Security Challenges in IoT Development: A Software Engineering Perspective

Anh Nguyen Duc*
Department of Computer and Information Science (IDI), NTNU.
Trondheim, Norway, Sør-Trøndelag, Norway NO-7491
anhn@idi.ntnu.no

Ronald Jabangwe†
Lero - The Irish Software Research Centre,
Regulated Software Research Centre,
Dundalk Institute of Technology.
Dundalk, Co.Louth, Ireland
ronald.jabangwe@dkit.ie

Pangkaj Paul‡
Lero - The Irish Software Research Centre,
Regulated Software Research Centre,
Dundalk Institute of Technology.
Dundalk, Co.Louth, Ireland
pangkajchandra.paul@dkit.ie

Pekka Abrahamsson
Department of Computer and Information Science (IDI), NTNU.
Trondheim, Norway, Sør-Trøndelag, Norway NO-7491
pekka.abrahamsson@idi.ntnu.no

ABSTRACT

The rapid growth of Internet-of-things (IoT) software applications has driven both practitioners and researchers' attention to methodological approaches for secure IoT development. Security issues for IoT is special in the way that they include not only software, but also hardware and network concerns. With the aim at proposing a methodological approach for secure IoT application development, we investigated what are security challenges in the context of IoT development. We reviewed literature and investigated two industry cases. The preliminary finding results in a list of 17 security challenges with regards to technical, organizational and methodological perspectives. Cross-case comparison provides initial explanation about the less emphasis on methodological and organizational security concerns in our cases.

KEYWORDS

Software Security, Security method, Security challenge, Internet-of-Thing, IoT, Software Engineering

ACM Reference format:
Anh Nguyen Duc, Ronald Jabangwe, Pangkaj Paul, and Pekka Abrahamsson. 2017. Security Challenges in IoT Development: A Software Engineering Perspective. In *Proceedings of XP '17 Workshops, Cologne, Germany, May 22-26, 2017,* 5 pages.
DOI: .1145/3120459.3120471

*Dr. Anh Nguyen Duc's second affiliation is Department of Business Administration and Computer Science, University College of Southeast Norway, Bø i Telemark, Norway
†Dr. Ronald Jabangwe's second affiliation is Software Engineering Research Lab Sweden, Blekinge Institute of Technology, Karlskrona, Sweden. Email address: ronald.jabangwe@bth.se
‡Pangkaj Paul's second affiliation is STATSports International, 1 Courtney Hill, Newry Co. Down, N. Ireland.. Email address: p.paul@statsports.com

XP '17 Workshops, Cologne, Germany

DOI: .1145/3120459.3120471

1 INTRODUCTION

Modern software-intensive organizations worldwide are moving towards development approaches that capture both agility and customer value. A popular fast-faced development approaches, such as Agile, DevOps and Lean Startup, with frequent release and fast feedback facilitate change management and increase productivity. However, agility can have severe adverse effects on the strength of security [1]. The security flaws increase as the software evolves through multiple iterative changes if they are not addressed. The picture of software industry nowadays is much larger with the rapid growth of IT products and services delivered on sensors and IoT technologies. The number of connected devices available in worldwide market is approaching 15 billion [9], illustrating the significant role of IoT application in software industry. IoT applications, for instance, smart home solutions, need to consider a comprehensive system, from a cloud-based storage and data analysis, end user applications, middleware and hardware devices and their connectivities. Integrating of IoT hardware-related features into software-based development and release cycles would be of concern from both practitioners and researchers. Moreover, the heterogeneousity of players in IoT market, from large companies, such as Siemens, Philips and Bosch, to SMEs and startups, means no-size-fit-all methodological approaches [7].

The awareness and concern by both researchers and practitioners of security has been increasing in recent years [10]. The number of reported security vulnerabilities in software systems is on the rise, which is consistent with the perception that software is developed with security as an afterthought. With the popularity of IoT and increase in sensitive data being collected and stored, security is becoming more and more important. In such applications, the border between software and hardware parts are less visible. Consequently.

the consideration of security concerns needs to be in a holistic view and take into account the idiosyncrasies of IoT [7].

We are interested in tackling the security concern and integrating security assurance approaches into IoT application development. As a first step, this paper particularly focuses on identifying security challenges and possible solutions in addressing security concerns in IoT application development. Our research question is: **RQ:** *What are security-related challenges in fast-faced development of IoT applications?*. The paper is organized as follows: Section 2 presents background on fast-faced software development, with Agile and DevOps, and security concerns. Section 3 describes two IoT case companies. Section 4 presents security-related challenges. Discussion and conclusion is presented Section 5 and Section 6, respectively.

2 BACKGROUND AND RELATED WORK

Enabling various devices to exchange data and to communicate over the Internet is the basis of Internet-of-things [15, 17]. Sun and Wang [15] defines IoT as a network of sensors or other information sensing equipments, as agreed in the protocols and any objects connected to the Internet, exchange information and communicate with each other to realize the intelligent identification, location, tracking, monitoring and management of the objects. IoT adoption has spread across a wide range of domains, not just household use, but also to regulated domains, e.g., medical and health-care [6].

In terms of security for IoT applications we are referring to software security, specifically the practice of implementing measures throughout the software development process to ensure that core security goals are achieved [12, 14]. These core goals are generally, confidentiality, integrity and availability [14]. The measures implemented for improving security are referred to security controls, which are safeguards to counter or to mitigate security risks that may compromise the confidentiality, integrity and availability of the system and its data [11].

IoT applications are complex systems with multifaceted architectural and abstraction layers, hence ensuring their software security is challenging [2, 4, 8, 17]. It is even more difficult to maintain and to improve their security when there are frequent software changes, which is the case in agile environments [1]. Adelyar and Norta [1] found that agile practices were linked to issues that could manifest into severe security flaws. Realizing the importance of security and prevalence of agile practices, other researchers have focused on tailoring agile approaches to ensure software security, e.g., Beznosov [3] and Ghani et al. [5]. Beznosov [3] proposed Extreme Security Engineering, which adopts agile software development and eXtreme Programming into security engineering. Ghani et al. [5] modified the roles and practices for eXtreme Programming by introducing a new role titled "Security Master" to specifically focus on ensuring that software security concerns are addressed throughout the process. Therefore, there are studies focusing on agile and security, however, there is still a need to better understand specific security-related challenges that can be addressed by tailoring agile practices.

3 METHODOLOGY

The list of challenge was initiated by looking at SE literature. We identified a set of security challenges that have been experienced in industrial projects [6, 8, 15, 17]. With little knowledge on the topic, we conducted two exploratory case studies with startups as a unit of analysis. The cases were selected because (1) they developed software solution based on connected devices, and (2) our close contact with the CEOs, which enabled insight from the cases. The data was collected via interviews with CEOs and CTOs of the startups.

Case1: STATSports, referred to as Case1 from here on in, is a startup company that has quickly grown to be one of the leading suppliers of performance tracking and monitoring systems for elite sports. Due to the success of their systems, they are expanding into the area of IoT. They are currently in the planning phase of the development of a wireless body-area-network that will be connected to a cloud-storage system. The system will enable multiple users with access to a mobile application or a computer desktop web-browser to monitor the performance, movement and health information of elite sports players in real time through the cloud-storage system.

Case2: Aquaccare, referred to as Case2 from here on in, is a Trondheim-based startup in aquaculture. The company is developing a water environment monitoring and peer-to-peer consultancy application for South-East Asian market. The company was selected as top 20 IoT startups in Vietnamese startup contests and funded under Korean goverment's incubator program. The company is finalizing a Minimum Viable Product (MVP) for fund raising by March 2017. The current teams included three software engineers, one electronic engineer and a UX designer.

In the first case (STATSports), we were able to have multiple insights as two of the co-authors, the second and the third authors, are working as a security researcher/consultant and a developer, respectively. In the second case (aquaccare.com), the first author was a part of the management board, which enables the understanding on product prototyping and development.

The challenges were placed into categories. The categories emerged from the data and were constructed 'a posteriori'. They were then placed in a table to enable a cross-case comparison of the challenges. The approach followed is common in coding of qualitative data [13]. The list was also refined based on input from practitioners from the two case companies and other security researchers at Norwegian University of Science and Technology and Regulated Software Research Centre, as well as practitioners from a Norwegian company Nordic Semiconductor to look at the list. The list is also public to a Quora forum for open discussion.

4 SECURITY-RELATED CHALLENGES IN IOT

Security-related challenges were found under three categories, namely methodological, organizational and technical challenges, as shown in Table 1. The asterisk (∗) in column four and five represents the relevance of the challenges in each case (Case1 and Case2). Methodological challenges relate to the difficulties companies found in integrating security identification, analysis, testing and monitoring in their development methodology. Organizational challenges relate to company's policies, factors about market and

Table 1: List of Challenges with addressing security in IoT

Categories	Challenges	Description	Case1	Case2
Methodological	Incorporating security requirements in Agile software development process	Considering security as a backlog item in iterative development	*	
Methodological	Security assurance approaches	Security test is complex to define, plan and execute, involving security experts and other stakeholders	*	
Methodological	Run-time security	Security patches and updates need to be implemented and delivered timely during system operations	*	
Methodological	Security for legacy code	Adding security into an existing IoT infrastructure, significant change impact	*	
Methodological	Prioritizing security controls	Due to a vast number of security controls the challenge is prioritizing and release planning without compromising security properties for each release	*	
Methodological	Security requirement evolution	Security objectives, requirements, controls might change overtime	*	*
Organizational	Security for 3rd party components	Developers have no clue about how secure 3rd party components are	*	*
Organizational	Market-specific regulatory requirements and security standards, policies and goals	Market-specific regulatory compliance and security standards, policies and goals need to be taken into consideration	*	*
Organizational	Variety of bespoken security requirements	Security requirements vary from different customers, different application domains		*
Organizational	Human factors in operating security	Threats related to permission, priviliges and access control during system operation	*	
Technical	Comprehensive understanding of the architecture for IoT security	architectural consideration of security at sensor, network, application and data storage level	*	*
Technical	Ensuring data security	Identifying and implementing appropriate security controls in order to ensure data confidentiality, integrity and availability	*	*
Technical	Network portability	network size and structure in an IOT system can dynamically change.	*	*
Technical	Inter-related to other non-functional requirements	Security is often closely related to safety and privacy	*	*
Technical	Physical resource constraints	Security mechanisms for IoT nodes, which are often limited by physical memory constraints, computational powers and storages	*	
Technical	Heterogeneous and distributed systems	IoT application heavily builds on top of machine-to-machine communication, which adds a level of complexity in terms of mitigating security-related threats	*	
Technical	Complex data-flow	Understanding the data flow around their system and what assets need to be protected	*	

external stakeholders. Technical challenges relate to specific security concerns when designing and implementing IoT applications.

In Case1, there appears to be more demands at methodological and organizational levels than the ones in Case2. This is most likely because of the difference in the target markets. The customers for Case1 have a high demand on data security because their product will collect and analyze sensitive data, such as health information. Hence, both the IoT application as well as the testing and development process need to comply with regulatory requirements and standards. This is because the final product needs to comply with regulatory requirements for software security and data protection in both the European and US market. Thus it is not surprising that Case1 currently faces more security-related challenges than Case2. In addition, Case1 appears to be more in need of tailoring their current agile development process to address their security challenges. Case2 seems to be more focused on technical challenges. At present the company has not yet considered delivering security as part of sprint delivery. There are no security specific tests and code reviews. In organizational perspective, both companies are concerned with the adoption of OSS (open source software) components as some of them lack security-related documentation. For Case2 the hidden security challenge lies in the fact that they are targeting several different Asian markets with unclear security regulations.

5 DISCUSSION

The preliminary investigation on the cases gave an impression that security is less concerned in comparison to functional and other non-functional requirements. Even though security was mentioned as an important value for the IoT products, it seems to be insufficient practical consideration of security during product development. Our two cases are characterized as early stage startup product development, so there would be limitation in applicability of security concerns for legacy code or various customer requirements. The small scale development in our cases might limit methodological demands, i.e. security engineering and processes. It seems that security is viewed from a static snapshot of product development, without taking into account organization, human and other context factors.

While considering security as a non-functional requirement, security assurance can leverage existing requirement engineering techniques, processes and practices. Security bugs can be treated as other issues in issue tracking systems. We argue that emerging security challenges, is the consideration of security assurance in IoT context, where software and hardware plays a inseparable role in providing customer value. Security concerns in IoT application is also unique in the comparison to sensor networks or mobile communication networks due to the concerns at application and cloud layers. Moreover, IoT applications are domain specific, so the security assurance approach need to take into account the context. The specific yet comprehensive concerns on security would be a methodological challenge for IoT development.

Jacobson argues that domain-specific approaches are needed to address IoT-related challenges [7]. Current security engineering approaches, especially in embedded systems, can be formal and laborious. Given that many companies are using or switching to Agile method, the question is how to tailor the methods to tackle security-related challenges that IoT companies are facing. Such companies might spend days in their Sprints to identify and resolve security threats. We propose an iterative and continuous approach to addressing security, which is an adaption of iterative software development and continuous delivery. This will promote awareness of security concerns and improve the likelihood of delivering secure IoT applications. The approach should also take into account IoT-specific security threats by adopting steps from threat modeling [16], which is a key aspect of security engineering. Identifying and implementing appropriate security controls to ensure regulatory compliance for certain target markets should be part of the process. It is important to note that this will mitigate the security-related challenges that we have classified as methodological and organizational. The technical challenges need more technological focus rather than a process-oriented solution.

6 CONCLUSION

Methodology for securing IoT application appears as a quickly emerging research topic. We studied literature in software and system engineering and two IoT startup cases to explore security-related challenges during product development. We identified and discussed 17 security challenges in technical, organizational and methodological categories. The preliminary result in two cases showed that companies would need supports with tailoring a process to address these challenges.

Although the challenge list was formed from both literature and expert opinions, the security challenges were mainly discussed in two early-stage IoT development projects. For the future work, we will investigate further the two cases and include other cases with various domain application and organizational sizes to validate our initial observation. The inclusion of projects in more mature stages, i.e. manufacturing and maintenance, might give different emphasis in our challenge list. We are also working towards a security engineering approach for Agile development. We also plan to proceed with the study by mapping current set of practices, processes to deal with such challenges.

ACKNOWLEDGMENTS

This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094 and co-funded under the European Regional Development Fund through the Southern and Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie). We appreciate Mr. Hung Bui from Nordic Semiconductor and security experts in Quora forums for constructive feedbacks on the challenge list. We also thank Dr. Fergal McCaffery the Director of the Regulated Software Research Centre, and is also affiliated with STATSports International and Lero.

REFERENCES

[1] S Hassan Adelyar and Alex Norta. 2016. Towards a Secure Agile Software Development Process. In *Quality of Information and Communications Technology (QUATIC), 2016 10th International Conference on the*. IEEE, 101–106.
[2] Subho Shankar Basu, Somanath Tripathy, and Atanu Roy Chowdhury. 2015. Design challenges and security issues in the Internet of Things. In *Region 10 Symposium (TENSYMP), 2015 IEEE*. IEEE, 90–93.
[3] Konstantin Beznosov. 2003. Extreme security engineering: On employing XP practices to achieve'good enough security'without defining it. In *First ACM Workshop on Business Driven Security Engineering (BizSec). Fairfax, VA*.
[4] Rajendra Billure, Varun M Tayur, and V Mahesh. 2015. Internet of Things-a study on the security challenges. In *Advance Computing Conference (IACC), 2015 IEEE International*. IEEE, 247–252.
[5] Imran Ghani, Nor Izzaty, and Adila Firdaus. 2013. Role-based Extreme Programming (XP) For Secure Software Development. *Special Issue-Agile Symposium* 25 (2013), 1071–1074. Issue 4.
[6] Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, and Silvana Andreescu. 2015. Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. In *Services Computing (SCC), 2015 IEEE International Conference on*. IEEE, 285–292.
[7] Ivar Jacobson, Ian Spence, and Pan Wei Ng. 2016. Is there a single method for the Internet of Things? *Ivar Jacobson International* (2016).
[8] Qi Jing, Athanasios V Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. 2014. Security of the Internet of Things: perspectives and challenges. *Wireless Networks* 20, 8 (2014), 2481–2501.
[9] Sam Lucero. 2016. IoT platforms: enabling the Internet of Things. *IHS Technology - Whitepaper* (2016), 1–21.
[10] Mohammad Alshayeb Nabil M. Mohammed, Mahmood Niazi and Sajjad Mahmood. 2017. Exploring software security approaches in software development lifecycle: A systematic mapping study. *Computer Standards and Interfaces* 50 (2017), 107 – 115. DOI : http://dx.doi.org/10.1016/j.csi.2016.10.001
[11] National Institute of Standards and Technology (Joint Task Force Transformation Initiative). 2014. Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. *Special Publication 800-53A, Recommendations of the National Institute of Standards and Technology*, 53A (2014), 487.
[12] James Ransome and Anmol Misra. 2013. *Core Software Security: Security at the Source*. CRC Press.
[13] Johnny Saldaña. 2015. *The coding manual for qualitative researchers*. Sage.

[14] Y Sattarova Feruza and Tao-hoon Kim. 2007. IT security review: Privacy, protection, access control, assurance and system security. *International journal of multimedia and ubiquitous engineering* 2, 2 (2007), 17–31.
[15] Xiangyu Sun and Changguang Wang. 2011. The research of security technology in the Internet of Things. In *Advances in Computer Science, Intelligent System and Environment*. Springer, 113–119.
[16] Frank Swiderski and Window Snyder. 2004. *Threat Modeling*. Microsoft Press, Redmond, WA, USA.
[17] Rolf H Weber. 2010. Internet of Things–New security and privacy challenges. *Computer law & security review* 26, 1 (2010), 23–30.