Editorial: Special Issue on Security and Privacy of IoT

Hua Wang^{1,2} · Zonghua Zhang³ · Tarek Taleb⁴

Published online: 19 August 2017
© Springer Science+Business Media, LLC 2017

1 Introduction

Recent years have witnessed the rapid development and deployment of the Internet of Things (IoT) thanks to the tremendous advancement of computer and communication technologies [4, 7]. Also, the proliferation of IoT devices in the past years, ranging from body sensors and wearable devices to home appliances and industrial monitoring sensors, has driven the rapid evolution of various computing paradigms such as pervasive and ubiquitous computing, mobile crowd sensing, edge computing, as well as the emergence of diverse applications and services like smart cities, eHealthcare, intelligent transportation systems [2, 6]. The resulting networking and computing paradigms, applications and services together have expedited the rising of the big data era, and significantly changed our daily life. For instance, the audio intelligent system of Amazon, Echo, can learn the habits of the customers so as to customise the unique audio services. Many other intelligent systems continue appearing [7].

Despite the technological and societal advantages and huge economical potentials of IoT, it is widely recognised that security and piracy has become one of the major concerns, which seriously impede the further development and deployment of IoT infrastructures, services, and applications [7]. Due to the intrinsic complexity and the huge amount of stand-alone devices involved in the IoT, the asymmetric advantages between Cyber defenders and attackers would

✉ Hua Wang
hua.wang@vu.edu.au

Zonghua Zhang
zonghua.zhang@imt-lille-douai.fr

Tarek Taleb
tarik.taleb@aalto.fi

¹ Department of Computer Science, Taiyuan Normal University, Jinzhong 030619, China

² Centre for Applied Informatics, College of Engineering and Science, Victoria University, Footscray, VIC, Australia

³ IMT Lille Douai, Institut Mines-Telecom, Paris, France

⁴ School of Electrical Engineering, Aalto University, Espoo, Finland

be definitely enlarged. Moreover, the extremely broad and unclear attack surface consisting of heterogeneous IoT device make it unprecedentedly challenging and costly to construct an in-depth defense line. A simple penetration to a single IoT device, by either exploring firmware misconfiguration or guessing password, may eventually lead to large-scale attacks. For example, the recent Mirai malware took advantage of the venerable IoT devices (e.g., digital camera) and launched destructive and massive DDoS attacks in the Internet, well demonstrating that IoT would potentially become the attractive targets, as well as the ideal and popular platform, for Cyber criminals in the near future [1, 5].

To date, lots of research attention to security and privacy of IoT have been drawn from many IoT key players, including device manufacturers, service providers and consumers. This special issue is dedicated to security and privacy issues of IoT, and is intended to gather the latest lessons learned, research efforts and contributions from industrial practitioners, academia researchers and other stakeholders to advance the state of the art, improve the security best practices, and develop novel security architectures, protocols, mechanisms, and standards. For example, it is meaningful to develop IoT use cases, covering architecture, communication protocols, applications and so on, and further conduct threat analysis for understanding the threat landscapes [3, 6]. As a matter of fact, many intelligent IoT devices nowadays are designed with ARM and Linux, which may contain a large number of vulnerable open source software especially the Linux kernels, thereby seriously threatening many IoT services and applications running with them [1]. It is also interesting to explore how the traditional security mechanisms, e.g., identity access management, intrusion detection and response systems, data encryption, security management, may encounter novel design requirements and challenges in IoT enabled use cases or scenarios [7]. Specifically, from a lifecycle management perspective, it is important to study how to achieve end-to-end (i.e., from IoT terminal devices to end users) security and privacy by ensuring authenticity, integrity, and confidentiality of the data collected from heterogeneous IoT devices, their secure transmission, integration, and aggregation at middleware and edge devices, as well as the privacy-preserving data analytics at IoT infrastructure. To do that, the straightforward applications of those existing crypto systems and protocols may not be efficient. It is rather imperative to develop a set of cryptographic primitives and protocols, which are expected to be data-driven, IoT context-aware, lightweight, mission-critical, energy-saving, and service-oriented.

2 Submissions

To tackle the identified challenges, we have solicited 26 high-quality submissions for this special issue, among which 11 have been finally accepted after a rigorous review process and a couple of rounds revisions. The selection process also took into account the topics of the submissions, with an intention to cover the scope as much as possible. In general, the 11 accepted submissions can be categorised into four categories in terms of their research topics. In the following, we will highlight the contributions of each paper.

The first category contains three papers, which address IoT security and privacy issues from an architectural perspective and are intended to protect IoT network as a whole by different approaches, e.g., data analytics and visualisation, cryptographic techniques, vulnerability analysis and security evaluation.

Paper “Traceability and Visual Analytics for the Internet-of-Things (IoT) Architecture” authored by Richard Lomotey, Joseph C. Pry and Chenshean Chai, a distributed n-tier IoT

ecosystem is considered, comprising of sensors, mobile devices, and cloud-hosted middleware. In particular, a provenance technique is proposed, which leverages the associative rules and lexical chaining methodologies to enable data traceability, as well as the detection of faulty data propagation, through the identification of propagation routes of data an object-to-object communications. By using visualisation tools, it is able to determine linkability and unlinkability between IoT devices.

Paper “An Infrastructure Framework for Privacy protection of Community Medical Internet of Things: Transmission Protection, Storage Protection and Access Control” authored by Fulong Chen, Yonglong Luo, Ji Zhang, Junru Zhu, Ziyang Zhang, Chuanxin Zhao, Taochun Wang, a set of cryptographic techniques is proposed to protect medical IoT with respect to data transmission, storage and access, including a multi-path asymmetric encryption fragment transmission mechanism, a distributed symmetric encryption cloud storage scheme and a dynamic access control scheme.

The third paper is focused on industry IoT (IIoT), which proposes a design called IIoT-SD to identify vulnerabilities in software and firmware of IIoT environment and measure security degree of sensitive information like passwords, so as to finally detect the leakage of sensitive information. The experiments conducted with IP cameras, smart meters, PLCs and smart routers demonstrate the effectiveness of IIoT-SD on detecting potential leakage of sensitive information. More details can be found in “IIoT-SIDefender: Detecting and Defense against the Sensitive Information Leakage in Industry IoT” authored by Le-Tian Sha, Fu Xiao, Wei Chen, and Jing Sun.

The second group of three papers is generally focused on the security and privacy of IoT terminals, i.e., smartphone apps and sensors.

Paper “Personalized App Recommendation Based on App Permissions” authored by Min Peng, Guanyin Zeng, Zhaoyu Sun, and Gang Tian presents a novel recommendation method based on the permissions of smartphone apps, their functionalities and the users’ interests, in order to better avoid downloading malicious apps. With the similar objective, the authors Xing Liu, Jiqiang Liu, Wei Wang, Yongzhong He, and Xiangliang Zhang study the sensor usage patterns by the Android apps in the paper entitled “Discovering and Understanding Android Sensor Usage Behaviors with Data Flow Analysis”. In particular, a tool called “SDFDroid” is designed to identify the types of the sensors used by the app and to generate the sensor data propagation graphs that are further used to discover the sensor usage patterns by the apps. Thus, the malicious third-party libraries misusing the embedded sensors can be potentially spotted. Considering the fact that many mobile apps use SSL to secure HTTP communications with the Web servers, while the inappropriate implementations and misconfigurations of the apps may make them vulnerable.

The third paper “An Automatically Vetting Mechanism for SSL Error-Handling Vulnerability in Android Hybrid Web Apps” authored by Yang Liu, Chaoshun Zuo, Zonghua Zhang, Xinshun Xu, and Shanqing Guo studies a particular SSL error-handling vulnerability in Android hybrid Web apps and proposes a hybrid approach that combines both static and dynamic analysis to detect the potentially vulnerable mobile apps.

The third category contains three papers, which aim at developing and designing effective cryptographic protocols and mechanisms to secure IoT applications or services. One of the major common concerns of these three papers is that the cryptographic operations must be computationally cheap, so that they can be implemented in resource-constrained IoT devices.

Paper entitled “DECENT: Secure and Fine-Grained Data Access Control with Policy Updating for Constrained IoT Devices” by Qinlong Huang, Licheng Wang, and Yixian Yang

proposes an access control mechanism based on hierarchical attributed based encryption (ABE) scheme to preserve the confidentiality of collected data in transmission and at the rest (i.e., stored at resource constrained IoT devices). The encryption and decryption operations are outsourced to the semi-trusted gateway and cloud servers, in order to reduce the computational overhead occurring at the IoT terminal devices. With a similar objective, the authors Kim Thuat Nguyen, Nouha Oualha, and Maryline Laurent propose an outsourcing mechanism for the encryption of ciphertext-policy ABE (attribute based encryption) in the paper entitled “Securely Outsourcing the Ciphertext-Policy Attribute-Based Encryption (CP-ABE)”, allowing the resource-constrained IoT devices to securely offload expensive encryptions to a semi-trusted party. Both theoretic analysis and experimental validations are provided in this paper, demonstrating that the proposed mechanism outperforms the existing one and can be applied in various IoT applications. Another big challenge in IoT is about secure data aggregation and transmission.

Paper “Trustworthy Service Composition with Secure Data Transmission in Sensor Networks”, the authors Tao Zhang, Lele Zheng, Yulong Shen, Yongzhi Wang, Ning Xi, Jianfeng ma, and Jianming Yong propose a distributed approach to enabling trustworthy service composition with secure data transmission. In particular, the rules for computing service trust and data trust are proposed based a multi-level trust model by analyzing their dependency relationships. Then each service component can be independently evaluated through a model checker, while the secure data transmission between different service components can be achieved thanks to an identity-based aggregate signature. Although secure data aggregation has been extensively studied in sensor networks, the authors experimentally demonstrated that their approach can achieve efficient trustworthy service composition with complex invocation structures, as well as cost-saving secure data transmission.

The arms race between attack and defence is endless, and the security researchers are always expected to study the novel attacks from attacker’s perspective. The last category is thus devoted to the novel attack variants in IoT, which contains two papers, which address different attacks from cryptographic and system perspective.

Paper “Practical Chosen-Message CPA Attack on Message Blinding Exponentiation Algorithm and Its Efficient Countermeasure” authored by Hui Wang, Wei Guo, Jizeng Wei is focused on side channel attacks, which often occur due to implementation errors of theoretically sound cryptosystems on embedded devices, e.g., smart cards, sensors or trusted platform. In particular, the authors propose a new chosen-message correlation power analysis (CPA) attack that combines the chosen-message method with CPA for side channel attack. The corresponding countermeasure is also proposed, implemented, and analyzed. This work clearly indicates that due to the limited computational resource of IoT devices, many crypto based security countermeasures may not be feasible and sufficiently efficient in realistic implementations even though they are theoretically sound.

Paper in this category is entitled “Spoofing Attacks and Countermeasures in FM Indoor Localization System” authored by Zi Li, Dingqi Pei, Yao Liu, which is essentially about spoofing attacks in indoor localization system. The authors study the specific FM-based indoor localization and found that an attacker can deceive a victim user to obtain a fake indoor location by remotely manipulating the received signal strength (RSS). Then the authors propose a two-layer detection system to defend against such spoofing attack, which firstly distinguishes the normal signal from attack/noise signal then further detects the attack signal.

List of Accepted papers (clustered into 4 categories)

[Cat. 1]

1. “Traceability and Visual Analytics for the Internet-of-Things (IoT) Architecture”, Richard Lomotey, Joseph C. Pry and Chenshean Chai
2. “An Infrastructure Framework for Privacy protection of Community Medical Internet of Things: Transmission Protection, Storage Protection and Access Control,” Fulong Chen, Yonglong Luo, Ji Zhang, Junru Zhu, Ziyang Zhang, Chuanxin Zhao, Taochun Wang
3. “IIoT-SIDefender: Detecting and Defense against the Sensitive Information Leakage in Industry IoT,” by Le-Tian Sha, Fu Xiao, Wei Chen, and Jing Sun

[Cat. 2]

4. “Personalized App Recommendation Based on App Permissions” authored by Min Peng, Guanyin Zeng, Zhaoyu Sun, and Gang Tian
5. “Discovering and Understanding Android Sensor Usage Behaviors with Data Flow Analysis,” Xing Liu, Jiqiang Liu, Wei Wang, Yongzhong He, and Xiangliang Zhang
6. “An Automatically Vetting Mechanism for SSL Error-Handling Vulnerability in Android Hybrid Web Apps”, Yang Liu, Chaoshun Zuo, Zonghua Zhang, Xinshun Xu, and Shanqing Guo

[Cat. 3]

7. “DECENT: Secure and Fine-Grained Data Access Control with Policy Updating for Constrained IoT Devices,” Qinlong Huang, Lichebng Wang, and Yixian Yang
8. “Securely Outsourcing the Ciphertext-Policy Attribute-Based Encryption,” Kim Thuat Nguyen, Nouha Oualha, and Maryline Laurent
9. “Trustworthy Service Composition with Secure Data Transmission in Sensor Networks,” Tao Zhang, Lele Zheng, Yulong Shen, Yongzhi Wang, Ning Xi, Jianfeng ma, and Jianjming Yong

[Cat. 4]

10. “Practical Chosen-Message CPA Attack on Message Blinding Exponentiation Algorithm and Its Efficient Countermeasure,” Hui Wang, Wei Guo, Jizeng Wei
11. “Spoofing Attacks and Countermeasures in FM Indoor Localization System,” Zi Li, Dingqi Pei, Yao Liu

Acknowledgements The guest editors would like to express their thanks to the Editor in Chief Professor Yanchun Zhang for giving them the opportunity to edit this special issue on “Security and Privacy of IoT”. Also, we gratefully thank the authors for submitting their work as well as the tireless reviewers who have constructively evaluated the papers within the stipulated time. Finally, we sincerely hope the reader will share our view and find this special issue very useful.

References

1. Hu, H., et al.: REPLACE: A reliable trust-based platoon service recommendation scheme in vanet. *IEEE Trans. Veh. Technol.* **66**(2), 1786–1797 (2017)
2. Huang, J., et al.: A probabilistic method for emerging topic tracking in Microblog stream. *World Wide Web.* **20**(2), 325–350 (2017)
3. Li, H., et al.: Multi-window based ensemble learning for classification of imbalanced streaming data. *World Wide Web.* 1–19 (2017)
4. Qin, Y., et al.: When things matter: A survey on data-centric internet of things. *J. Netw. Comput. Appl.* **64**, 137–153 (2016)
5. Sang, Y., et al.: Achieving probabilistic anonymity in a linear and hybrid randomization model. *IEEE Trans. Inf. Forensics Secur.* **11**(10), 2187–2202 (2016)
6. Wang, H., et al.: A flexible payment scheme and its role-based access control. *IEEE Trans. Knowl. Data Eng.* **17**(3), 425–436 (2005)
7. Wang, H., et al.: Special issue on Security, Privacy and Trust in network-based Big Data. *Inf. Sci. Int. J.* **318**(C), 48–50 (2015)