Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 6452157, 3 pages
https://doi.org/10.1155/2019/6452157

Editorial

Security, Privacy, and Trust on Internet of Things

Constantinos Kolias,[1] **Weizhi Meng**,[2] **Georgios Kambourakis**,[3] **and Jiageng Chen**[4]

[1]*Computer Science Department, University of Idaho, USA*
[2]*Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark*
[3]*Department of Information and Communication Systems Engineering, University of the Aegean, Greece*
[4]*School of Computer Science, Central China Normal University, China*

Correspondence should be addressed to Constantinos Kolias; kolias@uidaho.edu

Received 25 December 2018; Accepted 31 December 2018; Published 3 February 2019

1. Introduction

The ability of smart objects to stay connected to the Internet for purposes of transmitting and receiving data is referred to as the Internet of Things (IoT). As per recent estimates, the number of IoT devices will surpass 50 billion by 2020. Unsurprisingly, this mushrooming of IoT devices has drawn the attention of attackers who seek to exploit them for their own benefit, with the Mirai botnet being perhaps the most prominent example of IoT specific malware [1, 2]. Basically, IoT brings along a plethora of potential security and privacy risks to the end-users, including the unsanctioned access and abuse of private information, the enabling and strengthening of assaults against other systems, and the breeding of risks pertaining to personal safeness [3]. Especially, IoT facilitates the creation of an assortment of privacy risks to the consumer associated with the collection of personal and sensitive information, like their preferences, locations, habits, and so on. In the mid- or long-run these pieces of data can be used to, say, profile or impersonate the user or group of interest. On the other hand, such risks to security, privacy, and trust may significantly diminish end-user's confidence in IoT and therefore impede its full realization.

The feature topic at hand intends to promote the dissemination of the latest methodologies, solutions, and case studies pertaining to IoT security, privacy, and trust issues. Its objective is to publish high-quality articles presenting security algorithms, protocols, policies, frameworks, and solutions for the IoT ecosystem.

The goal of this special issue was to attract high-quality contributions from researchers working in the broad area of security, privacy, and trust for IoT ecosystems, including but not limited to (a) cloud computing-based security solutions for IoT data, (b) mobile service privacy for IoT devices, (c) standardization efforts related to IoT, (d) testbeds and case studies for IoT, (e) Intrusion detection for IoT, (f) trust management for IoT, and (g) virtualization solutions to IoT security

2. Submissions

This special issue presents high-quality articles describing security and privacy issues, attacks as well as their remedies for the IoT ecosystems. We received a total of 29 submissions and, after a rigorous review process, we selected 10 articles covering the subject from different perspectives, i.e., about 30% of all the submitted papers.

In "On the RCCA Security of Hybrid Signcryption for Internet of Things" by H. Dai et al., hybrid signcryption schemes are lucrative for protecting communications in IoT environments. Such schemes achieve multiple cryptographic services simultaneously but with much lower overhead than separate traditional cryptographic schemes. This attribute makes them ideal for resource-constrained environments. Unlike most approaches that verify such security schemes primarily against Chosen Ciphertext Attacks, this paper proposes verification against Repayable Chosen Ciphertext Attacks. Despite being a theoretically weaker security notion, it is "secure enough" for IoT applications and at the same time much more efficient.

In "A Hierarchical Matrix Decomposition-Based Signcryption without Key-Recovery in Large-Scale WSN" by C.

Yuan et al., identity-based encryption schemes present a great potential for wireless, low resources networks due to their lower resource requirements. However, such schemes assume that a central entity, namely, the Private Key Generator (PKG), maintains all private keys; therefore, it can easily impersonate any user. The paper proposes a novel signcryption technique based on hierarchical matrix decomposition to generate the keys for cluster head nodes. By limiting the control of central authorities on the private keys it becomes possible to solve the key escrow issue associated with such schemes.

In "A Blockchain-Based Contractual Routing Protocol for the Internet of Things Using Smart Contracts" by G. Ramezan and C. Leung, conventional secure routing protocols assume a central authority (CA) to facilitate the identification and authentication for each device in the network. Particularly, in the highly heterogeneous IoT environments the lack of a standardized central management system introduces the problem of trust. The paper proposes a blockchain based contractual routing protocol which operates in a fully distributed manner without requiring any trusted CA. The introduced protocol makes use of the smart contracts concept to discover a route to a destination or data gateway within heterogeneous IoT networks. The protocol is proven resistant to both Blackhole and Greyhole attacks.

While in "Shielding IoT against cyber-attacks: An event-based approach using SIEM" by D. D. Lopez et al., due to the high level of heterogeneity in IoT environments traditional security solutions cannot perform ideally. Security Information and Event Management systems seem to be an appealing solution; however, current practices known from conventional computer networks fail to take into account the possible correlations between IoT layers and the peculiarities of corresponding security events and attack surfaces. The paper proposes a custom-tailored security architecture and explores possible mappings between events, vulnerabilities, and attack surfaces for typical IoT ecosystems.

In "BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT" by Y. Zhang et al., cloud infrastructures are an indispensable component of IoT applications, yet they may not always be considered as fully trusted entities. This paper proposes a privacy-preserving and user-controlled data sharing architecture which permits detailed access control. The proposed approach is based on the Blockchain model and smart contracts to ensure the scalability of access control tables.

In "Towards Secure Network Computing Services for Lightweight Clients using Blockchain" by Y. Xu et al., the network-based service sharing paradigm may indirectly extend the abilities of the resource-constrained IoT devices; nevertheless it introduces additional risks since untrusted/unverified code can be loaded from the network and then be executed even natively. This paper proposes a novel blockchain-based secure service provisioning mechanism for protecting lightweight IoT devices from malicious or insecure services in network computing scenarios. The power of blockchain is primarily leveraged towards identifying and verifying the corresponding provider and service.

In "Security Vulnerabilities and Countermeasures for Time Synchronization in TSCH Networks" by W. Yang et al., numerous IoT applications require that all nodes must maintain high-precision time synchronization. Such communication systems suffer from time-synchronization attacks, primarily in single-hop pair-wise synchronization situations. The paper examines the security vulnerabilities of TSCH technology to identify the potential vulnerabilities and attacks. The corresponding security enhancements are also outlined and an authentication-based mechanism along with a clock-offset filter is proposed.

In "Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure" by I. Masood et al., Modern Wireless Body Area Networks (WBANs) systems extensively rely on cloud computing (CC) technologies to overcome their inherent computational constraints. Such hybrid infrastructures have been applied in the healthcare domain with great success, but at the same time, new threats against patient data privacy and security were surfaced. This paper surveys the techniques for patient data privacy and security in sensor-based cloud infrastructures. The paper also provides a framework for patient physiological parameters (PPPs) privacy and security particularly appropriate for such ecosystems.

In "Towards Privacy Preserving IoT Environments: A Survey" by M. Seliem et al., privacy is one pivotal requirement of IoT applications. One of the most essential concerns of IoT applications is the lack of control over raw personal data communicated from the sensors to the cloud application counterparts. This paper conducts a thorough survey of existing research and proposed solutions regarding privacy in IoT ecosystems, from a multipoint of view to outline the numerous associated risks and potential mitigations.

In "FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks" by N. T. Luong et al., IoT communications may sometimes be deprived of a centralized infrastructure thus completely relying on number of self-organizing nodes to form Mobile Ad hoc Networks (MANETs). Such types of networks are prone to request route flooding attack, a devastating attack which is trivial to initiate and challenging to remedy. The authors introduce the Flooding Attack Detection Algorithm (FADA) which is based on historical network traces and the k-NN algorithm to detect and isolate the malicious nodes in the network. Then a new routing protocol for such settings is introduced which incorporates FADA algorithm as part of its route request phase, minimizing the risk.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this special issue.

Acknowledgments

The guest editors would like to express their gratitude to SPTT editorial board for giving the opportunity to edit this special issue. Also, they wish to thank the authors for

submitting their work as well as the tireless reviewers who have constructively evaluated the papers within the short-stipulated time. Finally, they sincerely hope the reader will share their view and find this special issue very useful.

Constantinos Kolias
Weizhi Meng
Georgios Kambourakis
Jiageng Chen

References

[1] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: mirai and other botnets," *IEEE Computer Society*, vol. 50, no. 7, pp. 80–84, 2017.

[2] M. Antonakakis, T. April, M. Bailey et al., "Understanding the mirai botnet," in *Proceedings of the USENIX Security Symposium*, pp. 1092–1110, August, 2017.

[3] J. Voas, R. Kuhn, C. Kolias, A. Stavrou, and G. Kambourakis, "Cybertrust in the IoT Age," *The Computer Journal*, vol. 51, no. 7, pp. 12–15, 2018.