NCSIoT: Novel Cloud Approaches for Securing IoT Devices

Special Track running alongside CLOUD COMPUTING 2020, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization, October 25, 2020 to October 29, 2020 - Nice, France

Magnus Westerlund*, Bob Duncan†, Andreas Aßmuth‡ and Sebastian Fischer§

*Arcada University of Applied Sciences, Finland, Email: magnus.westerlund@arcada.fi
†University of Aberdeen, UK, Email: bobduncan@abdn.ac.uk
‡Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany, Email: a.assmuth@oth-aw.de
§Fraunhofer AISEC, Berlin, Germany, Email: sebastian.fischer@aisec.fraunhofer.de

***Abstract*—The field of Internet of Things (IoT) has both from a research and business aspect grown rapidly over the last decade. A major concern with the use of IoT has been the security of the technology. The use of IoT in safety-critical industrial and medical installations deserves a broad focus on the trustworthiness of such solutions. Considering the increase in the use of AI methods in combination with IoT will further demand a renewed focus on how we handle security in IoT systems. The special track "Novel Cloud Approaches for Securing IoT Devices (NCSIoT)" focuses on improving the understanding of trustworthy IoT. The special track has drawn great interest and include eight publications on topics that aim to deepen the understanding of how to improve security and reliability of IoT.**

***Index Terms*—Internet of Things, IoT, security**

I. Introduction

The proliferation of Internet of Things (IoT)-devices in society at large demands a renewed focus on securing and maintaining such systems. IoT-based systems are predicted to have a great impact on future business and the resilience of such systems must be guaranteed. This can be achieved by prevention, detection, response and mitigation of combined physical and cyber threats to IoT infrastructure.

The objective of the special track is to identify novel approaches for improving resilience in the evolving IoT domain. Such approaches can identify building blocks on a system or a device level. These building blocks can include intelligent security that actively and automatically adapts its own security. Introducing cryptographic-based building blocks that strive to ensure that distributed IoT networks remain in healthy condition throughout their lifecycle are of great importance. By supporting values of openness, automation, decentralization, inclusiveness and protection of privacy we can introduce novel means that reduces the threat of surveillance and theft, while also improving the level of trust for IoT technology.

In order to be agnostic in terms of sought solution implementations, this track extends the definition of cloud to include distributed cloud solutions. Traditional cloud architectures rely mainly on a conceptually centralized service provision model, while distributed clouds, e.g. based on distributed ledger technology (e.g., blockchain technologies) originate from a peer-to-peer and a completely distributed approach. The emergence of distributed clouds that are cryptographically secured through distributed ledgers may provide infrastructure for IoT solutions that provide more transparent and accessible services, more intelligence, greater involvement and participation.

II. Submissions

The paper, "A study about the different categories of IoT in scientific publications" [1], points out the difficulty for researcher to find the right kind of scientific publication for the intended category of IoT. Conferences, events, publications and even standardisation organisations suffer from the same problem, as it is not clear what target group is involved (e.g., consumer, enterprise, industrial). The authors started with some research in different research libraries and analysed the results. They found three important categories (consumer, enterprise and industrial), with which the publications can be distinguished. The different number of results in each library were given and additionally a manual study about 100 publications was done. The comparison with the results of the manual evaluation shows, that some search queries do not show all desired publications or that considerably more, unwanted results are returned. Most researchers do not use the keywords right and the exact category of IoT can only be accessed via the abstract. This shows major problems with the use of the term IoT and its minor limitations.

The second paper, entitled "Threat Analysis of Industrial Internet of Things Devices" [2], addresses the challenges of connecting Industrial Internet of Things Devices to Cloud services and the Internet in general. These so called opera-

tional technology (OT) devices have additional requirements in comparison to IT devices concerning security and safety. The authors explain these differences to traditional IT in their paper and provide a procedure for identifying and assessing threats and vulnerabilities that emphasizes the specialties of IIoT devices.

IoTAG, short for IoT Device IdentificAtion and RecoGnition [3], is a proposal for an open standard to detect IoT devices in an network and retrieve important security information about the device. These information range from the current software and firmware version to the used encryption and communication standards. The authors describe the proposed standard in detail an give information how to implement it into IoT devices. The goal of this project is to create an automated overview of an IoT network and rate the security for each device.

The paper "Development of a process-oriented framework for security assessment of cyber physical systems" [4], presents the required criteria for security assessment of cyber physical systems (CPS), the development of the process-oriented procedure for security assessment of cyber physical systems and the application of the security model. The requirement criteria for CPS are scalability, real-time, performance, functional safety and volatility. As the current models for data security are just two-level models, secure and insecure, new models are needed for the growing networking of systems. As a solution, they present a process-oriented procedure for security assessment and showed the application of the model using a use case from an research project.

Ahmed Alqattaa and Daniel Loebenberger present a concept of an IoT crypto gateway which sits in-between attached IoT devices and the Cloud in their paper "An IoT Crypto Gateway for Resource-Constrained IoT Devices" [5]. The task of this gateway is to secure the communication of potentially unsecure IoT devices and the Cloud services they are connected to. The gateway communicates with the Cloud implementing the Message Queuing Telemetry Transport (MQTT) protocol over a TLS 1.3 (Transport Layer Security) connection. In order to communicate with the attached IoT devices, the gateway uses MQTT over the Quick UDP Internet Connections (QUIC) protocol which is currently still being developed by IETF.

In the paper "Reliable Fleet Analytics for Edge IoT Solutions" Raj, Westerlund, and Espinosa-Leal [6] discusses a methodology for the use of AI in Internet of Things (IoT) services. Artificial Intelligence of Things (AIoT) combines Artificial Intelligence (AI) technologies and IoT infrastructure to provide robust efficient operations and decision making in various physical environments. Edge computing is emerging to enable AIoT applications to work in close proximity to the IoT installation. The paper proposes a framework to solve the demanding situations for facilitating machine learning at the edge for AIoT applications while continuously monitoring the health of the fleet. The design methodology used is Edge Machine Learning Operations (Edge MLOps) that enable continuous delivery, deployment, and monitoring of machine learning models at the edge of the network. The resulting architecture is verified through a use case that continuously predicts air quality conditions in different rooms. The obtained results indicate a stable and reliable architecture, incl. automated retraining and deployment of ML models that was performed according to specifications.

Leah Lathrop et al. investigate Physical Uncloneable Functions (PUFs) as a potential solution to securing devices against hardware attacks [7]. The authors have carried out a market analysis of products containing PUFs and present their key findings in their paper entitled "Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions". According to this market analysis, most of these integrated PUFs are still used in very rudimentary ways, although many different types of PUFs have been integrated into a variety of devices.

Bob Duncan, "Securing the Internet of Things from the Bottom Up Using an Immutable Blockchain-Based Secure Forensic Trail", has been investigating how to ensure that adding a secure Internet of Things system to an existing corporate system, can result in a strong overall system. Corporate systems seldom have the capability to ensure their forensic trail records can be kept complete and safe. The author proposes to achieve this using immutable forensic trail collection using Blockchain technology.

III. Conclusions

The NCSIoT special track includes a broad range of topics related to the security of Internet of Things. It contains both, academic research papers as well as studies from industry introducing interesting ideas for future work in this thriving research domain.

Acknowledgment

We would like to thank the organizers of Cloud Computing 2020 for their tireless efforts and for accepting NCSIoT as a special track. Last, but not least, we are very thankful to the authors for their very interesting contributions.

References

[1] S. Fischer, K. Neubauer, and R. Hackenberg. "A Study About the Different Categories of IoT in Scientific Publications," in Special Track: Novel Cloud Approaches for Securing IoT Devices (NCSIoT), along with Cloud Computing 2020. IARIA XPS Press, 2020.

[2] S. Liebl, L. Lathrop, U. Raithel, M. Söllner, and A. Aßmuth. "Threat Analysis of Industrial Internet of Things Devices," in Special Track: Novel Cloud Approaches for Securing IoT Devices (NCSIoT), along with Cloud Computing 2020. IARIA XPS Press, 2020.

[3] L. Hinterberger, S. Fischer, B. Weber, K. Neubauer, and R. Hackenberg. "IoT Device IdentificAtion and RecoGnition (IoTAG)," in Special Track: Novel Cloud Approaches for Securing IoT Devices (NCSIoT), along with Cloud Computing 2020. IARIA XPS Press, 2020.

[4] K. Neubauer, and R. Hackenberg. "Development of a Process-oriented Framework for Security Assessment of Cyber Physical Systems," in Special Track: Novel Cloud Approaches for Securing IoT Devices (NCSIoT), along with Cloud Computing 2020. IARIA XPS Press, 2020.

[5] A. Alqattaa, and D. Loebenberger. "An IoT Crypto Gateway for Resource-Constrained IoT Devices," in Special Track: Novel Cloud Approaches for Securing IoT Devices (NCSIoT), along with Cloud Computing 2020. IARIA XPS Press, 2020.

[6] E. Raj, M. Westerlund, and L. Espinosa-Leal. “Reliable Fleet Analytics for Edge IoT Solutions,” in Special Track: Novel Cloud Approaches for Securing IoT Devices (NCSIoT), along with Cloud Computing 2020. IARIA XPS Press, 2020.

[7] L. Lathrop, S. Liebl, U. Raithel, M. Söllner, and A. Aßmuth. “Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions,” in Special Track: Novel Cloud Approaches for Securing IoT Devices (NCSIoT), along with Cloud Computing 2020. IARIA XPS Press, 2020.

[8] R. Duncan. “Securing the Internet of Things from the Bottom Up Using an Immutable Blockchain-Based Secure Forensic Trail,” in Special Track: Novel Cloud Approaches for Securing IoT Devices (NCSIoT), along with Cloud Computing 2020. IARIA XPS Press, 2020.