A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges

Maaike Harbers
Ministry of Security and Justice
Rotterdam University of Ap. Sc.
m.harbers@hr.nl

Mortaza S. Bargh
Ministry of Security and Justice
m.shoae.bargh@minvenj.nl

Ronald Pool
Ministry of Security and Justice
r.l.d.pool@minvenj.nl

Jasper van Berkel
Ministry of Security and Justice
j.j.van.berkel@minvenj.nl

Susan van den Braak
Ministry of Security and Justice
s.w.van.den.braak@minvenj.nl

Sunil Choenni
Ministry of Security and Justice
Rotterdam University of Ap. Sc.
r.choenni@minvenj.nl

Abstract

The Internet of Things (IoT) is rapidly growing, and offers many economical and societal potentials and benefits. Nevertheless, the IoT also introduces new threats to our Security, Privacy and Safety (SPS). The existing work on mitigating these SPS threats often fails to address the fundamental challenges behind the mitigation measures proposed, and fails to make the relations between different mitigation measures explicit. This paper, therefore, offers a conceptual framework for understanding and approaching the challenges and obstacles that arise in addressing the SPS threats of the IoT. This contribution aims to help policymakers in adopting policies and strategies that stimulate others to develop, deploy and use IoT devices, applications and services in secure, privacy-friendly and safe ways.

1. Introduction

The Internet of Things (IoT), a network of (smart) devices, sensors and other objects, is rapidly growing and increasingly affecting our society. The World Economic Forum predicts that the IoT will contain 20 to 30 billion objects in 2020 [63], where objects can range from toothbrushes and lamps to buildings and roads. The IoT has all kinds of potentials and benefits. For instance, it can improve health by monitoring patients' activity and food consumption patterns [30], increase productivity by increasing the efficiency of manufacturing processes [60], and support sustainability by saving energy through smart meters [27].

The IoT, however, also introduces threats to our Security, Privacy and Safety (SPS). Security threats entail cybercrimes such as breaking into, and taking over IoT devices, and stealing data. Privacy threats arise because (sensitive) data are used for purposes other than they were collected for. Safety threats come with system failures because of dysfunctional IoT devices. As the IoT expands, the consequences of these threats, which are mostly not specific to the IoT, will increase. The fast and ad-hoc growth of IoT products and services makes it difficult for system designers (concerning the technical aspects) and policymakers and legislators (concerning the non-technical aspects) to foresee and devise mechanisms that guarantee responsible use and development of IoT systems. Yet, if IoT threats are not addressed by adequate mitigation measures, the IoT can inflict major physical, mental and monetary damages [47].

The IoT consists of different components (software, hardware, infrastructure), is applied in many different domains (e.g., healthcare, logistics, agriculture), and involves multiple stakeholders (e.g., manufacturers, service providers and consumers). Therefore, in order to design an integrated set of mitigation measures for IoT SPS threats, an in-depth analysis of the threats and their possible countermeasures is needed. The literature offers several accounts that address the mitigation of IoT SPS threats, both from a technical and policy-based perspective. Most of the works proposing mitigation measures, however, only provide a list of measures, but fail to address how these measures are related to each other and what the obstacles are in implementing them (e.g., [16][18][28]).

In this paper, we offer a conceptual framework for understanding and approaching the technological and non-technological challenges and obstacles that arise in addressing SPS threats. The non-technological challenges and measures framed in this contribution are at a strategic, policymaking and governance level.

URI: http://hdl.handle.net/10125/50166
ISBN: 978-0-9981331-1-9

By this, the proposed framework aims at helping policymakers to adopt policies and strategies that stimulate others (e.g., service providers, manufacturers, and consumers) to develop, deploy and use IoT systems in secure, privacy-friendly and safe ways. Unlike other works, the conceptual framework presented in this paper models and captures the fundamental challenges that impede a successful deployment of the solutions proposed in the literature, and points out some solution directions to deal with these fundamental challenges.

This paper is based on research [8] performed by the WODC (Dutch abbreviation for Wetenschappelijk Onderzoek- en Documentatiecentrum, in English: Research and Documentation Centre) for the CSR (Dutch abbreviation for Cyber Security Raad, in English: Cyber Security Council). The WODC is the research center of the Dutch Ministry of Security and Justice, and the CSR is a national advisory body that provides solicited and unsolicited advice to Dutch policymakers and legislators on cyber security. Methods used to perform the research are: literature review, interviews and round-table discussions with experts and stakeholders in the Netherlands (for more detail, see [8]). The work focuses on the situation in the Netherlands, but we expect that many of the findings are applicable to other countries as well.

The outline of the paper is as follows. Section 2 provides a more comprehensive discussion of IoT SPS threats, and (technical) solutions for addressing these issues. Section 3 discusses related work on policy measures to mitigate SPS threats. Section 4 introduces a conceptual framework including four obstacles that impede addressing SPS threats and solution directions for overcoming these obstacles. Section provides a conclusion.

2. Background

This section discusses IoT SPS threats, and describes important measures that can be taken to design and deploy IoT systems in secure, privacy-friendly and safe ways. Some of these measures have critical issues, but those will be discussed in Section 4. The aim of this section is to provide a general overview of threats and solutions, and is by no means an exhaustive list of either of these.

Security threats are caused intentionally (in contrast to safety issues, which are caused unintentionally), and can be classified according to the so-called CIA triad: 1) confidentiality, 2) integrity, and 3) availability [59]. First, confidentiality threats involve unauthorized access to data of IoT systems, possibly leading to the collection of sensitive data, blackmail or digital espionage. Second, integrity threats concern unauthorized adaptation of settings and/or data of IoT systems, e.g., altering the setting of a pacemaker to increase someone's heartrate. Third, availability threats occur, for example, when a malicious person gains access to an IoT system by taking over the control of a self-driving car, demanding ransom to regain access to one's system, or taking out IoT networks through a distributed denial-of-service attack (DDoS attack; note that IoT objects can be used to carry out such attacks).

IoT systems collect large amounts of (personal) data, increasing the risk of *Privacy* threats. These issues can arise, for instance, when personal data are used by insurance companies for price discrimination, or by the police to determine someone's (risk) profile. The IoT can also be used by companies and authorities to continuously monitor people's behavior, which can be experienced as a privacy violation, and lead to behavior change. In addition, data might be used for other purposes than they were collected for (a so-called function creep). Data anonymization does not necessarily provide a solution to the problems described above, as supposedly anonymous data can often be de-anonymized by combining different data sets [47].

Safety threats, as mentioned above, are non-intentional [4]. Similar to security and privacy threats, safety threats originate from shortcomings in, e.g., the design, production, deployment, or maintenance of IoT objects. Other causes of safety issues include failing infrastructure or (unpredictable) emergent behavior due to the interaction between different IoT objects. Finally, IoT objects are not always adequately provided with software updates, which makes them more susceptible to security leaks over time.

Above described SPS threats should be considered during the whole lifecycle of an IoT system (i.e., before, during and after deployment). Before deployment, SPS threats should be accounted for in the design of IoT systems. This is often referred to as security, privacy, and safety by design [38]. When used for collection and storage of (personal) data, IoT devices can be made SPS-friendly, for instance, by adding features such as a delete button or an opt-out option. During and after deployment, it should be made sure that IoT devices are transparent, accountable and regularly provided with software updates [23].

During all stages of the product lifecycle, solutions should be used that are based on best practices, or if these are not available, on new or innovative practices that may turn into best practices. An example of such a practice is to deploy a layered defense strategy against SPS threats, ranging from user awareness to process procedures, so that SPS can still be guaranteed even if one of the layers fails [24]. Furthermore, the development and use of (international) standards and

guidelines to cover known issues promote SPS-friendly IoT systems. This requires public-private and international collaborations.

3. Related work

There are many survey articles that discuss IoT or IoT-related issues, and possible measures against them (e.g., [16][15][18][20][28][44][53][64][65]). Some of these articles have a different or narrower focus than the current contribution. Related papers address, for example, the Internet [64], big data [65], privacy protection [18], or cyber security [44].

Articles that specifically concern the IoT often have different aims. In 2015, the Dutch Ministry of Economic Affairs published a report that focuses on the technological trends and applications of the IoT [48]. In the same year, the European Parliament brought out a research report on the "opportunities and challenges" of the IoT [20][53], while the Internet Society published one on its "issues and challenges" [48]. The British Government Office for Science [28] and the Dutch CSC [16] both published a report proposing measures against IoT SPS threats. Although some of these papers review IoT issues and their solution directions based on some insightful taxonomies, they fail to account for the underlying obstacles, as we do in this contribution.

Some papers bring up obstacles such as lack of governance, incentives, and knowledge and education (also see Section 4). For example, Danezis and colleagues [18] mention these issues in the context of privacy engineering techniques in the general setting of ICT systems. However, they do not provide a link between the aforementioned obstacles in a directive way indicating an approach to address those fundamental issues and challenges.

4. Obstacles

Based on our study, we developed a conceptual framework of addressing IoT threats. Figure 1 provides a schematic overview of the framework. The top of the figure (dark gray boxes) shows that IoT SPS threats (top left) require adopting and developing SPS mitigation measures (top right), as discussed in Section 2. Below that, the figure shows four fundamental obstacles (middle dark gray boxes) in realizing and deploying these measures (IoT complexity, lack of awareness, lack of incentives, and lack of monitoring and enforcement), and the corresponding solution directions to address them (light gray boxes).

The explicated relations among the obstacles in the figure are the ones that we considered most important, but they are not the only ones possible. For example, an increase in complexity may increase the other obstacles. Facing obstacles (like lack of incentives and monitoring) properly, often call for new information needs. Implementation of these needs causes, in turn, an increase of the technical complexity. The relations in the figure thus do not necessarily imply causality.

The four obstacles and solution directions will be discussed in the following subsections. We view complexity as the main obstacle for taking effective SPS mitigation measures, involving multiple layers and reasons and, therefore, it is described in more detail than the other three obstacles. The first obstacle is technological of nature, and mainly requires solutions in the field of software and system engineering. The other three obstacles are procedural, and require policy-related solutions.

4.1. IoT Complexity

In this section we explain the reasons behind and the impact of IoT complexity (Subsection 4.1.1), and present a number of solution directions to deal with IoT complexity, particularly from the viewpoint of addressing its SPS threats (Subsection 4.1.2).

4.1.1. Reasons and impacts. IoT complexity stems from a number of reasons. First, the basic architecture of IoT systems is generally divided into four layers: the perception layer (representing the interaction with the physical world), the network layer (embodying global communication among system components), the middleware layer (enabling management and processing of sensory data and actuation signals), and the application layer (representing the provisioning of IoT services to (end-) users) [3][15][27][38]. With that, IoT systems have two layers more than traditional ICT systems: the perception and middleware layers. This is the main cause of IoT complexity, as these layers comprise a large number of sensory, actuation and processing devices with heterogeneous software and hardware components from many (possibly small and unknown) manufacturers.

Second, proliferation of IoT devices creates large amounts of data of various formats, types and granularities. These (big) data can be processed and linked to other data sets in order to deliver enriched information about people and their physical and virtual environments, often containing (new) personally identifiable data [31][48][65]. As such, the collection and use of IoT data may result in many privacy threats. Usually, IoT data pass through many organizational, judicial, national and system boundaries, and are combined with other data sets along the way. The data subjects, consequently, may not know how their data

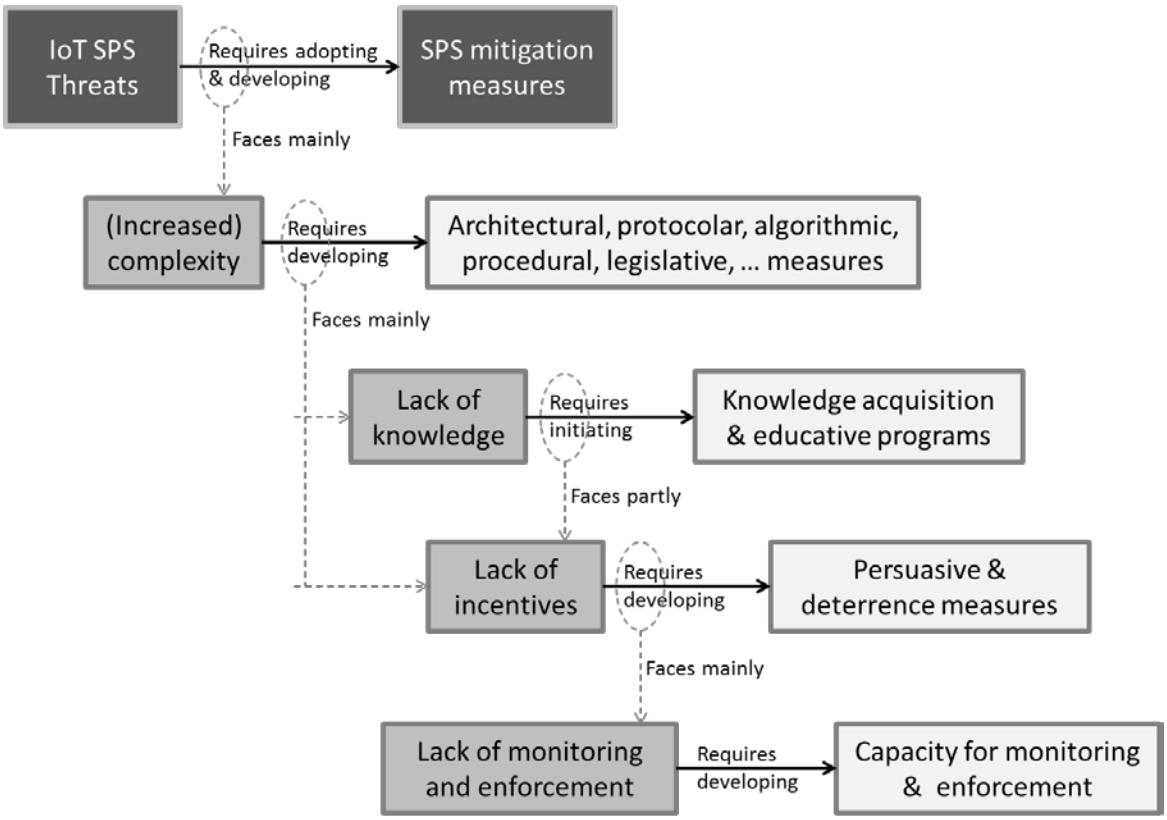

Figure 1. Conceptual framework of the obstacles in addressing IoT SPS threats (boxes on left side), and solution directions to overcome them (boxes on the right side).

are treated and cannot apply their data ownership rights appropriately. Data recipients and processors, on the other hand, cannot identify the data subjects and do not know their preferences about how to treat their data.

Third, a wide range of stakeholders – e.g., citizens, scholars, entrepreneurs, and civil servants [11] – play a role in developing, deploying, and using IoT-based services. As these stakeholders are spread over various geographical, governmental, judicial and administrative boundaries, it becomes difficult to enforce or apply the rules, regulations, interests, and standards that apply within those boundaries. For example, those who misuse IoT data cannot easily be identified and held accountable for their deeds.

IoT complexity makes it more challenging to realize efficient, scalable and interoperable SPS mechanisms for IoT than for traditional ITs [66]. We identified five reasons for that. First, malicious attackers in IoT have access to a vast number of attack vectors [49][66], pertaining to the perception and middleware layers. For example, the middleware layer introduces a new type of stakeholders acting as service enabling intermediaries. These parties may become a source of privacy and security threats by launching man-in-the-middle attacks or inferring privacy-sensitive information from collected sensory data.

Second, SPS mitigation mechanisms for traditional ICTs are often insufficient in IoT settings and therefore they should be improved before being applied to the IoT [38]. For example, due to the large volume and velocity of IoT data, it is ineffective to apply solutions such as informed consent (as users get overburdened if they are asked for consent every time that (new) data are collected), privacy policies (due to increased complexity of policies when they are specified for IoT data), and data provenance (due to increased overload and complexity in marking the origin of the IoT data, and the processes applied to them). Furthermore, DDoS attacks (the most common network attacks especially in IoT settings) cannot be mitigated effectively by using traditional intrusion detection and prevention mechanisms [33].

Third, non-comprehensive mitigation mechanisms, i.e., those that aim at addressing SPS threats within a limited temporal, spatial or legal scope, may not work well in IoT settings because different layers of IoT are melt into one large system integration [33]. Interaction among such localized mechanisms, with limited

scopes, may cause undesired emergent behaviors [42]. Thus "security technologies should provide the strong protection for all levels of system components at all stages" and system layers, [39, p. 13].

Fourth, similarly, at the governance level it is ineffective to have small-scale measures, such as unilateral sanctioning of stakeholders who do not adopt appropriate SPS measures, or defining narrow regulations and standardizations for IoT systems. Even when a (limited) number of countries impose sanctions on specific IoT products and services, the use and adoption of such products and services in other countries may still have adverse impact on the first group of countries.

Fifth, due to complexity, more trade-offs arise between, for example, privacy and public security, privacy and utility, connectivity and disconnectivity. It is also difficult to seek one-size-fits-all solutions due to the contextual dependency of IoT systems in terms of when, where, how or why they are applied. These contextual conditions dictate the degree of risk involved and, therefore, SPS solution(s) should be adopted accordingly.

In summary, dealing with IoT SPS threats is rather complex. Considering the inherent complexity of the IoT, system developers and companies may be reluctant to adopt SPS mitigation measures (e.g., using security and privacy by design principles).

4.1.2. Solution directions. Realizing SPS by design in IoT systems requires designing an IoT infrastructure that is pervasive, interoperable and intelligent by thoroughly correlating the SPS-related design decisions with the requirements and characteristics of those IoT systems [34]. Creating this ubiquity, interoperability, and smartness is complex and should be realized at all system levels, such as architecture, protocols, and algorithms, as will be elaborated upon in the following.

At the *architectural level*, solution directions such as 1) Service Oriented Architecture (SOA), 2) web service architecture, 3) intelligence distribution, 4) cloud computing, and 5) employing software development tools are proposed. Firstly, SOA decomposes "complex and monotonic systems" into well-defined simpler components, and offers common interfaces and standard communication protocols among these components [6]. In recent years, IoT middleware architectures are often based on the SOAs [6], offering, among others, a way to deal with complexity issues. Secondly, web service architectures, relying on open and royalty free IETF (Internet Engineering Task Force) standards and best practices, offer a flexible and interoperable system design that is proven for traditional web services. Using the web service architecture for IoT services – or "Web of Things" as considered in [6] – has been widely viewed as a promising way to realize flexible and interoperable IoT systems [67]. Thirdly, intelligence distribution is another way to cope with IoT complexity issues at the architectural level. This can be done in two directions. On the one hand, costly computations, processes and operations (like data exchange, decision-making and computation) can be shifted from low power and low computing capacity IoT devices to resourceful system components located in access and core networks like gateways [38] and proxies [6]. On the other hand, some processing tasks and functions can be shifted from central components to those at the edge network to yield improved functionalities like system availability, fault tolerance, data sharing and management, trust management, and governance [49]. This so-called edge intelligence principle can be created by "connected intranets of things" located in (spatial) areas like hospitals, stations and households [49]. Fourthly, cloud computing is a promising approach for distributing intelligence towards a core network. Moreover, the cloud can realize some IoT middleware functions like device interconnection, data processing, and data storage. Here the cloud offers sensing as a service, as mentioned in [66] and the references therein. Lastly, having a set of common toolkits for application developers can make it easier for them to design and reprogram IoT devices after deployment [14].

At the *protocol level*, proposed solution directions are 1) designing lightweight IoT protocols, 2) supporting existing SPS protocols, and 3) mapping new and existing protocols. Communication protocols for IoT systems should have lower complexity compared to those devised for traditional IT systems due to the power and networking limitations of IoT devices. Designing lightweight IoT protocols, for example, for key management, access authentication, and access control, is considered a continuous future research direction [33]. Additionally, in designing lightweight IoT protocols one should support existing security protocols (like IPsec) [49]. In order to have both new lightweight and old protocols, it is necessary to map them to each other. This entails mapping existing standards for internet communications with low-complexity counterparts designed for IoT communication over constrained networks. To this end, a reference protocol architecture is proposed in [67] to carry out protocol mapping at three layers of data, application/transport, and network. The proposed architecture maps three typical de-facto protocols XML, HTTP, and IPv4 to their IoT counterparts: EXI (Efficient XML Interchange), CoAP (Constrained Application Protocol), and 6LoWPAN, respectively.

At the *algorithmic level*, there are solution directions proposed such as 1) devising lightweight

cryptographic mechanisms, 2) adding self-organizational capabilities, and 3) designing adaptive and context-aware IoT middleware. Security and privacy solutions often rely on cryptographic methods, which typically demand a high amount of communication, processing and/or energy capacity. In IoT settings, where these resources are scarce, new solutions are required "to provide a satisfactory level of security regardless of the scarcity of resources" (like lightweight symmetric key cryptographic schemes) [6, p. 16]. For instance, decentralized architectures with loosely coupled "smart objects" (i.e., autonomous objects that can sense, process and network) also show potentials for coping with IoT complexity [36]. In [50], three types of smart objects are identified, namely: activity-aware (able to record information about activities), policy-aware (able to interpret activities based on some predefined policies), and process-aware (able to interpret a collection of related activities in time and space). When smart objects are equipped with artificial intelligence capabilities, the corresponding IoT systems can portray self-protection, self-healing, self-optimization, self-management and self-configuration characteristics [41][57][66]. In addition, such self-organization capabilities can also be employed in the middleware layer components [34] to deliver context-aware IoT middleware [66] that copes with the complexity of connecting billions of IoT devices. In [6], semantic-oriented IoT visions are considered as promising for describing, modeling and reasoning about IoT data. Using well-defined languages to describe IoT data with adequate metadata (i.e., in standardized formats, models, and semantic content descriptions) will enable IoT systems to support automated reasoning which, in turn, leads to the successful adoption of such IoT systems [41].

Besides implementing technical solutions, adopting a collaborative approach is important for having an effective and sustainable impact on the security of the IoT ecosystem [35]. To this end, collaboration and cooperation among IoT stakeholders can take place on various levels such as smart object [34], policy, legislation, standardization, and governance [12][14][49]. Additionally, one should coherently and cost-effectively validate and test the interoperability and compatibility of different IoT devices [57].

4.2. Lack of knowledge

Dealing with the complexity of the IoT is impeded by a lack of awareness and knowledge among users, IoT producers and providers, and policy-makers (see Figure 1). In order to successfully deal with the SPS threats of the IoT, awareness of the existence of these issues is needed in the first place. Subsequently, knowledge of mitigation measures is needed to protect oneself against cyber threats [52].

4.2.1. Reasons and impacts. The human factor forms a crucial element in the defense against cyber security. When information systems become better protected by technological solutions, attackers shift their attention to human elements to break into these systems [2]. For instance, users often use standard passwords [8] or reuse passwords for multiple services [19], increasing the risk that attackers gain access to sensitive information. Another malicious strategy for tapping into human vulnerability is the use of phishing emails, which entice users to click on links leading to websites with malicious software [22]. Both examples show that human behavior can play an important role in mitigating cyber security risks and that users are currently not protecting themselves as much as they could. This can be explained by a lack of knowledge and awareness among users. When people are well informed, on the other hand, they are better capable of defending themselves against cyber threats [37][53].

Besides users, it is also important that IoT producers and providers, and policymakers have knowledge and awareness concerning SPS threats. With the right knowledge, producers and providers can develop safe, secure and privacy-friendly IoT systems [38], and policy-makers can take the measures needed to support the development of these systems [51]. Currently, however, this knowledge is not always present. A report on IT projects initiated by the Dutch government, for example, concludes that there is an "almost unbridgeable gap" between IT experts and policymakers [45]. Another report concludes that policymakers have insufficient awareness and knowledge of IoT threats [8].

There is an interplay between IoT complexity on the one hand, and lack of knowledge and awareness on the other hand. The fast developments and the high complexity of IoT systems require a continuous update of knowledge in order to stay well informed. As this is difficult, the fast developments and high complexity create a lack of knowledge and awareness. At the same time, because hardly anyone has an overview of the latest developments in the whole IoT field, this knowledge gap impedes dealing with the complexity of the IoT.

4.2.2. Solution directions. There are a couple of measures that can be taken to overcome the knowledge gap. First, investments in education can help to increase knowledge and awareness concerning the IoT [12][44]. These investments could target primary and secondary education, and universities, which educate future generations of IoT users and developers.

Research should yield insight into the best teaching practices. The UK, for instance, considers to base mathematical education in schools on computational thinking, with a focus on problem solving rather than making calculations [28], but others advocate other approaches [12]. Investments should also be made in the (re-)education of employees that currently work with, provide or develop IoT systems.

Second, awareness campaigns about cyber security can increase digital resilience of citizens [20]. Such campaigns should be accompanied by easily accessible and clear information to citizens, e.g., in the form of a website or an online crash course. Campaigns can also be used to start or foster public debate between citizens, companies and researches, on the trade-offs between security and other values.

Last, investments in (scientific) research can help creating SPS solutions, taking into account that most users do not have expert knowledge [49]. Many of the approaches for addressing IoT threats discussed in Section 2 and the current section originated from or were inspired by scientific research.

4.3. Lack of incentives

As discussed in Subsection 4.1, the complexity of the IoT makes it expensive and difficult to devise and apply appropriate measures against SPS threats. On top of that, taking such measures often yields little benefits for the respective party. For example, once a user has paid for a certain product, the company has little incentive to keep on investing in security updates for that product. Additionally, regarding the demand for increased knowledge and awareness, as discussed in Subsection 4.2, different parties do not always immediately experience the benefits of more knowledge and awareness themselves. In other words, dealing with IoT complexity and the lack of awareness and knowledge is impeded by a lack of appropriate incentives and motivations (see Figure 1).

4.3.1. Reasons and impacts. The lack of incentives to create or use SPS friendly IoT devices applies to both users and companies. Users often do not experience harm when their IoT devices are hacked, and in many cases, they do not even notice that this happened. For instance, a smart thermostat does not necessarily loose its functionality when it becomes part of a botnet. Moreover, when settings are hidden in a complex menu, it can be a hassle to adopt SPS measures. Thus, users often do not feel the need to adjust their behavior when using IoT devices, or to improve their knowledge about IoT use, in a way that promotes safety, security and privacy.

For companies, there are different reasons for the lack of incentives. First, it is attractive for companies to be the first to launch a new product, and the development and implementation of security measures takes time [62]. Second, once a product is sold, there is little incentive for companies to provide updates that ensure security [32]. Developing security updates costs time and money [44], and can even hinder the functionality, compatibility and ease of use of the product [7]. For startups, which introduce many new IoT products, there are even fewer incentives than for bigger companies since they have little reputation to loose [29]. Internet Service Providers (ISPs) could play an important role in mitigating security risks, but also for them, the extra costs yield little benefits [5][7].

4.3.2. Solution directions. The lack of incentives to cope with complexity (by adopting suitable SPS mitigation measures), and to increase knowledge applies to both users and companies. For users, however, it is reasonable to assume that companies sell sound products. Therefore, measures to generate incentives should mainly target companies. We will discuss several of these measures in the following.

First, a measure to generate incentives for companies is to strengthen the so-called duty of care. Duty of care refers to someone's duty to take into account and act in accordance with the interests of others [56], which can also involve companies' duty to provide secure and privacy-friendly IoT systems. Current duty of care regulations are not always suitable to apply to IoT products or services. For instance, it is unclear what companies' responsibilities are regarding the updating of unsafe software on IoT devices. Current Dutch case law shows that this is judged on a case-by-case basis [56][62].

Second, accountability based on damage caused by IoT systems can be an important incentive for companies to offer safe and secure products [43]. Moreover, solid accountability regulations can provide the basis for duty of care. Though companies are currently already accountable for the products they sell, accountability is often evaded. It is often difficult (due to IoT complexity) to pinpoint the source of the problem in malfunctioning software, and thus to identify who is responsible for that problem. Moreover, accountability is sometimes circumvented by excluding it in a product's terms and conditions [26].

Third, since various parties are involved in the production of IoT systems, the introduction of supply chain responsibility can help making IoT systems more secure [10]. This means that all parties involved in the supply chain share the responsibility for the end quality of a product. Parties in a chain can impose rules and

make demands to each other and, if necessary, hold each other accountable for possible damage [12].

Fourth, cyber risk insurances can create incentives for companies, provided that the insurers require companies to comply with certain security standards [40]. As the risks of cyber-attacks are growing and the potential damage of such attacks increases, it becomes attractive for companies to insure themselves against such risks. Insurance companies often make use of security standards to estimate the risk of an attack, and thus the height of the premium a company has to pay. This provides an incentive for companies to comply with higher security standards.

Finally, policymakers can offer incentives to ISPs to mitigate security risks [5]. As ISPs act as a doorway to the Internet for many, they are in an advantageous position to mitigate cyber security risks. Providing policy-based incentives lowers the costs for ISPs to take mitigating measures, and it increases the pressure for them to act. In the Netherlands, for example, several ISPs collaborate in the Dutch anti-botnet center AbuseHub [25], which is partially financed by the Dutch government.

4.4. Lack of monitoring and enforcement

Increasing and creating incentives requires devising and applying appropriate mechanisms such as monitoring and enforcement. Lack of monitoring and enforcement mechanisms impedes the effects of the incentives described above, as indicated in Figure 1.

4.4.1. Reasons and impacts. Current regulations on privacy and security in IT are limitedly monitored and enforced. An example of this is the data breach notification obligation introduced in the Netherlands as of January 2016. This obligates companies to report data leaks and take measures against them. If no measures are taken, the Dutch data protection authority can impose fines up to a maximum of €820,000 or 10% of a company's year revenue. In the first year, 5,500 data leaks were reported. Some warnings were given, but no fines were imposed so far. It is estimated that 18,500 data leaks were unreported [46].

In addition, standards only work with effective monitoring and enforcement. Conformité Européenne (CE) marking offers an example of this mechanism. CE is a mandatory marking for certain products sold within the European Economic Area. The marking represents the manufacturer's declaration that the product meets European requirements on security, health, environment, etc. Each year, however, several CE-marked unsafe or unsecure products are withdrawn from the market, due to insufficient capacity for monitoring and enforcement [1]. Though CE marking is not specifically aimed at cyber security or privacy, the above example demonstrates that a standard alone does not guarantee the safety or security of a product.

The current duties of care and accountability regulations are not specific for IoT systems, which can create uncertainties about their scope. As discussed in Subsection 4.3, it is unclear what companies' responsibilities are regarding updating unsecure software on IoT devices [56][62]. Because of these ambiguities in duty of care and accountability regulations, it is harder to effectively monitor and enforce them.

4.4.2. Solution directions. Adequate monitoring and enforcement are important conditions for incentives such as duty of care and accountability. It is also important for effectuating standards. An obvious measure to overcome a lack of monitoring and enforcement is thus to invest in increased capacity at involved supervision authorities.

Another measure is to improve current duties of care and accountability regulations. As mentioned earlier, these regulations are sometimes unclear when applied to IoT systems. To be effective, duty of care should become more concrete on what an end-user can expect from a provider, which may require additional research. In addition, both duties of care and accountability regulations should be clear on the timespan during which they are applicable. This timespan may vary for different IoT products. A thermostat, for instance, is seldom replaced, whereas smart phones are regularly renewed.

5. Conclusion

This paper introduced a conceptual framework for addressing IoT SPS threats, as shown in Figure 1. The framework proposes the deployment of SPS by design to minimize SPS threats, and identifies four obstacles in realizing this: 1) IoT complexity, 2) lack of awareness, 3) lack of incentives, and 4) lack of monitoring and enforcement. The framework also shows how these obstacles, and solution directions to overcome them, are related to each other in that addressing one impacts the other one(s) and vice versa. The conclusion that can be drawn from this work is that there is no one-size-fits-all measure to address SPS threats. Instead, a variety of measures is needed to create an SPS-friendly IoT.

We have a number of suggestions for future work. First, the research presented in this paper was performed in a Dutch context. Additional research could focus on other countries. Second, the research

presented in this paper is rather general. Further research could focus on addressing SPS threats in specific application domains. Third, research is needed to investigate the feasibility and effects of different measures. Fourth, a closer study of the technical aspects of IoT systems could enhance SPS-by-design practices. Finally, future research could investigate the legal implications of adopting legislations concerning the IoT.

The above recommendations for future work can be used to improve and specify the conceptual framework proposed in this paper, thus contributing to the aim of creating a secure, privacy-friendly and safe IoT.

Acknowledgements

The authors thank the participants of the interviews and roundtables for sharing their knowledge and insights. Thanks to the guidance advisory committee for their critical feedback on earlier drafts of the work.

References

[1] Algemene Rekenkamer, *Producten op de Europese markt: CE-markering ontrafeld*, Algemene Rekenkamer, 2017.

[2] Abawajy, J., "User preference of cyber security awareness delivery methods", *Behaviour & Information Technology*, Taylor & Francis, 2014, pp. 237-248.

[3] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M., "Internet of things: A survey on enabling technologies, protocols, and applications", *Communications Surveys & Tutorials*, IEEE, 2015, pp. 2347-2376.

[4] Aoyama, T., Koike, M., Koshijima, I., & Hashimoto, Y., "A unified framework for safety and security", *Safety and security engineering V*, WIT Press, 2013, pp. 67-77.

[5] Asghari, H., van Eeten, M. J., & Bauer, J. M., "Economics of fighting botnets: Lessons from a decade of mitigation", *Security & Privacy*, IEEE, 2015, pp. 16-23.

[6] Atzori, L., Iera, A. & Morabito, G., "The Internet of Things: A survey", *Computer Networks*, Elsevier, 2010, pp. 2787–2805.

[7] Bauer, J. M., & Van Eeten, M. J., "Cybersecurity: Stakeholder incentives, externalities, and policy options", *Telecommunications Policy*, Elsevier, 2009, pp. 706-719.

[8] Berkel, J. J. van, Pool, R. L. D., Harbers, M., Oerlemans, J. J., Shoae Bargh, M. S., & Braak, S. W. van den, *(Verkeerd) Verbonden in een Slimme Samenleving: Het Internet of Things: Kansen, Bedreigingen en Maatregelen*, WODC, 2017.

[9] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F., "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", *Symposium on Security and Privacy*, IEEE, 2012, pp. 553-567.

[10] Boyson, S., "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems", *Technovation*, Elsevier, 2014, pp. 342-353.

[11] Carayannis, E. G., & Campbell, D. F., "Mode 3 knowledge production in quadruple helix innovation systems", *Mode 3 Knowledge Production in Quadruple Helix Innovation Systems*, Springer, 2012, pp. 1-63.

[12] Caron, T.A., "Learning multiplication: The easy way", *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, Tailor & Francis, 2007, pp. 278-282.

[13] Castellani, A. P., Bui, N., Casari, P., Rossi, M., Shelby, Z. & Zorzi, M., "Architecture and protocols for the Internet of things: A case study", *International Conference on Pervasive Computing and Communications Workshops*, IEEE, 2010, pp. 678–683.

[14] Chen, Y., "Challenges and opportunities of Internet of things", Asia and South Pacific Design Automation Conference, IEEE, 2012, pp. 383–388.

[15] CSR (Cybersecurity Raad), *De economische en maatschappelijke noodzaak van meer Cybersecurity: Nederland digitaal droge voeten*, CSR, 2016.

[16] CSR (Cybersecurity Raad), *The opportunities and risks of the Internet of Things: Perspectives for Action*, CSR, 2016.

[17] Cvitić, I., Vujić, M., & Husnjak, S., "Classification of security risks in the IoT environment", *International Symposium on Intelligent Manufacturing and Automation*, DAAAM, 2016, pp. 731-740.

[18] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Le Métayer, D., Tirtea, R., & Schiffner, S., *Privacy and Data Protection by Design – from policy to engineering*, Technical Report TP-05-14-111-EN-N0, ENISA, 2014.

[19] Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X., "The tangled web of password reuse", *NDSS Symposium*, Internet Society, 2014, pp. 23-26.

[20] Davies, R., *The Internet of Things Opportunities and challenges*, European Parliamentary Research Service, 2015.

[21] De Lange, M., & Von Solms, R., "The importance of raising e-safety awareness amongst children", *World Wide Web applications*, Springer, 2011, p. 14.

[22] Dhamija, R., Tygar, J. D., & Hearst, M., "Why phishing works", *Human Factors in computing systems*, ACM, 2006, pp. 581-590.

[23] DHS (Department of Homeland Security), *Strategic Principles for Securing the Internet of Things (IoT)*, US DHS, 2016.

[24] Easttom II, W.C., *Computer security fundamentals*, Pearson IT Certification, 2012.

[25] Eeten, M., van, Lone, Q., Moura, G., Asghari, H., & Korczyński, M., *Evaluating the Impact of AbuseHUB on Botnet Mitigation*, report, Cornell University Library, 2016.

[26] Engelfriet, A., "Ben ik aansprakelijk voor de fouten in mijn software?" *IUS Mentis*, 2011, consulted on 4 April 2017 via: https://blog.iusmentis.com/2011/09/19/ben-ik-aansprakelijk-voor-de-fouten-in-mijn-software.

[27] Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A. & Kamal, T., "A Review on Internet of Things", *International Journal of Computer Applications*, FCS, 2015, pp. 1-7.

[28] GO-Science (The Government Office for Science), *The Internet of Things: Making the most of the Second Digital Revolution*, GO-Science, 2014.

[29] Haas, A., Haas, M., & Weinert, M., "The Internet of things is already here, but who bears the risks?", *World Risk and Insurance Economics Congress*, WRIEC, 2015, pp. 1-30.

[30] Healey, J., Pollard, N., & Woods, B., *The healthcare internet of things: Rewards and risks*, Atlantic Council, 2015.
[31] Hildebrandt, M., "Defining profiling: A new type of knowledge?", in M. Hildebrandt, & S. Gutwirth (Red.), *Profiling the European citizen*, Springer, 2008, pp. 17-45.
[32] Jacobs, B., "Aftercare for the Internet of Things", *CSR Magazine*, CRS, 2016, pp. 61-62.
[33] Jing, Q., Vasilakos, A. V, Wan, J., Lu, J. & Qio, D., "Security of the IoT: perspectives and challenges", *Wireless Networks*, Springer, 2014, pp. 2481-2501.
[34] Katasonov, A., Kaykova, O., Khriyenko, O., Nikitin, S. & Terziyan, V., "Smart semantic middleware for the IoT", *ICINCO-ICSO*, INSTICC Press, 2008, pp. 169–178.
[35] Kolkman, O., "Trust Isn't Easy: Drawing an Agenda From Friday's DDoS Attack and the Internet of Things", *Internet Society*, 2016, consulted on 14 June 2017 via: https://www.linkedin.com/pulse/trust-isnt-easy-drawing-agenda-from-fridays-ddos-attack-olaf-kolkman?trk=hp-feed-.
[36] Kortuem, G., Kawsar, F., Fitton, D. & Sundramoorthy, V., "Smart objects as building blocks for the Internet of things", *Internet Computing*, IEEE, 2010, pp. 30–37.
[37] Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E., "Protecting people from phishing: the design and evaluation of an embedded training email system", *Conference on Computer Human Interaction*, ACM, 2007, pp. 905–914, ACM.
[38] Langheinrich, M., "Privacy by Design: Principles of Privacy-Aware Ubiquitous Systems", In *Ubicomp 2001: Ubiquitous Computing*, Springer, 2001, pp. 273-291.
[39] Li, S., Xu, L. Da & Zhao, S., "The IoT: a survey", *Information Systems Frontiers*, Springer, 2015, pp. 243–259.
[40] Low, P., "Insuring against cyber-attacks", *Computer Fraud & Security*, Elsevier, 2017, pp. 18-20.
[41] Miorandi, D., Sicari, S., Pellegrini, F. De & Chlamtac, I., "Ad hoc networks Internet of things: Vision, applications and research challenges", *Ad Hoc Networks*, Elsevier, 2012, pp. 1497–1516.
[42] Mogul, J., "Emergent (mis)behavior vs. complex software systems", *SIGOPS Operating Systems Review*, ACM, 2006, pp. 293–304.
[43] Moore, A. (Ed.), *Privacy, Security and Accountability: Ethics, Law And Policy*, Rowman & Littlefield International, 2015.
[44] Munnichs, G., Kouw, M. & Kool, L., *Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid*, Rathenau Instituut, 2017.
[45] Elias, T., Ulenbelt, P., Fokke, M., Bruins Slot, H., & Meenen, P. van, *Parlementair onderzoek naar ICT-projecten bij de overheid*, Report Commissie Elias, Tweede Kamer, 2014.
[46] Pb7 Research, *Meldplicht datalekken in de praktijk*, Pb7 Research, 2017.
[47] Peppet, S.R., "Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent", *Texas Law Review*, University of Texas, 2014, pp. 85-176.
[48] Rose, K., Eldridge, S., & Chapin, L., *The IoT: an overview - Understanding the Issues and Challenges of a More Connected World*, Internet Society, 2015.
[49] Roman, R., Zhou, J., & Lopez, J., "On the features and challenges of security and privacy in distributed internet of things", *Computer Networks*, Elsevier, 2013, pp. 2266-2279.
[50] Sanchez Lopez, T.C., Ranasinghe, D., Harrison, M. & Mcfarlane, D., "Adding sense to the Internet of things: An architecture framework for Smart Object systems", *Personal and Ubiquitous Computing*, Springer, 2012, pp. 291–308.
[51] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A., "Security, privacy and trust in IoT: The road ahead", *Computer Networks*, Elsevier, 2015, pp. 146-164.
[52] Singer, P.W., & Friedman, A., *Cybersecurity: What Everyone Needs to Know*, Oxford University Press, 2014.
[53] Stratix, *IoT in the Netherlands: Applications, trends and potential impact on radio spectrum*, Stratix, 2015.
[54] Thomson, K.-L., Von Solms, R. & Louw, L., "Cultivating an organizational information security culture", *Computer Fraud & Security*, Elsevier, 2006, pp. 7-11.
[55] Talbot, E. B., Frincke, D. & Bishop, M., "Demythifying cybersecurity", *Security and Privacy*, IEEE, 2010, pp. 56–59.
[56] Tjong Tjin Tai, T.F.E., Koops, E. J., Heij, D. O., Silva, K. E., & Skorvánek, I., *Duties of care and diligence against cybercrime*, Technical Report, Tilburg University, 2015.
[57] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Soler Jubert, I., Mazura, M., Harrison, M., Eisenhauer, M. & Doody, P., "Internet of things strategic research roadmap", *Internet of Things-Global Technological and Societal Trends*, River Publishers, 2011, pp. 9–52.
[58] Weber, R. H., "Internet of things – new security and privacy challenges", *Computer Law & Security Review*, Elsevier, 2010, pp. 23-30.
[59] Whitman, M.E., & Mattord, H.J., *Principles of Information Security*, Cengage Learning, 2014.
[60] Whitmore, A., Agarwal, A., & Xu, L.D., "The Internet of Things: A survey of topics and trends", *Information Systems Frontiers*, Springer, 2015, 261-274.
[61] Wolff, J., "Perverse effects in defense of computer systems: When more is less", Hawaii International Conference on System Sciences, IEEE, 2016, pp. 4823–4831.
[62] Wolters, P.T.J. & Verbruggen, P.W.J., "De verplichting tot het bijwerken van onveilige software", *Privaatrecht, Notariaat en Registratie*, SDU, 2016, pp. 832-839.
[63] WEF (World Economic Forum), *Deep Shift: Technology Tipping Points and Societal Impact*, WEF, 2015.
[64] WRR (Wetenschappelijke Raad voor het Regeringsbeleid), *De publieke kern van het internet: Naar een buitenlands internetbeleid*, WRR, .2015.
[65] WRR (Wetenschappelijke Raad voor het Regeringsbeleid), *Big Data in een vrije en veilige samenleving*, WRR, 2016.
[66] Xu, L. Da, He, W. & Li, S., "Internet of things in industries: A Survey", *Transactions on Industrial Informatics*, IEEE, 2014, pp. 2233–2243.
[67] Zanella, A., Bui, N., Castellani, A., Vangelista, L. & Zorzi, M., "Internet of things for smart cities", *Internet of Things Journal*, IEEE, 2014, pp. 22–32.