International Journal of Information Security (2020) 19:1–2
https://doi.org/10.1007/s10207-019-00472-9

EDITORIAL

Message from the guest editors

Takeshi Takahashi[1] · Rodrigo Roman Castro[2] · Bilhanan Silverajan[3] · Ryan K. L. Ko[4] · Said Tabet[5]

Published online: 12 October 2019

Cyberspace is an indispensable social infrastructure that consists of myriads of networked devices. The emergence of the Internet of Things (IoT) has drastically increased the number of such devices and significantly enriched human life. However, it also posed security concerns; many IoT devices being inherently vulnerable have become a huge threat to cyberspace. Indeed, cyber attacks on these devices are on the rise. Because of this and other reasons, IoT security is a very important topic that continues to be relevant today, with many security measures being studied and implemented. For instance, a national project called NOTICE has been initiated in Japan to identify vulnerable IoT devices and provide security warnings to the responsible persons. Still, security aspects of IoT-specific issues must be studied further to improve the security of today's hyperconnected cyberspace.

This special issue focuses on the research challenges and problems in IoT security. We solicited contributions from leading-edge researchers and accepted eight high-quality papers. Among these are six papers on the security aspect, and two papers cover the trust aspect in IoT. These papers provide cutting-edge research results in the field of IoT security and share valuable information with researchers as well as practitioners, standards developers, and policymakers.

The first paper "The IoT security gap: a look down into the valley between threat models and their implementation" by Peter Aufner, addresses three important issues researchers in the IoT security domain need to recognize. First, the existing threat modeling frameworks need to be advanced further to cope with IoT security needs. In particular, such frameworks need to take into consideration the hardware on which the software runs. Second, many academic papers do not elaborate on threat models despite various frameworks being available; there are no definitions of other problems that may exist and no explanations on why they are not relevant for a given research question. Third, IoT researchers need to consider the physical part in addition to the network part; security research mostly focuses on applying network attacks or software attacks to IoT and leaves out the new attack concepts that new devices bring with them. The author claims that these three issues need to be considered to provide a holistic picture of the threat landscape in the IoT domain.

The second paper "Key-Updatable Public-Key Encryption with Keyword Search" by Hiroaki Anada, Akira Kanaoka, Natsume Matsuzaki, and Yohei Watanabe, focuses on encrypted data. Secure search is an important functionality that allows cooperation among users' devices and non-trusted servers, such as IoT devices and cloud servers. One example of technology that facilitates such operations is public-key encryption with keyword search, or PEKS. However, many resource-constrained IoT devices may not be able to store keys in a tamper-proof manner. The paper illustrates such key-exposure problems on PEKS and introduces the concept of PEKS with a key-updating functionality.

The third paper "Protection against reverse engineering in ARM" by Raz Ben Yehuda and Nezer Jacob Zaidenberg, explores Man-at-the- Endpoint attacks on ARM-based systems, such as embedded and mobile devices, and focuses on protection against reverse engineering for the ARM platform. In particular, the authors present a method of applying a thin hypervisor technology as a generic security solution by port-

✉ Takeshi Takahashi
takeshi_takahashi@nict.go.jp

Rodrigo Roman Castro
roman@lcc.uma.es

Bilhanan Silverajan
bilhanan.silverajan@tuni.fi

Ryan K. L. Ko
ryan.ko@uq.edu.au

Said Tabet
Said.Tabet@dell.com

1 National Institute of Information and Communications Technology, 4-2-1 Nukuikitamachi, Koganei, Tokyo 184-8795, Japan

2 NICS Research Group, University of Malaga, Campus de Teatinos s/n, 29071 Málaga, Spain

3 Tampere University, 33014 Tampere, Finland

4 The University of Queensland, Brisbane St Lucia, QLD 4072, Australia

5 Dell Technologies, 176 South St, Hopkinton, MA 01748, USA

ing TrulyProtect, a microvisor that was initially designed for x86 environment, to the ARM platform.

The fourth paper "Feature Dynamic Deep Learning Approach for DDoS Mitigation within the ISP Domain" by Ili Ko, Desmond Chambers, and Enda Barrett, addresses DDoS attacks caused by compromised IoT devices. The paper introduces a stacked self-organizing map (SOM), which is a feature dynamic deep learning approach that utilizes Netflow data collected by the Internet service provider (ISP) to combat the dynamic nature of novel DDoS attacks. The proposed scheme can dynamically select features, helping to cope with evolving attacks that may pose different features. Also, in comparison with other existing models, the proposed mitigation system is assumed to be deployed within the ISP domain for greater efficiency.

The fifth paper "A Prototype Implementation and Evaluation of the Malware Detection Mechanism for IoT Devices using the Processor Information" by Hayate Takase, Ryotaro Kobayashi, Masahiko Kato, and Ren Ohmura, proposes a malware detection scheme that aims to suppress the consumption of hardware resources in resource-constrained IoT devices. The paper proposes a malware detection mechanism of extracting value from the processor to minimize the consumption of hardware resources by using hardware offloading. The prototype implemented on the open-source emulator QEMU can classify malware and benign programs by using processor information, as well as detect malware variants belonging to the same family.

The sixth paper "A Study of IoT Malware Activities Using Association Rule Learning for Darknet Sensor Data" by Seiichi Ozawa, Tao Ban, Naoki Hashimoto, Junji Nakazato, and Jumpei Shimamura, aims at discovering regularities in attacks from the big-stream data collected on a large-scale darknet by applying the association rule learning (ARL). By exploring these regularities in IoT-related indicators such as destination port, type of service (ToS), and transmission control protocol (TCP) window size, the activities of attacking hosts associated with well-known classes of malware programs can be discovered. Through experiments, the proposed scheme is demonstrated to be effective in early detection and tracking of new malware activities on the Internet (e.g., Mirai) and thus contributes toward automating and accelerating the identification and mitigation processes of new cyber threats.

The seventh paper "A Trust Management Scheme for IoT-Enabled Environmental Health/Accessibility Monitoring Services" by Behshid Shayesteh, Vesal Hakami, and Ahmad Akbari, addresses the trust challenges associated with IoT-enabled health and accessibility monitoring services. More specifically, the authors emphasize that trust management is a key success factor in such services as these services might be misused by malicious users through altered or fake sensor data. The authors propose a hybrid entity and data trust computation scheme for this particular context.

The eighth paper "TrUStAPIS: A Trust Requirements Elicitation Method for IoT," Davide Ferraris and Carmen Fernandez-Gago argue that it is desirable to guarantee trust during the entire life cycle of an IoT entity when developing it. Domains such as security and privacy need to be considered together with trust as a whole, and the right requirements should be elicited in the early phases of the system development life cycle. The paper introduces TrUStAPIS, a JSON-based requirement elicitation method that helps developers to elicit proper requirements during system development of an IoT entity.

Finally, in the ninth paper "An Elliptic Curve Cryptography based Enhanced Anonymous Authentication protocol for Wearable Health Monitoring Systems", Kan-disa Sowjanya, Mou Dasgupta, and Sangram Ray focus on the authentication of wearable medical devices. In particular, the authors analyze the security of an existing lightweight end-to-end authentication protocol, uncover its vulnerabilities, and propose an enhanced protocol that not only provides perfect forward secrecy but also reduces the overall complexity.

We believe the papers published in this special issue will contribute to the IoT security and trust research landscape and add to the development of a secure and healthy cyber society.