Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2018 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2018

State-of-the-Art in Security Thinking for the Internet of Things (IoT)

Miranda Kajtazi
Lund University

Bahtijar Vogel
Malmö University

Joseph Bugeja
Malmö University

Rimpu Varshney
Sony Mobile Communications AB

Recommended Citation

Kajtazi, Miranda; Vogel, Bahtijar; Bugeja, Joseph; and Varshney, Rimpu, "State-of-the-Art in Security Thinking for the Internet of Things (IoT)" (2018). *WISP 2018 Proceedings*. 5.
https://aisel.aisnet.org/wisp2018/5

State-of-the-Art in Security Thinking for the Internet of Things (IoT)

Miranda Kajtazi[1]
Department of Informatics, School of Economics and Management, Lund University,
Lund, Sweden

Bahtijar Vogel
Department of Computer Science and Media Technology, Malmö University,
Malmö, Sweden

Joseph Bugeja
Department of Computer Science and Media Technology, Malmö University,
Malmö, Sweden

Rimpu Varshney
Department of Security and Enterprise, Sony Mobile Communications AB,
Lund, Sweden

ABSTRACT

In this paper we propose a model for Internet of Things (IoT) practitioners and researchers on how to use security thinking in parallel with the IoT technological developments. While security is recognized as a top priority, repeatedly, IoT products have become a target by diverse security attacks. This raises the importance for an IoT security mindset that contributes to building more holistic security measures. In understanding this, we present the state-of-the-art in IoT security. This resulted in the identification of three dimensions (awareness, assessment and challenges) that are needed to develop an IoT security mindset. We then interviewed four security and IoT-related experts from three different organizations that formed the basis for our pilot study to test the model. Our results show that the identified three-dimensional model highlights continuous security thinking as a serious matter to sustain IoT development with positive outcomes for its users.

Keywords: Security thinking; Internet of Things; IoT; Awareness, Assessment; Challenges.

[1] Corresponding author. miranda.kajtazi@ics.lu.se

INTRODUCTION

According to the research of the International Telecommunication Union (ITU) there were about 4.3 billion users expected to be online only through mobile broadband globally by the end of 2017 (Brahima 2017). The latest report by IHS Markit (Lucero 2016), shows that the Internet of Things (IoT) market is predicted to grow from an installed base of 20 billion devices in 2017, to 30.7 billion devices in 2020, and 75.4 billion devices in 2025, a growth that will put to the test the security resilience of Internet-connected devices. Within less than a decade, we have seen how a new IoT infrastructure for online sociality and creativity has emerged, which forms a new layer of the digital infrastructure, through which people have started to organize their lives (van Dijck 2013). This emergence made it possible for IoT vulnerabilities to emerge too, putting that digital infrastructure in the spotlight for frequent and serious data breaches.

The presence of the IoT is increasing at a fast pace bringing various benefits to diverse stakeholders. For instance, efficient energy management through the utilization of smart technologies. But constraints set by the environment around the IoT (Porras et al. 2018) present the challenge for security that is not guaranteed (Alaba et al. 2017). Indeed, securing the IoT has been identified in 2014 by the Defense Advanced Research Projects Agency (DARPA), as one of the four projects with a potential impact broader than the Internet itself (Sfar et al. 2018). A badly secured system can lead to privacy violations, financial losses, corporate liability and other crafted security attacks that also leads to uncertainty among IoT adopters (Petersen et al. 2014; Porras et al. 2018). Such uncertainty comes as a result of IoT vulnerabilities that can even lead to take control and ownership of devices, e.g. pacemakers, through the installation of malware possibly leading to loss of lives (Lowry et al. 2017). While the IoT infrastructure is based on the Electronic Product Code (EPC), where physical objects carry an RFID tag with a unique EPC, this method has shown to leave traces of data in the cyberspace unwillingly (Weber 2010). Security and privacy precautions are at the top of the agenda for the industry, yet a growing number of smaller IoT vendors, typically startups, whose core competence does not focus on security, brings a bigger challenge to set-up a secure IoT infrastructure (Weber 2010; Spanaki et al. 2017; Devine 2018). As an example, if a traditional hardware manufacturing company enables Internet connectivity on their product, they can accomplish this with a small group of software developers. However, they might not necessarily have the security expertise and budget allocated to conduct security processes such as threat modelling, risk assessment and security audits. This results in poor quality and insecure systems that could be relatively easily exploited by hackers due to a number of security vulnerabilities they may contain (Lowry et al. 2017).

Highlighting the inevitable presence of IoT, in this study the goal is to prioritize security as a mandatory characteristic for the IoT. We motivate the key concept and models that were developed to target security in the IoT infrastructure. We then focus on the state-of-the-art, particularly in relation to security in IoT. In addition, we provide some empirical input by understanding how four security experts view IoT security. We identify *three key security dimensions* and related aspects. Followed by the research approach and results from the state-of-the-art in IoT security, we then bring the pilot study data. We finally conclude the paper.

MOTIVATION AND BACKGROUND

Mark Wieser's seminal work on ubiquitous computing, considered as the precedent of what we frame today as the IoT, proposed the idea of technology working in the background while its actions come in the forefront (Wieser 1991). Today, we strive to develop such technology through IoT, where safety, security and privacy should be key. According to Agarwal and Dey (2016), these three aspects must be tackled from the ground-up. But aspects like extreme heterogeneity, lack of standardization for the openness (Vogel and Gkouskos 2017) and ineffectiveness of traditional methods of security (Agarwal and Dey 2016) are a constant target for finding the right security solutions. Challenging IoT security from a security thinking approach, puts security in the spotlight for continuous efforts among practitioners and researchers to improve it.

Security thinking is expressed in two forms. First, it refers to the technical measures the IoT practitioners take when developing an IoT system. IoT systems often expand with security and privacy considered as an afterthought (Sicker and Lookabaugh 2004), at the expense of lack of security expertise, cost-savings and time trade-off (Spanaki et al. 2017), which should be carefully planned with an ethical use and development of IoT by investing significant resources on the sociotechnical IoT aspects (Dhillon et al. 2016). Second, it refers to progress towards a secured organizational culture often by ensuring employee training and education to influence and activate their thinking about information security (Moody et al. 2018). Recent studies like Kajtazi et al. (2018) and Moody et al. (2018) show that security thinking is not developed enough in organizations, a trend that has likely influenced the immature thinking of security across IoT systems. Instead, organizations prioritize to release their products to the market at the stake of security.

Likewise, we argue that we should be striving for an IoT security thinking mechanism expressed in the two forms above, but following a consecutive order, first a proactive security mechanism during requirements, development and implementation, and then security awareness tactics. Echoing Lowry et al. (2017) that IoT is rewriting all the rules on how we once considered security, the IoT infrastructure will fail if we don’t act already now.

RESEARCH APPROACH

This study begins by formulating a state-of-the-art on concepts and models for security in IoT. While some studies were not directly focusing on IoT per se, we reasoned to include them by realizing that their input was key in strengthening security thinking for IoT developers, implementers and users. Scrutinizing the security literature from the IoT perspective to form the state-of-the-art we observe that security insights from practitioners are very few. In dealing with this challenge, we conducted a pilot study driven by the semi-structured interview approach. This study uses the first-hand experience of four security and IoT practitioners from 3 different organizations. These respondents identifiers (ID) alongside their corresponding details are presented in Table 1.

Table 1. Number of Respondents with Semi-Structured Interviews

ID	**Role**	**Organization**	**Length**
R1	Security Architect	Sony Mobile Communications AB	60 mins
R2	Senior IOT Architect	Sony Mobile Communications AB	55 mins
R3	Security Coach	Axis AB	50 mins
R4	Security Expert	Hyker Security AB	67 mins

Details on how the interview guide was developed and the presentation of raw data from the interviewees can be found in the work of Varshney (2018).

TOWARDS SECURITY THIKING FOR IOT: IDENTIFYING NEW DIMENSIONS

In the traditional view, a good security practice was likely achieved through effective technologies, policies, standards and procedures that intended to ensure the CIA-triad: confidentiality, integrity and availability. Confidentiality is seen as the prevention of unauthorized disclosure, integrity as the prevention of the unauthorized modification, and availability as the prevention of unauthorized withholding of data (Dhillon and Backhouse 2001). The CIA-triad has been extended over the years – e.g., the CIA+ to deal with network security attacks (Simmonds et al. 2004). Nonetheless, the IoT domain poses additional aspects that are not covered by the mentioned models. Additionally, in IoT systems, new security requirements have arisen due to specific features and properties of IoT systems. Even if security and privacy must go hand-in-hand, often there are situations when the prior becomes a cause for concern for the former. For example, strengthening surveillance systems for a better security comes at the expense of privacy.

In light of the aspects mentioned above, below we provide an overview of related studies that have introduced concepts and models towards conceptualizing about security in IoT. In doing so, we find that concepts and models can be both innovative and risky at the same time, due to their constricted singular view upon the IoT infrastructure. We thus identify new dimensions and a number of aspects that are important for continuous security thinking in IoT, targeting not only practitioners alone, but also developers, users and the society at large.

IoT Awareness Dimension

Raising awareness for *data management* in terms of sensitive information in the IoT domain current practices is an important feature (Aggarwal et al. 2013; Benson et al. 2015; Kolias et al. 2016). However, *training and education* require broader spectrum of stakeholders to be included, such as policy makers, regulators and the general public in order to raise such awareness regarding IoT challenges, risks and opportunities (Törngren et al. 2015). More specifically, there is a need for user *awareness and security education* for both developers and users of smart products and services (Izosimov and Törngren 2016). The best way to keep security on users' attention is to offer continuous security awareness and education programs (Stallings et al. 2014). Because these smart products and services should be *designed-in security* concepts in mind (Peisert 2014) and at the same time dealing with *ethical concerns* in terms of bringing awareness to owners of IoT smart products related to the degree of privacy (Kaleta et al. 2018). Thus, *continuous education* for engineers and other stakeholders in IoT field is important for enabling life-long learning regarding security and privacy aspects likewise (Dhillon et al. 2016; Törngren et al. 2015; Harbers et al. 2018; Stallings et al. 2014). Additional features for organizing learning mechanisms, team building and knowledge management systems need to be provided in connection to *people and team management* aspects (Wan and Zeng 2015). For raising awareness among IoT industry management and practitioners there is a need for an adequate *legal framework* that would take the underlying technology into account (Weber, 2010). This legal framework could be established by the legislator which can also be supplemented by the IoT industry according to their specific needs (Weber 2010). Furthermore, a legal framework could ensure stakeholders awareness and protection of subjects, e.g., when it comes to privacy breaches (Hoepman 2014). In order to place this framework into practice, *policy enforcement* as another feature of IoT security awareness aspect is important to be considered (Sicari et al. 2015; Porras et al. 2018).

IoT Assessment Dimension

Building trust in human is an essential assessment item of security and privacy within IoT field (Kounelis et al. 2014; Sicari et al. 2015). IoT devices need to be designed with *identity management* appropriate for the IoT environment (Kumar et al. 2017; Sicari et al. 2015; Sfar et al. 2018) for e.g., in terms of maximizing data integrity and ensuring trust mechanisms (Dhillon et al. 2016). Security risks can arise due to multiple reasons, e.g., unawareness of maliciously manipulated products or the lack of information on potential countermeasures (Izosimov and Törngren 2016). In order to avoid certain vulnerabilities and risks, *risk management* is an important aspect of assessment in security in terms of threat modeling, code reviews, and various testing aspects such as white/black-box testing (Choobineh et al. 2007; Peisert et al. 2014; Törngren, et al. 2015). In this case, also mitigation measures should be considered by utilizing *security and privacy by design principles* (Harbers et al. 2018). Having *trust management* usually helps to overcome the uncertainties and risks within the IoT environment (Porras et al. 2018; Sfar et al. 2018; Vogel and Varshney (2018)). *Auditing* is another important IoT feature (Dhillon et al. 2016). This feature is important in order to verify security vulnerabilities of IoT devices (Dhillon et al. 2016). Especially, auditing, e.g., when done repeatedly against security standards, helps in building user trust (Ali et al. 2016). In the end, *compliance* sets the frontal image of how assessment should be developed within the IoT infrastructure (Kajtazi et al. 2018; Dhillon et al. 2016). Having an IoT provider compliant to security standards may also contribute in attracting more users to use the provider services (Ali et al. 2016).

IoT Challenges Dimension

Many IoT devices used today were originally designed in *closed* way for non-Internet use and with *proprietary* code, i.e., weak protocols and practices (Benson et al. 2015; Kolias et al. 2016). Even though many *standardization* bodies together with industry tried to provide solutions for security and privacy aspects (Kolias et al. 2016), standardization in IoT still remains as a continues challenge (Izosimov and Törngren 2016). *IoT complexity* makes it almost impossible to realize secure systems efficiently in terms of the problems related to scalability and interoperability (Harbers et al. 2018; Törngren et al. 2015). *IoT environment constraints* to date present many security challenges in terms of devices computational power, memory, battery, network, operating system, and bandwidth, among others. (Porras et al. 2018; Bugeja et al. 2018). Constant evolution of new IoT technologies, *heterogeneity and continuous updates* of technologies present challenges regarding potential security vulnerabilities (Wan et al. 2015). Furthermore, *business and technical level standards* must not be taken lightly as IoT security constraints (Izosimov and Törngren 2016).

Table 2 highlights our conceptual framework derived from the state-of-the-art that initiated the development of our three-dimensional model for continuous security thinking in relation to awareness, assessment and challenges. This table presents the mapping of the three dimensions with a number of aspects identified that are important for IoT security thinking.

Table 2. State-of-the-art: three dimensions and related aspects for IoT Security Thinking

Continuous Awareness	
Aspects	**Sources**
Data management	Aggarwal et al. (2013); Benson et al. (2015); Kolias et al. (2016)
Training and education	Stallings et al. (2014); Törngren et al. (2015); Izosimov and Törngren (2016); Dhillon et al. (2016); Harbers et al. (2018);
Designed-in security	Peisert (2014); Miorandi (2012)
Ethical concerns	Kaleta et al. (2018); Dhillon et al. (2016)
People and team management	Wan and Zeng (2015)
Legal framework and policy enforcement	Weber (2010); Hoepman (2014); Porras et al. (2018)
Continuous Assessment	
Identity management	Kounelis et al. (2014); Kumar et al. (2017); Dhillon et al. (2016); Sfar et al. (2018)
Risk management	Izosimov and Törngren (2016); Choobineh et al. (2007); Peisert et al. (2014); Törngren et al. (2015)
Security and privacy by design principles	Hoepman (2014); Harbers et al. (2018)
Trust management	Sicari et al. (2015); Porras et al. (2018); Sfar et al. (2018); Vogel and Varshney (2018)
Auditing	Dhillon et al. (2016); Ali et al. (2016)
Compliance	Kajtazi et al. (2018); Dhillon et al. (2016); Moody et al. (2018); Ali et al. (2016)
Continuous Challenges	
Closed and proprietary	Benson et al. (2015); Kolias et al. (2016); Vogel and Gkouskos (2017);Bugeja et al. (2018);
Standards (both technical and business level)	Kolias et al. (2016); Izosimov and Törngren, (2016)
IoT complexity	Harbers et al. (2018); Törngren et al. (2016); Bugeja et al. (2018)
IoT environment constraints	Porras et al. (2018); Agarwal and Dey (2016); Vogel and Varshney (2018)
Heterogeneity and continuous updates	Wan and Zeng (2015); Agarwal and Dey (2016)

In reference to our findings presented as three dimensions, the call to mitigate security risks almost two decades ago still remains vital today: “the open and semi-chaotic Internet…is the creation of opportunities for leakage of threats from robust into vulnerable networks" (Sicker and Lookabaugh 2004, p. 62).

A Pilot Study: Interviews

Our study shows that there is a need for continues security thinking in terms of awareness, assessment and challenges that are new dimensions for security in IoT. We highlight our pilot study data and classify the practitioners' insights based on these three dimensions.

Awareness is about *introducing security awareness* in order to cultivate security mindset among IoT practitioners, such as by providing appropriate security training (R3). Security should be introduced in a form of *security as a process* aspect that would help thinking about security from the initial design phase and throughout the development lifecycle (R3). Developers should understand the context and then apply security patterns, mechanisms and tools that work for their team (all respondents). This is especially important in IoT as often it is not possible to state general practices or guidelines for designing secure IoT system (R1, R3). *Learn by observing* instead of reinventing the wheel is another aspect, as there is a need to look at the success models because often the problems IoT practitioners face are already encountered and solved in other mature industries (R3). *Addressing the digital divide* aspect deals with IoT practitioners that need to have larger responsibility for securing IoT users, mainly because of their various levels of understanding the security and privacy risks (R1, R4). Security is a continuous process, thus *keep secure always* aspect could enable timely upgrades and updates of the system by issuing necessary and critical fixes (all respondents). Security fixes must be enforced on the IoT users to keep their system always secure (R4). *Plan for end-to-end* security should be designed and implemented addressing all the components of an IoT ecosystem, from the end-user to devices to network, and so on (R4). Once security awareness is created next dimension to consider is assessment, which involves assessment of security risks, tools, trust, data, and related.

Assessment for IoT developers should let them think about necessary *tools and software assessment*. A security toolbox helps practitioners conduct e.g., threat modeling, architectural review, code review, and running automated security tests (R3). *Security risk assessment* e.g., by incorporating threat modeling iteratively, system architecture reviews, and other related mechanisms (R3, R4). Based on the results of risk assessment, practitioners need to frame security requirements on the system and platform (R3). With *trust management* developers need to manage and assess device trust, entity trust, data trust and include strong authenticity into the system (R1, R2). IoT stakeholders should think about *data assessment* aspects as well, in order to assess data for its correctness, trustworthiness, and reliability (R1, R4). *Security audits, certifications and approvals* as governance procedures are needed to oversee and strengthen the implementation of IoT security (R3, R4). In the process of implementing security thinking in IoT, one can encounter various challenges related to resource constraints, operational environment and heterogeneity (Varshney 2018).

Challenges related to *resource constraints* such as processing power, battery, memory, space, etc., that put restrictions on the type of security solutions that can be used (R1, R2, R4). Challenges related to *operational environment* in terms of complex, dynamic and distributed execution environment poses further issues on usage of existing security and privacy mechanisms (all respondents). *Migration to public networks* aspect is related to most connected systems that are migrating towards public networks. While this offers cost benefits for the technology providers, it may expose the system to new malicious threat agents (R3). Moreover, some IoT devices are not originally designed to be connected to public networks (R1). Hence, appropriate mechanisms should be implemented to protect against attacks related to public network. Challenges related to *heterogeneity* where multitude of standards makes existing security and privacy tools and mechanisms to be insufficient (R4). *Fragmentation* of IoT market with incompatible devices, platforms and protocols impose further challenges in implementing effective security measures (R1, R2). *Multiple Verticals* systems as created by IoT stakeholders contributes to fragmentation and interoperability problems within the IoT industry creating standardization challenges (R2).

DISCUSSION AND CONCLUSION

Reflecting upon our conceptual framework we consider that security is hard to be achieved specifically in the field of IoT. This is mainly due to constantly evolving new technologies and platforms that create extreme heterogeneity and fragmentation due to lack of standardization. The dynamic nature of IoT brings a need to have a new security thinking into this area. In terms of describing security thinking, the results of our study show that when it comes to secure IoT development there is a need for continuous security thinking in terms of awareness, assessment and challenges. Increased awareness of security aspects is crucial for IoT developers and end-users to help reduce security risks. The best way to keep security on different stakeholders' attention is to offer continuous security awareness, training and education programs. Practitioners of IoT products and services should have designed-in security concepts in mind. For raising awareness, there is a need to continuously think about several more aspects, particularly for data management, team management, legal frameworks, policy enforcements and ethical concerns. Next, assessment becomes key where practitioners always need to have in mind identity management, risk management, trust management, certifications and last but not least the compliance aspects. Assessment is useful as a mechanism for evaluating the effectiveness of security controls. Finally, challenges inform us that the IoT itself is a new environment, but with continuous challenges that often foregoes rules on how technology should be handled.

Continuous challenges such as resource constraints and heterogeneity of devices, protocols and standards add to the difficulty of securing the IoT infrastructure.

Autonomous systems, from cars to pacemakers can become serious malfunctioning systems, led by weak security thinking. While such failures often become headlines in the press, they have yet to receive full attention by the IoT community to bring security thinking at the forefront. In this study, we show that novelty and risks concurrently target security in the IoT, and thus the importance of the three identified dimensions: awareness, assessment and challenges, together with a number of aspects, uplift continuous security thinking. We consider that our findings make an attempt to reverse the mindset that security is not guaranteed in IoT systems, particularly that the three dimensional model can help pave the way for a future robust and secure IoT system. It is often reported that the speed of IoT technology surpasses the capacity for the existing security requirements to keep the technological environment more secure. With continuous security thinking at hand, we foresee that an IoT security agenda can be built beforehand as a precursor to secure IoT technological developments.

The results of this study anchor an important, yet an often overlooked IoT technological development at a crucial phase: continuous security thinking. Putting attention on how to design more secure IoT technological systems can push future studies to develop specific measures to objectively test how security thinking can turn into action. Future research can also attempt to measure the impact continuous security thinking has on actual IoT security by observing the activities performed by the users. With IoT gaining reputation for insecurity, our study can be seen as a result of reversing that effect in the future.

REFERENCES

Agarwal, Y., & Dey, A. K. (2016). “Toward Building a Safe, Secure, and Easy-to-Use Internet of Things Infrastructure,” *IEEE Computer Society*, *49(4)*, 88–91.

Aggarwal, C. C., Ashish, N., & Sheth, A. (2013). "The internet of things: A survey from the data-centric perspective," *Managing and mining sensor data,* 383–428.

Alaba, F. A., Othman, M., Hashem, I. A. T., and Alotaibi, F. (2017) "Internet of things security," *Journal of Network and Computer Applications*, 88, 10–28.

Ali, I., Sabir, S., & Ullah, Z. (2016). "Internet of things security, device authentication and access control: a review. *International Journal of Computer Science and Information Security*, *14*(8), pp. 456-466.

Benson, K., et al. (2015). "SCALE: Safe community awareness and alerting leveraging the internet of things," *IEEE Communications Magazine*, *53*(12), 27–34.

Brahima. S. (2017) "ICT Facts and Figures," Technical report. (http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf, accessed October 15, 2018).

Bugeja, J., Jacobsson, A., & Davidsson, P. (2018). "Smart Connected Homes." *Internet of Things A to Z: Technologies and Applications*, pp. 359-384.

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). "Management of Information Security: Challenges and Research Directions," *Communications of the Association for Information Systems*, *20*(20), pp. 958–971.

Devine. S. M. (2018) "Open Source and the Internet of Things," *Network Security* (2), 14-19.

Dhillon, G. and Backhouse, J. (2001) "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* 11(2), 127-153.

Dhillon, G., Lemuria C., and Javad Abed, R.S. (2016). "Defining Objectives For Securing The Internet Of Things : A Value-Focused Thinking Approach," *WISP Proceedings*, *3*.

Harbers, M., Bargh, M., Pool, R., Van Berkel, J., Van den Braak, S., & Choenni, S. (2018). "A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges," Proceedings of the 51st Hawaii International Conference on System Sciences

Hoepman, J. H. (2014). Privacy design strategies. *IFIP International Information Security Conference*, pp. 446–459.

Izosimov, V., & Törngren, M. (2016). "Study of Security-Awareness in Cyber-Physical Internet of Things. *Proceedings of the TRUDEVICE 2016 Workshop*.

Kajtazi, M., Cavusoglu, H., Benbasat, I., and Haftor, D. (2018). "Escalation of Commitment as an Antecedent to Noncompliance with Information Security Policy" *Information and Computer Security* (26:2) pp. 171–193.

Kaleta, J. P., Thackston, R., & Ojagbule, O. (2018). "Exploring user privacy based on human behavior with internet of things devices at home (formative research) ," pp. 3–23.

Kounelis, I., Baldini, G., Neisse, R., Steri, G., Tallacchini, M., & Pereira, A. G. (2014). "Building Trust in the Human?Internet of Things Relationship," *IEEE Technology and Society Magazine*, *33*(4), pp. 73–80.

Kumar, S. A., Vealey, T., & Srivastava, H. (2016). "Security in internet of things: Challenges, solutions and future directions," *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2016–March* (October 2017), pp. 5772–5781.

Lowry, P. B., Dinev, T., and Willison, R. (2017). "Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) artefact: Proposing a Bold Research Agenda," *European Journal of Information Systems* (26:6).

Lucero, S (2016). "IoT platforms: enabling the Internet of Things," *IHS Technology*. (https://cdn.ihs.com/www/pdf/enabling-IOT.pdf, accessed December 2, 2018).

Miorandi, D., Sicari, S., Pellegrini, F. D., and Chlamtac, I. (2012) "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks* 10(7), 1497-1516.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly*, *42*(1), pp. 285–311.

Peisert, S., Margulies, J., Nicol, D. M., Khurana, H., & Sawall, C. (2014). "Designed-in security for cyber-physical systems," *IEEE Security and Privacy*, *12*(5), pp. 9–12.

Porras, J., Pänkäläinen, J., Knutas, A., & Khakurel, J. (2018). "Security In The Internet Of Things - A Systematic Mapping Study," *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 3750–3759.

Petersen, H., Baccelli, E., and Wahlisch. M. (2014) "Interoperable Services on Constrained Devices in the Internet of Things," *Workshop on the Web of Things*, pp. 1-3.

Sfar, A. R., Natalizio, E., Challal, Y., and Chtourou, Z. (2018) "A Roadmap for Security Challenges in the Internet of Things," *Digital Communications and Networks*, pp. 118–137.

Sicari, S., Rizzardi, A., Griecob, L. A., and Coen-Porisinia, A. (2015) "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, 76(15), 146–164.

Simmonds, A., Sandilands, P., & Van Ekert, L. (2004). "An ontology for network security attacks," *Asian Applied Computing Conference*, pp. 317-323.

Sicker, D. C., & Lookabaugh, T. (2004). "VoIP Security: Not an Afterthought," *Queue*, *2*(6), 56.

Spanaki, K., Gurguc, Z., Mulligan, C., and Lupu, E. (2017). "Organizational Cloud Security and Control: A Proactive Approach," *Information Technology and People.*

Stallings, W.; Brown, L. "*Computer Security: Principles and Practice*," 3rd ed.; Prentice Hall Press: Upper Saddle River, 2014.

Kolias, C., Stavrou, A., Voas, J., Bojanova, I., & Kuhn, R. (2016). "Learning Internet-of things Security "Hands-On",". *IEEE Security & Privacy*, 14(1), pp. 37-46.

Törngren, M., et al. (2015). "Education and training challenges in the era of Cyber-Physical Systems," *Proceedings of the WESE'15: Workshop on Embedded and Cyber-Physical Systems Education - WESE'15*, pp. 1–5.

Van Dijck, J. (2013) "The Culture of Connectivity. A Critical History of Social Media," *New York: Oxford University Press*.

Vogel, B., and Gkouskos, D. (2017). "An Open Architecture Approach: Towards Common Design Principles for an IoT Architecture," *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings* (pp. 85–88). ACM.

Vogel, B., Varshney, R. (2018). "Towards Designing Open and Secure IoT Systems: Insights for Practitioners," *In Proceedings of the 8th International Conference on the Internet of Things (IOT '18)*. ACM, Article 36, 6.

Varshney R. (2018). "Towards Designing Open Secure IoT System - Insights for practitioners," pp. 1–147, 2018.

Wan, J., & Zeng, M. (2015). "Research on Key Success Factors Model for Innovation Application of Internet of Things with Grounded Theory," *WHICEB 2015 Proceedings*. Weber, R. (2010). "Internet of Things – New security and privacy challenges," *Computer Law & Security Review,*" 23–30.

Weiser, M. (1991). "The computer for the 21st century. *Scientific American*, *265*(3), 94–104.