Ethical Hacker and a GIAC Web Application Penetration Tester by GIAC in 2020. He is currently working as a Senior Cyber Security engineer with one of the three main telecommunication companies in Malta having previously worked as an Information Security Analyst in a bank. His research interests are privacy and security in distributed systems, mainly the Internet of Things (IoT). The main areas of expertise revolve around interpreting cybersecurity standards, drafting and reviewing policies and procedures whilst also implementing Information Security best practices or systems which support the underlying policies.

Konstantinos Markantonakis is a Professor at the Information Security Group at Royal Holloway University of London and the Director of the Information Security Group Smart Card and IoT Security Centre (SCC) with research, teaching, and managerial responsibilities. He is also the Director of the Transformative Digital Technologies, Security and Society Catalyst responsible for coordinating multidisciplinary and impactful research. His main research interests involve smart card security and applications, IoTs/CPS, embedded system security and trusted execution environments, secure payment systems, cloud computing and transparent and explainable AI. He has published more than 210 papers, articles and book chapters in international conferences/journals. He continues to act as a consultant on a variety of information security topics.

Series editor: Dr Maryam Mehrnezhad, ISG, RHUL