Security and Privacy Functionalities in IoT

1st Elahe Fazeldehkordi
Dept. of Informatics/Technology Systems
University of Oslo
elahe.fazeldehkordi@its.uio.no

2nd Olaf Owe
Dept. of Informatics
University of Oslo
olaf@ifi.uio.no

3rd Josef Noll
Dept. of Technology Systems
University of Oslo
josef@jnoll.net

***Abstract*—Internet of Things (IoT) offers a variety of technologies for connecting different kinds of heterogeneous devices. Security and privacy are becoming the main issue for IoT systems and their developers. Nevertheless, most works on IoT security and privacy requirements look at these requirements from a high-level view. Hence, the essential aspects of security and privacy functionalities will be disregarded, causing wrong design decisions. To combat this problem, this paper summarizes the most current documents related to security and privacy functionalities in the setting of IoT and provides a new taxonomy framework that organizes all aspects of security and privacy baselines, guidelines, and recommendations. To give an understanding of how the framework can help to improve security and privacy of IoT products, we combine it with a security classification method and demonstrate the usefulness by a case study of health products. Our framework can serve as a cornerstone towards the development of appropriate security solutions.**

***Index Terms*—security; privacy; IoT; IoT functionalities.**

I. Introduction

Internet of Things (IoT) represents the concept of information flow among different kinds of embedded computing devices interconnected through the internet. The aim of IoT is to provide an advanced mode of communication among the various systems and devices, and also to facilitate the interaction between humans and the virtual world. With this aim, IoT plays a significant role in the modern society and has applications in almost all fields including healthcare systems, automobile, industrial appliances, sports, homes, entertainments, environmental monitoring etc. IoT devices have already outnumbered the number of people at a computerized workplaces, and by 2020, connected "things" based on IoT will be around 212 billion [17], [21]. Those "things" will be daily used appliances like smart-phones, smart-watches, smart television, smart refrigerators, and others. As a result of this expansion, and as most things are connecting to the internet for exchanging information, IoT is vulnerable to various security issues and attacks (e.g., man in the middle attack, eavesdropping attack, denial of service attack, access attack, as well as major privacy concerns for the end users). Despite the advance abilities provided by IoT in the data communication area, its vulnerability implications from a security and privacy standpoint are still of great concern. Therefore appropriate steps in the initial phase of design and development of IoT systems should be taken.

Supported by the Norwegian Research Council through the IoTSec project, with number 248113/O70, and by the European Leadership Joint Undertaking (under EU H2020) through the SCOTT project, grant agreement No 737422.

In this paper, we focus on the comprehensive view of the state-of-the-art concerning security and privacy functionalities and requirements for IoT systems. Consequently, we suggest a complementary methodology for analyzing the functionalities in a comprehensive framework that can help both providers and consumers of IoT devices to have a better understanding of the security and privacy aspects. By functionality we mean: "The security and privacy-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate" [23]. We explore how the framework can facilitate the process of improving IoT security and privacy, in combination with the security classification method suggested in [4], [25]. Security classification of a system will lead to a better understanding of the value of security and promote the extra cost of securing a system. An IoT system includes different devices, and protecting all of these devices at the same level is costly. It is economically impractical to employ all the security protection mechanisms for all the devices in a system. Dividing security into different classifications is necessary, to secure IoT systems to an appropriate level.

One attractive application area of IoT is health care [15], [20], where IoT devices are becoming common. Medical applications like remote health monitoring, fitness programs, chronic diseases, elderly care, compliance with treatment and medication at home and by health-care providers are some of the important potential applications that can be facilitated by IoT. IoT-based health-care services can help to reduce costs, increase the quality of life, and enrich the users' experience. Therefore, we choose to demonstrate the framework on a case study concerning health products. Through the development of this framework together with security classification, extensive attention has been given to the requirements and limitations for securing IoT systems.

For this framework, we have investigated the most important IoT-related security baselines and guidelines developed by ENISA [9], [10], OWASP [18], Industrial Internet Consortium [24], Cloud Security Alliance[8], and Broadband Internet Technical Advisory Group [6], etc., as well as security and privacy guidelines from ISO [1], [2] and NIST [23], which could be relevant for securing IoT systems. With respect to privacy, the European Union (EU) has passed the general data protection regulation (GDPR), which regulates who can access private data, how and for what purpose, based on the consent

of the data subject [10]. We have extracted the parts of these documents that deal with IoT and security/privacy, and then we have unified them using a common vocabulary, and have then categorized and integrated the resulting guidelines and requirements in a uniform style, and embedded them in a graphical representation by means of a tool based on diagrams.

Having a comprehensive view and taxonomy of security and privacy requirements and functionalities in IoT is a prerequisite for architecting optimal security solutions, designing, and developing secure and privacy-aware IoT systems. To give an understanding of how the framework can help to improve security and privacy in practice, we combine the framework with the security classification method of [4], [25], and demonstrate how the combined methodology can be used on a case study of health products.

The contribution of this paper is to present a new functionality framework for security and privacy of IoT systems, as outlined above, and show how it can be combined with the security classification method to analyse and evaluate the security and privacy weaknesses of IoT systems, and to reduce these weaknesses, as demonstrated in the case study. Systems are often made without the help of security and privacy experts. Our framework is easy to follow, even for non-experts. The case study shows that by following our guidelines, one can detect security problems and get help in avoiding them.

The remainder of this paper is structured as follows: Section II explains IoT-related standards and guidelines. Section III provides related work. Section IV introduces the IoT security and privacy functionality framework. Section V explains the security classification method. Section VI describes the pacemaker case study, and Section VII concludes the paper.

II. IoT-Related Standards and Guidelines

Cloud Security Alliance [8] has provided considerations and guidance for designing and developing secure IoT devices. It aims to reduce some of the more common issues that can be found in the development of IoT devices. A number of activities that will enable a development organization to begin enhancing the security state of IoT devices have been outlined. This document has provided a graphical view of the steps needed in order to develop more secure IoT devices. Although IoT systems are complex, including devices, gateways, mobile applications, appliances, web services, datastores, analytics systems and more, the focus of this guidance is mainly on the "devices". In contrast, our work summarizes security and privacy functionalities considerations in the whole range of IoT system.

A security framework has been presented in Industrial Internet Consortium [24] which comprises of six interacting building blocks. These building blocks are organised into three layers. The top layer includes four core security functions, which are supported by a data protection layer and a system-wide security model and policy layer. The four core security functions are: endpoint protection, communication and connectivity protection, security monitoring and analysis, and security configuration management. And then they break down each layer into related key functions and explain the responsibility for each function. This document explains and positions security or related architectures, designs, and technologies. It also identifies procedures relevant to trustworthy Industrial Internet of Things (IIoT) systems. Security characteristics, technologies, and techniques that should be applied, and methods for addressing security, have been described. However, it lacks some of the security functionalities, and in particular, it does not focus on privacy issues. The layer structure is a bit complicated, and we believe our framework has a more relaxed structure to use.

The ISO [1], [2] and NIST [23] standards are general requirements for establishing, implementing, maintaining and continually improving an information security management system, and protecting the confidentiality of Controlled Unclassified Information (CUI), respectively. We have extracted the IoT-related requirements from these standards and included these parts in our framework, while combining them with baselines and guidelines from other IoT-related documents, including OWASP and ENISA discussed below.

OWASP [18] presents guidance at a basic level, giving builders of IoT products a basic set of guidelines to consider from their perspective. The idea is that ensuring that these fundamentals are covered, will significantly improve the security of any IoT product. ENISA [9] elaborates baseline cybersecurity recommendations for IoT with a focus on Critical Information Infrastructures, which encompass facilities, networks, services, and physical and information technology equipment. Both of these guidelines, OWASP and ENISA, are addressing IoT, but both are presented in textual form, without defining a framework.

III. Related Work

In a work presented by Sicari et al. [26], the most relevant available solutions regarding security, privacy, and trust in IoT have been analyzed. Proposals related to security middleware, secure solutions for mobile devices, and ongoing international projects on this subject, have been discussed in their work; however, the focus is more general, addressing authentication, confidentiality and access control, while we break down security and privacy requirements in more detail, using a framework of functionalities for all the baselines.

Main challenges and security threats in smart home networks have been analyzed by Lee et al. [16], and the fundamental requirements in order to provide secure and confidential operations in smart homes are explained from the results of their analysis. Although these requirements have been listed, they still lack practical solutions or recommendations in this matter. In [27], Suo et al. have deeply analyzed security architecture and features, and divided IoT systems into four key levels of architecture. According to this analysis, the security requirements for each level have been summarized. Furthermore, the research status of key technologies including encryption mechanism, communication security, protection of sensor data, and cryptography algorithms, have been discussed.

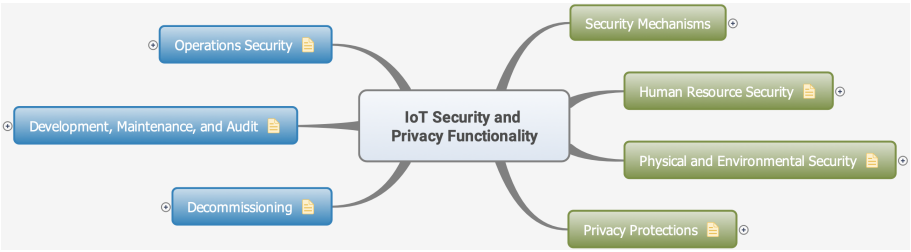


Fig. 1: IoT Security and Privacy Functionality Framework.

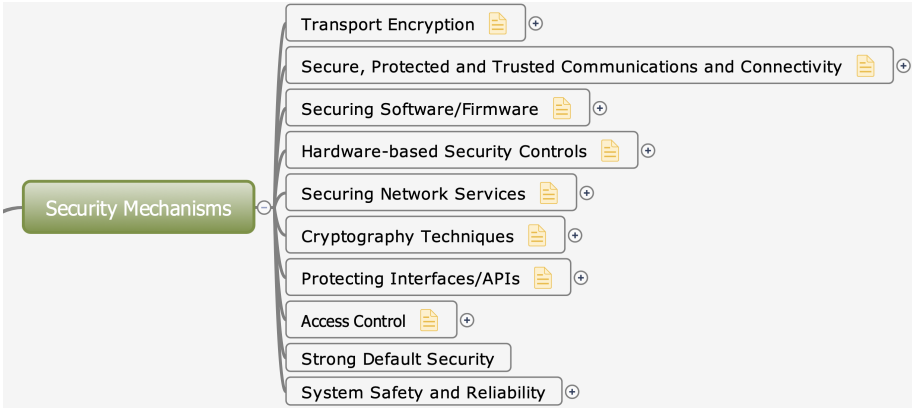


Fig. 2: Security Mechanisms.

Roman et al. [22] have discussed threats faced by IoT, as well as security and privacy foundations based on objectives in a scenario involving a smart meter. However, they did not give any details about practical baselines and guidelines showing how to achieve these foundations.

Babar et al. [5] have presented a threat taxonomy and high-level security requirements for IoT, which like most of the other works only highlight these requirements without any practical recommendations for each category. And at the end, they introduced a security model based on high-level requirements of security, privacy and trust. Related security requirements of IoT systems are discussed by Alqassem and Svetinovic [3], proposing a taxonomy of quality attributes, and some of the existing security mechanisms and policies in this matter have been reviewed, to reduce the identified security attacks and mitigate future vulnerabilities in these systems. They also have applied this taxonomy in a smart grid AMI as an IoT scenario. In contrast, our framework considers both security and privacy requirements and decomposes the related mechanisms, policies, and requirements with more details. In summary, our work provides a comprehensive view and a framework that covers all of the IoT security and privacy baselines, guidelines, and recommendations for every requirement.

IV. Framework Explanation

In Fig. 1, we present an overview of the security and privacy functionality framework, including the top-level security and privacy concepts. The functionalities are separated into two major parts, the *life cycle* aspects of a system and the *management* aspects of security and privacy. The life cycle relates to the different phases in the life of a system, while the management of security and privacy is the ability to put supporting functionality elements in the system. We believe that awareness about where we are in the life cycle is essential, and makes it easier to apply the right functionalities and how to do the appropriate security and privacy management. We use blue color to distinguish subtopics related to the *life cycle* of a system from those associated with the *management* of security and privacy, colored in green. The coloring makes the division clear, and gives a better structure of the framework, separating the two primary concerns.

In the following, we describe each part of the framework and the related subtopics. For brevity, we do not expand the whole framework and just mention some of the aspects. For more details and complete expansion of the framework refer to the long version [11].

Security Mechanisms - Different security mechanisms are illustrated in Fig. 2. Security mechanisms are processes designed to detect, prevent or recover from a security attack in IoT devices, including:

- *Secure, Protected and Trusted Communications and Connectivity:* This includes information flow protection, standardising security protocols (i.e., Transport Layer Security (TLS) for encryption) guaranteeing data authenticity, signing data, disabling specific ports and/or network connections for selective connectivity, etc.
- *Hardware-based Security Controls:* product developers should evaluate and implement hardware protection

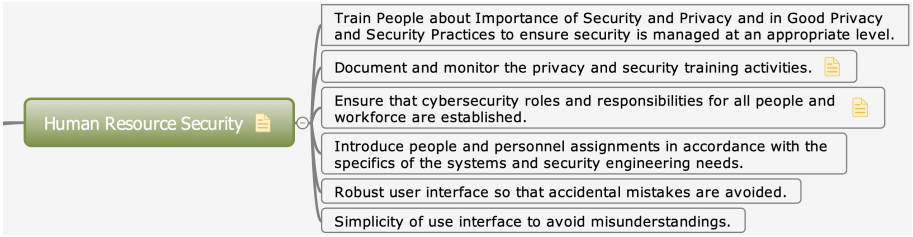


Fig. 3: Human Resource Security.

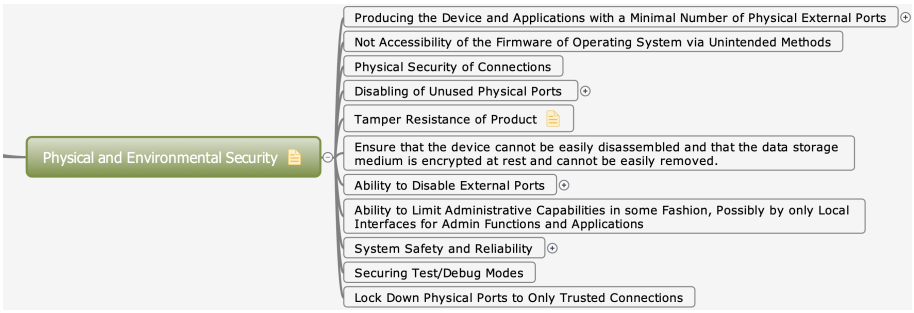


Fig. 4: Physical and Environmental Security.

Fig. 5: Privacy Protection.

mechanisms, including the use of Memory Protection Units (MPUs), considering a Trusted Platform Module (TPM) into IoT Devices, securing physical interfaces, tamper protections, etc.

- *Protecting Interfaces/Application Programming Interface (APIs):* Interface security is one of the critical tasks when it comes to developing IoT devices. IoT products interact with so many cloud services, custom-developed smartphone apps and also peer IoT products. If APIs do not protect adequately, service providers might be exposed. APIs must protect adequately against misuse, by techniques like rate-limiting to protect against compromised IoT devices that attempts to flood the service, error handling, embedding time-stamps or counters into messaging to protect against replay attacks, certificate pinning to protect against sensitive data transmission into GET requests, etc.
- *Access Control:* only authorized users should have access, applications and services and unauthorized accesses should be prevented, user accountability should be enabled to safeguard their authentication information.

Human Resource Security - People and contractors should understand the cybersecurity responsibilities suitable for their roles, and be trained about the importance of security and privacy. Further, to avoid misunderstanding, the user interfaces should be simple yet robust enough to avoid accidental mistakes. See Fig. 3.

Physical and Environmental Security - The objectives of this section include prevention of unauthorized physical access, damage, and interference with IoT's information and premises, as well as prevention of loss, damage, theft or compromise of assets and interruption to the activities and operations of IoT devices and systems. All the equipment and processing facilities should be placed in secure areas and protected from physical and environmental threats. The functional requirements of this matter are listed in Fig. 4.

Privacy Protection - Personally identifiable information (PII) needs to be protected, according to the European General Data Protection Regulation (GDPR) regulations [29]. Privacy protection is also advisable to increase trust in the internet (see Fig. 5 for practical requirements).

Operations Security - Information processing facilities should ensure correct and secure operation, including protection against attacks. Further, accountability auditing must be enabled for all events to ensure the integrity of operational systems, and prevent against exploitation of technical vulnerabilities. See Fig. 6.

- *Logging and Monitoring:* IoT products should have suf-

Fig. 6: Operations Security.

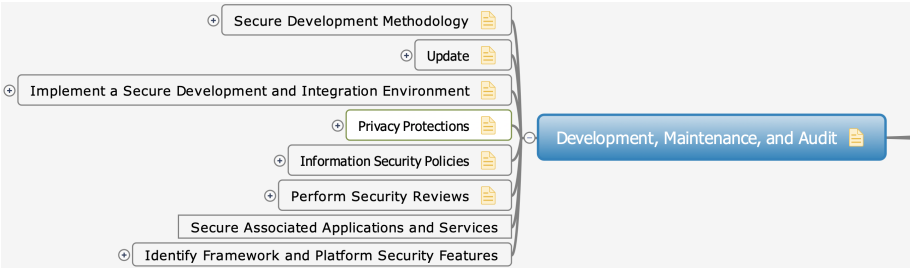


Fig. 7: Development, Maintenance, and Audit.

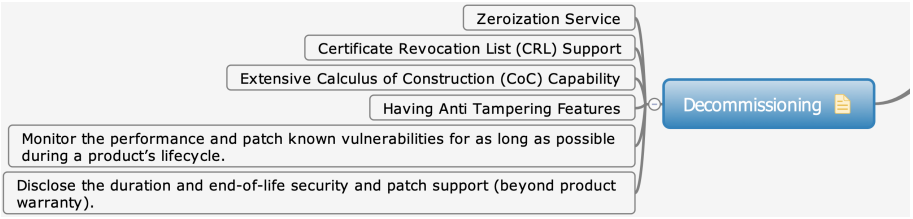


Fig. 8: IoT Security and Privacy Functionality Framework - Decommissioning.

ficient observations of occurrences happening on the device. For instance, connection requests, authentications (successful or failed), physical tamper, account updates, etc. It is essential to be able to monitor users' interaction with the system or a device, and in particular when they fail to login. Therefore, to detect possible security and integrity errors or potential threats, data should be captured on the entire state of the system from the endpoints, connectivity traffic and verifying the device behavior, in addition to analysing it.

- *Security Configuration and Management:* Includes the control of modifications to the operational functionality of the system (which covers reliability and safety behaviors) along with the security controls ensuring its protection,
- *Trust and Integrity Management:* Some of the practices in this matter include the following.
  1. Establishing trust in the boot environment before anything else since both the main hardware components and the operating system have been initialized by the boot process,
  2. Signing code cryptographically to prevent tampering,
  3. Controlling the installation of software on operating systems to prevent loading unauthorized software and files onto it, etc.
- *Management of Security Vulnerabilities and/or Incidents:* To ensure a quick, effective and orderly response to information security incidents, management procedures should be established. To address identified vulnerabilities, disclosure of vulnerabilities should be coordinated. Participate in information sharing platforms, in order to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners, is recommended.

Development, Maintenance, and Audit - To ensure that security controls are efficient, audits and reviews for security controls should be organized periodically. Penetration tests also should be done regularly. Good practices in this area are shown in Fig. 7.

- *Secure Development Methodology:* Documentation, peer reviews, and incorporating security requirements into the product life cycle should be included, in addition to the technological checks. Additionally, essential feedback loops should be included in the engineering process to create more secure IoT products.
- *Update:* Ensuring a secured system update is probably one of the biggest challenges in an IoT life cycle. While initial systems are subject to secure testing on both the producers and the customers, a similar awareness is often missing for system updates. In the absence of sufficiently secured update, an intruder may change legitimate software and firmware, and put new malicious software and firmware into the device. Malicious software and firmware can disable security controls, apply new features or build data exfiltration mechanisms. End-to-end protection of software and firmware is essential to the whole life cycle. And so are permissions regarding the update process, the integrity of updates, and authentication of update transactions of software and firmware.

- *Information Security Policies:* Regulatory, organizational and machine levels of security are covered here. The purpose of security in a system come as a security policy, and the security model represents security policies which should formally apply to the system. A security model and policy should state how to protect endpoints, communications and data, and specify what should be monitored, and analyzed, etc.
- *Perform Security Reviews:* Continuous feedback loops (i.e., the link connecting design, development, and test) and optimization during the life cycle of an IoT product are essential in this practice area. Identified faults/vulnerabilities have to go back to the design and threat modeling process, hardware and software baselines must be updated accordingly, and then be tested again to make sure that the patches do not identify new vulnerabilities. These vulnerabilities might be detected using IoT device security testing processes. Tests like Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST) are a recommendation.
- *Secure Associated Applications and Services:* Applications (Apps) and services connected to IoT devices must be developed securely. Configuring IoT devices, or interacting with IoT devices are usually being done using smartphone apps. These apps also create gateway functionality to transfer data from IoT devices to the cloud. So developers must use security credentials in order to provide authenticated and integrity protected communications to IoT devices.
- *Implement a Secure Development and Integration Environment:* A framework, addressing both physical and IT-security, is required to ensure a controlled environment for software and hardware development.

Decommissioning - To prevent exposing critical information to any possible attacker, the product must be disposed in a secure way at the end of life time. Therefore, secure devices should not be placed into the supply chain again. A low-cost and high-guaranty way to decommission can be provided by an automated decommissioning procedure. We show the practical considerations of decommissioning in Fig. 8.

V. Security Classification

Concepts of security classes have been suggested and defined in [4], [25]. In this section, we briefly touch on these concepts to give an overview. There are six classes of security, from A to F, with A representing the best security and F representing the least security. Further, we based these security classes on the *exposure* and the *impact* factors of the possible attacks on the system (see Fig. 9 and Table I). A lower exposure level means a lower attack surface. Therefore, attacks that have low exposure are relatively safe and vice-versa. The high impact of attacks on a system affects the security class of the system, and necessary precaution should be considered to protect the system. Consequently the security class of the

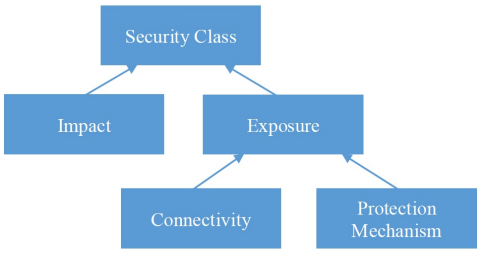


Fig. 9: Basic Inputs for Defining a Security Class [25]

system will increase. A system with low exposure and low impact is relatively safe.

Impact is a consequence of the possible attacks on a system. When a system is compromised, it can have an impact on several sectors beyond the system itself, including business, government, or society. We divided this *impact* into five levels, namely, Insignificant, Minor, Moderate, Major, and Catastrophic. Defining each of these levels depends on the system under evaluation, the type of impacts it can have (e.g. financial, social), or the application area. Therefore, we base the security classification level assigned to the system on the security/risk analyst responsible for that particular application or system discretion.

Exposure (see Table II) is a consequence of connectivity and the protection level of a system. According to the connectivity of the system, an appropriate set of security and privacy functionalities is identified to protect the system, while the strength of the identified security and privacy functionalities determines the protection levels (i.e., for authentication we can use passwords or PINs or two/multi-factor authentication). The definition of the protection levels (P1 to P5) is according to the ISA99 standard. However, the protection level evaluation depends on the expert and the particular scenario considered. The connectivity is divided into five levels, C1 to C5, according to ANSSI [4]:

- (C1): a closed and isolated Information & Communication System (ICS)
- (C2): an ICS connected to a corporate Management

TABLE I: Security Classes (from [25])

Impact	E1	E2	E3	E4	E5
Catastrophic	Class A	Class D	Class E	Class F	Class F
Major	Class A	Class B	Class D	Class E	Class F
Moderate	Class A	Class B	Class C	Class E	Class E
Minor	Class A	Class B	Class B	Class C	Class D
Insignificant	Class A	Class A	Class A	Class B	Class C

Exposure

TABLE II: Exposure (from [25])

Protection	C1	C2	C3	C4	C5
P1	E4	E4	E5	E5	E5
P2	E3	E3	E4	E4	E4
P3	E2	E2	E3	E3	E3
P4	E1	E1	E2	E2	E2
P5	E1	E1	E1	E1	E1

Connectivity

Information System (MIS) for which operations from outside the network are not allowed
- (C3): an ICS connected to wireless technology.
- (C4): an ICS with *private* infrastructure permitting operations from outside (VPN, APN, etc.)
- (C5): a distributed ICS with *public* infrastructure.

Increasing the protection level or reducing the connectivity level can reduce the exposure (see Table II). From Tables I and II we observe that by keeping the protection level in the highest level (P1 is the lowest and P5 the highest protection level), exposure will be in the lowest level (E1), therefore resulting in the highest security class. And the way we can provide the highest protection level is by applying an effective and appropriate set of security and privacy functionality criteria in a particular device, for instance, use of multi-factor authentication instead of just passwords or PINs for authentication. Adequate and proper sets of security and privacy functionality criteria used in the case study have been taken from our framework.

VI. Pacemaker Case Study

We have built a methodology for looking at the functionalities from both security and privacy points of view. In order to understand how we can use the functionality framework to improve security and privacy of IoT systems in practice, we here use a case study of health products involving a pacemaker and related control units such as a mobile phone and a heart rate sensor. In the domain of health services, the highest security class is recommended for devices like pacemakers that directly control life functions of a patient.

A pacemaker is a medical device that is implanted under the skin to help with abnormal behaviors of heartbeats [14], [7]. It consists of a battery, a computerized generator, and wires with sensors at their tips [13]. The generator is powered by the battery, and both are surrounded by a thin metal box. The generator is connected to the heart by the wires. The pacemaker helps to monitor and control the heartbeat. The sensors detect the heart's electrical activity and send data through the wires to the computer in the generator. If the heart rhythm is abnormal, the generator will be directed by the computer to send electrical pulses to the heart, and the pulses travel through the wires to reach the heart. Embedded microprocessors in modern pacemakers have enabled them to do additional tasks like monitoring heart activity and providing a record for the patients and their healthcare providers, as well as collecting data on heart functions to help doctors to identify and diagnose patient conditions, and send required shock signals when needed. Doctors can monitor the patient's heart activities and control the pacemaker using a mobile phone or a computer device, or send required shock signals in case of observation of abnormal behavior.

Beside threatening patients' lives, malicious attackers can get access to patients' medical records through a pacemaker [30], [28], or track a patient's location. In addition, malicious software can be run on pacemakers and cause security and privacy breaks. Therefore, any security or functional weakness can result in a security failure. Like any device that uses remote technology, pacemakers are also vulnerable against cyber attacks, and hackers can break into the pacemaker itself, the back-end systems or the communication between the pacemaker and its surrounding. By breaking into a pacemaker, an attacker can send strong shock signals, disturb the pacemaker setting or heart functions, or disturb them from working properly. One simple example of hacking into a pacemaker is to change the setting from battery-saving "sleep" mode to "standby" mode, and this can quickly drain the battery, which is normally supposed to last for years. Furthermore, an attacker can steal private and personal information of a patient from the device that for instance can later track the patient's location. Hence, security in this kind of device is crucial and should have the highest (best) security class, meaning security class A.

We will below discuss the security and privacy challenges for each of the three devices. In each case we discuss connectivity, protection level and relevant functionality criteria. We use the general criteria given in the functionality framework, select and discuss the parts relevant for each device.

Pacemaker Security Controller. We consider Connectivity 2 (explained in Section V) for the pacemaker security controller, since it is only connected to the pacemaker. We define below the protection levels which are relevant for the pacemaker security controller:

- Protection Level 1 (P1): includes secure authentication, securing software/firmware, secure communication, and human interface security. For authentication we consider: requiring passwords, option to change the default username and password. For communication we consider: data authenticity to enable reliable exchanges from data emission to data reception. For securing software/firmware we consider: update capability for *some* of the system devices and applications, transmitting the files using encryption.
- Protection Level 2 (P2): includes P1 and in addition, for authentication: requiring strong passwords, securing password recovery mechanisms, making sure that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed. For communication: verifying any interconnections, discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services, prevent unauthorised connections to it or other devices the product is connected to, at all protocol levels, providing communication security using state-of-the-art mechanisms, standardising security protocols, such as TLS for encryption. For securing software/firmware: encrypting update files for *some* of the applications.
- Protection Level 3 (P3): includes P2 and in addition, for authentication: having options to force password expiration after a specific period, and to change the default username and password, making sure that the password

recovery or reset mechanism are robust and do not supply an attacker with information indicating a valid account. The same should apply to key update and recovery mechanisms. For communication: data authenticity to enable reliable exchanges from data emission to data reception.
- Protection Level 4 (P4): includes P3 and in addition, for authentication: implementing two-Factor Authentication (2FA), making sure that default passwords and even default usernames are changed during the initial setup. For communication: signing the data whenever and wherever it is captured and stored, making intentional connections, disabling specific ports and/or network connections for selective connectivity. For securing software/firmware: capability of quick updates when vulnerabilities are discovered for *some* of the system devices and applications, and offering an automatic firmware update.
- Protection Level 5 (P5): includes P4. In addition, for authentication: using Multi-Factor Authentication (MFA) (considering biometrics for authentication), considering Certificate-Less Authenticated Encryption (CLAE), and User Managed Access (UMA). For communication: rate limiting – controlling the traffic sent or received by a network to reduce the risk of automated attacks. For securing software/firmware: update capability for *all* system devices and applications, capability of quick updates when vulnerabilities are discovered for *all* system devices and applications, encrypting update files for *all* applications, signing update files and validating by the device before installing, securing update servers, having ability to implement scheduled updates, having backward compatibility of firmware updates.

According to Tables I and II, we might have protection levels 2, 3, 4, or 5 to obtain security class A; however we choose to use protection level 3 since it is a realistic level in this case. A higher level would be costly, and P2 would give poor protection. We therefore consider how to obtain that protection level, and select the following set of relevant functionality criteria from the functionality framework, adapted to the challenges of pacemakers. In this selection we have used the guidelines for securing pacemakers from [12]. This gives a certain guarantee that we cover all relevant aspects.

- *Secure Authentication/Authorization*: Access to the pacemaker security controller and mobile phone connected to the doctor, should be limited using the authentication of users (for example user ID and password, Personal Identification Numbers (PINs), biometric authentications). Authorization refers to checking necessary permissions of an identified individual to do an action. Authentication and authorization are completely related to each other. Authorization checks should immediately be followed by authentication of a request. In order to have secure authorization, the roles and permissions of the authenticated user should only be verified through information in backend systems, not through roles or permission information coming from the device. Any incoming identifiers with a request alongside should be verified by backend code independently. Failure in a secure authentication/authorization would give access to unauthorized people and could lead to reputational damages, fraud, unauthorized access to information, information theft, and modification of data.
- *Securing Software/Firmware*: Before any software or firmware update, user authentication or other suitable controls should be required. Software/firmware updates should be restricted to authorised code. Manufacturers may consider code signature verification as an authentication method.
- *Secure Communication*: Data transmission between the pacemaker security controller and the mobile phone connected to the doctor must be secure enough so that a third party cannot listen to their communication. The communication should not be vulnerable to eavesdropping or interception. Failure in having a secure communication can cause identity theft, fraud, data modification, privacy information leakage. One should consider strong handshaking, correct SSL versions, no clear-text communication of sensitive assets, etc.
- *Human Interface Security*: Patients should be trained about the importance of security and privacy and how to use the pacemaker properly to ensure security is managed at an appropriate level. For instance, if we consider all the security protections in the highest level in the security controller, but the patient does not know how to deal with error notifications (restart, turn off or low battery errors) in the security controller, all the security considerations in the controller will be useless.
- *Data Privacy*: Measures to avoid risk of breaches in connection with long term storage of private information, handling of encryption of private information, and GDPR compliance including consent, purpose, and access rights.

The final discussion of the security class of the pacemaker system depends on the scenario chosen and the other components involved. We next consider the mobile phone.

Mobile Phone. In our case study, a mobile phone is used in the communication between the pacemaker and the healthcare provider/doctor. Security in this mobile phone is then important in order to send correct data to/from the pacemaker controller. Hacking or tampering into this mobile phone can result in sending wrong data from the pacemaker to the doctor, something that could result in wrong decisions from the doctor, or possibly sending inappropriate shocks to the patient's heart.

Therefore, it is important to secure the mobile phone properly. However, the security class of the mobile phone is only considered class B, since mobile phones are inherently not of the highest security class and have a number of possibilities for attacks due to high exposure. For instance, because of all the applications and browsers on the device, as well as software developed by third parties. Therefore, both the impact of attack as well as the connectivity are in a higher level for the mobile phone compared to the pacemaker. Hence the security class

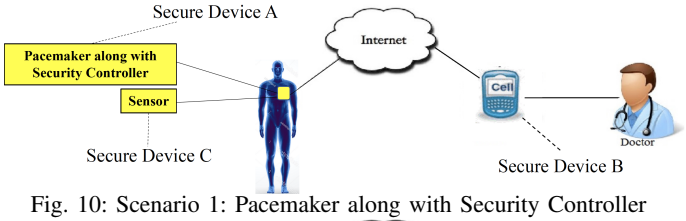


Fig. 10: Scenario 1: Pacemaker along with Security Controller

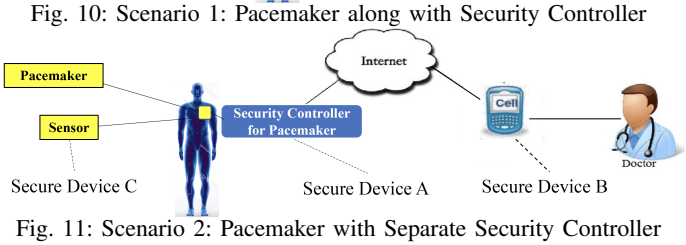


Fig. 11: Scenario 2: Pacemaker with Separate Security Controller

of the mobile phone is lower than the security class of the pacemaker security controller.

We consider C4 in the mobile phone connected to the doctor. According to Tables I and II, we might have protection levels 2, 3, or 4 to obtain security class B, however since mobile phones naturally have moderate impact of attacks as discussed above, we should use protection level 4 in order to reach security class B. So based on that the following set of relevant security and privacy functionality criteria are selected to ensure that the mobile phone has a sufficiently high protection level, following the functionality framework and the OWASP guidelines for securing mobile phones [19]:

- *Secure Authentication/Authorization* and *Secure Communication*: are the same as what we discussed for the pacemaker security controller.
- *Sufficient Cryptography Techniques*: Appropriate cryptography techniques should be considered for instance using AES instead of DES.
- *Code Tampering*: When an application is on the device, the code and data resources are also available there. An attacker modify the code through either malicious apps in third party app stores or trick the user via phishing attacks and install the app on the device. Code tampering could result in revenue loss due to piracy, reputational damage, unauthorized new features, identity theft or fraud.
- *Secure Data Storage*: Failure in having secure data storage can result in data loss, extraction of sensitive data using malware, modified apps or forensic tools, identity theft, fraud, reputation damage, material loss or external policy violations.
- *Proper Platform Usage*: Misuse of a platform feature or failure to use platform security controls fall under this category. Android intents, platform permissions, misuse of TouchID, Keychains, or other security controls which are part of the operating system could be included. To prevent the attacks in this category, secure coding and configuration practices must be applied on the server side of the application.
- *Data Privacy*: are as discussed above for the pacemaker security controller.

We next consider the protection levels of ISA99, and select the relevant criteria from the functionality framework, and adjust them for the case of the mobile phone connected to the doctor. These are defined below:

- Protection Level 1 (P1): includes secure authentication, secure authorization, securing software/firmware, sufficient cryptography techniques, code tampering, secure data storage, secure communication, and proper platform usage. Secure authentication, securing software/firmware, and secure communication are the same as the considerations for protection level 1 for the pacemaker security controller.
- Protection Level 2 (P2): includes P1. Secure authentication, securing software/firmware, and secure communication are the same as the considerations for protection level 2 for the pacemaker security controller. In addition, for cryptography techniques we should consider: ensuring proper selection of standard encryption algorithms and keys.
- Protection Level 3 (P3): includes P2. Secure authentication, securing software/firmware, and secure communication are the same as the considerations for protection level 3 for the pacemaker security controller. In addition, for cryptography techniques we should consider: strong encryption algorithms, strong keys.
- Protection Level 4 (P4): includes P3. Secure authentication, securing software/firmware, and secure communication are the same as the considerations for protection level 4 for the pacemaker security controller. In addition, for cryptography techniques we should consider: verifying the robustness of the implementation, establishing secure and scalable key management. And cryptographic keys must be securely managed.
- Protection Level 5 (P5): includes P4. Secure authentication, securing software/firmware, and secure communication are the same as the considerations for protection level 4 for the pacemaker security controller. In addition, for cryptography techniques we should consider: disabling insecure protocols.

Finally, the security class of the heart rate sensor in our case study is considered below.

Heart Rate Sensor. The heart rate sensor does not have any external connectivity; it has only connections to the heart and computerized generator inside the pacemaker in order to transfer the captured heart rate from the heart to the pacemaker generator. So the connectivity in the sensor is C1. Furthermore it has only a chip set from the company provider. Hence, the sensor has the least chance of attack. However, there is still a possible vulnerability if the wired connection is not sufficiently shielded and allows eavesdropping by inductive sensors or senders. But this requires very short physical distance. Therefore we may assume only minor impact, and do not need a high protection level for this device, and may use P1. Exposure is then E4 (see Table IV). This gives security class C.

Pacemaker scenarios. The challenge in the case study is how

TABLE III: Security and Privacy Challenge Comparison of Scenario 1 and 2

	Security and Privacy Challenges	Scenario 1	Scenario 2
In Sensor	Draining battery by changing battery saving controls		
	Interrupting into heartbeat capturing		
	Data and private information breaches		
In Pacemaker	Sending/Receiving wrong data to/from mobile phone connected to the doctor		
	Changing pacemaker shock settings		
	Draining battery by changing battery saving controls		
	Higher battery usage		
	Data and private information breaches		
	Transparency of GDPR compliance		
	Risk of long-term storage of private information		
In Mobile Phone Connected to the Doctor	Sending/Receiving wrong data to/from pacemaker		
	Sending wrong unnecessary/necessary shocks		
	Changing pacemaker shock settings		
	Draining pacemaker battery by changing battery saving controls		
	Data and private information breaches		
	Transparency of GDPR compliance		
	Risk of long-term storage of private information		

Severity of Challenge: Insignificant: Minor: Moderate: Major: Catastrophic:

to implement the security controls like decryption, authentication, etc. For instance, whether to do data decryption in the mobile phone, and then send the decrypted data to the pacemaker. If the mobile phone is compromised, wrong data and signals could then go to the doctor and pacemaker, since mobile phones can get compromised, as we discussed before. Whereas, if we consider security controls in the pacemaker itself, we only have software provided by one company. Thus it would be much more secure to do the security controls directly in the pacemaker, and use the mobile phone just as a gateway to transfer the information. However, this will require additional computational power and battery capacity. Another issue is whether we can do all the security controls inside the computerized generator of the pacemaker - or consider a security controller as a separate unit out of the body with a close and secure connection to the pacemaker.

We therefore define two scenarios: In scenario 1 (see Fig. 10), the security controls for the pacemaker are done inside the computerized generator of the pacemaker, and in scenario 2 (see Fig. 11), a separate security controller unit makes the security controls of the pacemaker, such that this unit is outside the body with a close and secure connection to the pacemaker. In scenario 1, we would need computational power inside the body, needing more storage, stronger CPU, much more battery capacity and so on. This is not desirable since it might increase the potential necessary surgeries in order to change the battery, maintain, or update the pacemaker. Moreover, we might not be able to consider some of the security and privacy functionalities in order to avoid increasing CPU usage, which results in even more battery usage.

Therefore, we might want to have a pacemaker with a simple sensor inside the body and a security controller out of the body, say in the pocket or at home very close to the pacemaker. Here, it is essential that the security controller be close to the pacemaker, since the pacemaker must have very weak signals, limited interactions and computations, to avoid using too much battery power and resulting battery changes. So, all the security and battery-intensive controls would be done in the external security controller, which can have a stronger and easily rechargeable battery. The controller can maintain the device in case of any problem, update or troubleshoot its computer system, or even increase the level of protection by adding more security and privacy functionalities or appropriate software at any time because of easy access.

According to all the security considerations in scenario 2, we can then have a better security class in the pacemaker security controller: In Table III we summarize all the security and privacy challenges in the sensor, pacemaker, and mobile phone connected to the doctor, and compare the severity of these security and privacy challenges in scenarios 1 and 2. This table determines the impact. The challenges considered in the table are found by following the functionality framework, for each device, in a top-down manner and in each case determining the problems that may occur. The further we break down the problems according to the functionality framework, the easier it is to find the specific challenges for the given device.

In the following, we see that the severity of the security and privacy challenges in the sensor and pacemaker has been reduced from very high in the worst case to low. Hence, the impact of attacks is reduced from catastrophic to minor.

Discussion. The pacemaker in scenario 1 is a complex device because all security controls are done inside the computerized generator of the pacemaker. The security controller is very close to the sensor, the signals received by the sensor from the pacemaker are very frequent. Interference is possible and that can have negative effect on correct heartbeat capturing. However, by transferring the security controller outside of the body this effect would be low (still there are some frequencies from devices close by such as mobile phones that can affect

the sensor) resulting in more precise heartbeat capturing. As mentioned earlier in the heart rate sensor, there are low possibilities of data and private information breaches in both scenarios.

In the pacemaker in scenario 1, because of the complexity of the system and having all the security controls inside the computerized generator of the pacemaker, we need higher CPU and memory consumption and then battery usage would be very high, while in scenario 2 this problem would decrease to very low. In scenario 1, because of difficulties in accessing the pacemaker and its security controller on time (in case of maintenance, update, troubleshooting or installing new software/equipment, also not being able to apply all the necessary criteria with high protection level in order to avoid high battery usage), the level of the security and privacy functionality criteria as well as the level of the protection is low.

Therefore the vulnerability of the pacemaker and sensor against attacks compromising the device (that can cause changing battery saving controls so draining the battery more quickly, changing pacemaker shock settings, tampering of transferred information from/to the pacemaker, data and private information breaches, transparency of GDPR compliance, risk of long-term storage of private information) is high; however, this problems decrease to very low when we change to scenario 2, due to easier access to the security controller out of the body.

By compromising the mobile phone connected to the doctor, the problems listed in the last part of Table III may occur. In both scenarios, we have considered high level of protection for the mobile phone by using appropriate set of security and privacy functionality criteria with high protection level,

TABLE IV: Security Class of the Sensor

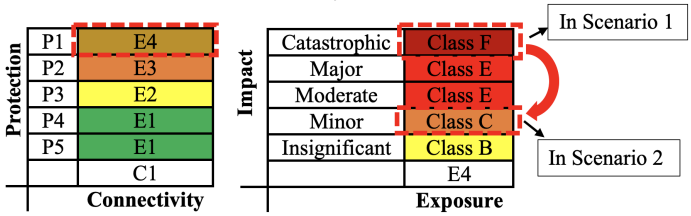


TABLE V: Security Class of the Pacemaker Security Controller

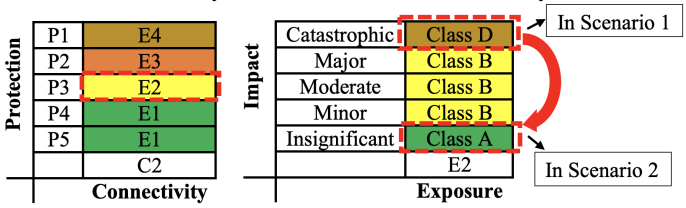
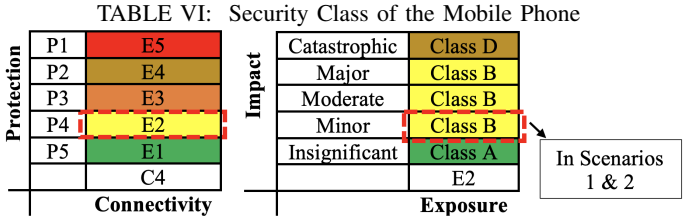


TABLE VI: Security Class of the Mobile Phone



therefore we have reduced the vulnerability of the device to low, but as discussed earlier, these devices still have a number of vulnerabilities for attacks, and therefore the vulnerability is not in a very low level.Furthermore, softening the problems in scenario 1 results in obtaining higher protection level and security class. For instance, we can easily recharge the battery of the security controller, maintain the device in case of any problem to avoid shutting down all the security considerations, and increase the level of protection by updating or troubleshooting its computer system..

In the sensor, as explained above, we have connectivity C1, and protection level P1, therefore exposure is E4 (see Table IV), and because of very high problem severity, the impact of attacks is Catastrophic, resulting in security class F in this device. By changing from scenario 1 to 2, the severity of the security and privacy challenges has reduced from very high to low, therefore the impact of attacks is reduced from Catastrophic to Minor, and consequently, the security class has improved from class F to class C.

In the pacemaker, we have connectivity C2, and protection level P5, however in scenario 1, the severity of security and privacy challenges have affect on the protection level, which falls to level 3, therefore exposure is E2 (see Table V), and because of very high security and privacy challenge severity, the impact of attacks is Catastrophic, then we have security class D in this device. By changing from scenario 1 to 2, the severity of the security and privacy challenges has reduced from very high to very low, therefore the impact of attacks has reduced from Catastrophic to Insignificant, and consequently, the security class has improved from class D to A.

And, in the mobile phone connected to the doctor, we have connectivity C4, and protection level P4, therefore the exposure is E2 (see Table VI), and the security is class B in both scenarios. By considering security and privacy challenges, as well as the effect of these challenges on the protection level of each device and the whole system, and also their affect on the impact of attacks, we have changed scenario 1 to 2, and were able to improve the security class in the sensor and pacemaker security controller from class F to C, and class D to A, respectively. Hence the security of the overall system has improved significantly.

In this case study, we started out with security and privacy design requirements to each device: class A for the pacemaker security controller, class B for the mobile phone, and class C for the sensor. We have seen that this is not realistically possible to achieve for the design of scenario 1, while it was possible to satisfy these requirements for scenario 2. The framework was most useful in these design evaluations. Indeed, the case study shows that by following the guidelines given by our framework, one can achieve security easily and decrease the impact of a possible attack.

VII. Conclusion

The expansion of IoT in the last decade has resulted in several security and privacy issues and attacks against things and people. Unfortunately, the security and privacy

functionalities to combat these attacks are not well-recognized in the domain of IoT. This paper summarizes and categorizes IoT security and privacy functionalities, and as the main contribution, the paper presents a new taxonomy framework that organizes the related standards in this area. The proposed framework is oriented towards practical application. We have demonstrated the application of this framework in combination with the security classification method using a case study about pacemakers. Our case study is quite generic and reveals general issues that can be found in other case studies.

The security class of a system is based on two factors: exposure and impact of possible attacks. The exposure is a consequence of the protection level of the system and its connectivity. A lower exposure level means a lower attack surface. Therefore, by reducing the exposure level of a system we can have a more secure system. A higher protection level in a system or lower connectivity can result in lower exposure. At the same time, lower impact of attacks on a system raises the security class of the system. By applying the appropriate set of security and privacy functionality criteria from our framework, the protection level of a system can increase, while exposure can decrease, as demonstrated by the case study and discussed at the end of Section VI.

The main objective of this paper is to give security developers, designers, and end-users an opportunity to understand and explore what the IoT security and privacy functionalities are, and how these functionalities can help to improve the security and privacy of IoT systems. Our approach combines detailed information about security and privacy functionalities with a security classification method. The approach is systematic and structured; it is easy to use and is oriented towards practical engineering. The framework is based on the available recommendations and standards for IoT systems. This should imply that all aspects are covered, but there is no guarantee for that. This can be seen as a limitation of the work. Secondly, the application of the methodology is ultimately depending on the judgements of software engineers or security experts, and is therefore not 100% precise. If their judgement is wrong, for instance if they choose the wrong connectivity or protection level, it will in general give a wrong estimate.

Future work will consider case studies with several kinds of IoT devices and sensors involved. This will be a valuable step toward validating our framework, and possibly allowing the framework to be complemented with even more elements.

REFERENCES

[1] 27000, I.: Information technology — security techniques — information security management systems — overview and vocabulary (fourth edition). ISO/IEC 2016 (2016)

[2] 27001, I.: International standard iso/iec 27001 information technology—security techniques —information security management systems —requirements. ISO/IEC 2013 (2013)

[3] Alqassem, I., Svetinovic, D.: A taxonomy of security and privacy requirements for the Internet of Things (IoT). In: 2014 IEEE Intern. Conf. on Industrial Engineering and Engineering Management (IEEM). pp. 1244–1248. IEEE (2014)

[4] ANSSI: Classification method and key measures (2014), https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf

[5] Babar, S., Mahalle, P., Stango, A., Prasad, N., Prasad, R.: Proposed security model and threat taxonomy for the Internet of Things (IoT). In: Intern. Conf. on Network Security and Applications. pp. 420–429. Springer (2010)

[6] BITAG: Internet of Things (IoT) security and privacy recommendations. (2016), https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[7] Boulos, P., Sargolzaei, A., Ziaei, A., Sargolzaei, S.: Pacemakers: a survey on development history, cyber-security threats and countermeasures. Int. J. Innov. Stud. Sci. Eng. Technol **2**(8) (2016)

[8] Future-proofing the connected world: 13 steps to developing secure IoT products (2016), https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

[9] ENISA: Baseline security recommendations for IoT in the context of critical information infrastructures. European Union Agency for Network and Inf. Sec. (2017)

[10] ENISA: Guidelines for SMEs on the security of personal data processing (2017), https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

[11] Fazeldehkordi, E., Owe, O., Noll, J.: Security and privacy functionalities in the Internet of Things (long version). Tech. rep., Dept. of Informatics, Univ. of Oslo (2019), https://its-wiki.no/wiki/IoTSec:Security_and_Privacy_Functionality

[12] FDA: Content of premarket submissions for management of cybersecurity in medical devices guidance for industry and food and drug administration staff. U.S. Food and Drug Administration (FDA) (2014)

[13] of Health & Human Services, U.D.: Pacemaker (2019), https://www.nhlbi.nih.gov/health-topics/pacemakers

[14] Healthline: Heart pacemaker (2019), https://www.healthline.com/health/heart-pacemaker

[15] Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S.: The Internet of Things for health care: a comprehensive survey. IEEE Access **3**, 678–708 (2015)

[16] Lee, C., Zappaterra, L., Choi, K., Choi, H.A.: Securing smart home: Technologies, security challenges, and security requirements. In: Communications and Network Security (CNS), 2014 IEEE Conf. on. pp. 67–72. IEEE (2014)

[17] MacGillivray, C., Turner, V., Lund, D.: Worldwide Internet of Things (IoT) 2013–2020 forecast: Billions of things, trillions of dollars. International Data Corporation (2014), http://www.idc.com/getdoc.jsp?containerId=243661f

[18] OWASP: IoT security guidance, https://www.owasp.org/index.php/IoT_Security_Guidance

[19] OWASP: OWASP mobile security project, https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

[20] Pang, Z.: Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being. Ph.D. thesis, KTH Royal Institute of Technology (2013)

[21] Pishva, D.: Internet of Things: Security and privacy issues and possible solution. In: Advanced Communication Technology (ICACT), 2017 19th Intern. Conf. on. pp. 797–808. IEEE (2017)

[22] Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. Computer **44**(9), 51–58 (2011)

[23] Ross, R., Viscuso, P., Guissanie, G., DEMPSEY, K., Riddle, M.: Protecting controlled unclassified information in nonfederal information systems and organizations. NIST Special Publication **800**, 171 (2015)

[24] Schrecker, S., et al.: Industrial Internet of Things volume G4: Security framework. Industrial Internet Consortium (2016), https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

[25] Shrestha, M., Johansen, C., Noll, J.: Security classification for smart grid infra structures (long version) (2017)

[26] Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in Internet of Things: The road ahead. Computer networks **76**, 146–164 (2015)

[27] Suo, H., Wan, J., Zou, C., Liu, J.: Security in the Internet of Things: a review. In: Computer Science and Electronics Engineering (ICCSEE), 2012 Intern. Conf. on. vol. 3, pp. 648–651. IEEE (2012)

[28] Thehackernews.com: Over 8,600 vulnerabilities found in pacemakers, https://thehackernews.com/2017/06/pacemaker-vulnerability.html

[29] Union, E.: Regulation (EU) 2016/679 of the european parliament and of the council, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[30] www.foxnews.com: Heart alert: Pacemakers can be hacked (2018), http://www.foxnews.com/health/2018/02/21/heart-alert-pacemakers-can-be-hacked-new-research-shows.html