University of Zurich[UZH]

Department of Informatics
University of Zürich UZH
Binzmühlestrasse 14
CH-8050 Zürich
Switzerland

Prof. Dr. Burkhard Stiller
Dr. Eryk Schiller
Dr. Bruno Rodrigues
Katharina Müller

Communication Systems Group
CSG@IFI
Head: Prof. Dr. Burkhard Stiller
Phone: +41 44 635 43 37 (E. Schiller)
Fax: +41 44 635 68 09
E-mail: stiller@ifi.uzh.ch
schiller@ifi.uzh.ch
rodrigues@ifi.uzh.ch
mueller@ifi.uzh.ch

URL: https://www.csg.uzh.ch/

Bachelor Thesis (Bachelorarbeit) for Armin Veres

Task Description:	Dr. Eryk Schiller
Title:	**Inventorying & Secure Life-Cycle of IoT Devices**
Start Date:	June 1, 2023
End Date:	December, 2023
Supervisor:	Dr. Eryk Schiller, Dr. Bruno Rodrigues, Katharina Müller
Location:	Home, Institut für Informatik (IfI)
Support:	References, Meetings, CSG Hardware Support

1. Introduction and Motivation

Countless Internet of Things (IoT) devices connect to the Internet daily, while people need to gather and process massive amounts of information from the real world. The advent of the 3rd Generation Partnership Project (3GPP) 5th Generation (5G) network, allowing for massive information exchange, is a game-changer in IoT. However, enhanced connectivity and widespread adoption of IoT stimulate cyber attacks, which get more sophisticated every day, thus affecting a large number of IoT-related infrastructures and raising security and privacy concerns of consumers and businesses. This highlights the importance of proper IoT security management, enhancing IoT infrastructures with continuous security improvements integrated into IoT lifecycle management. This is a challenging task considering IoT device heterogeneity, the dynamism of the security landscape, and the number of IoT stakeholders. Any security change caused by a new vulnerability or an insecure update (e.g., patch) on a single device can put the whole IoT system at risk.

Security management of IoT infrastructures encompassing the entire lifecycle of products and continuous certification are fundamental tools to guarantee a high level of security, as emphasized by the European Union Agency for Cybersecurity (ENISA) Cybersecurity Act (CSA) [1]. Indeed, a practical security framework must stimulate collaboration among IoT stakeholders (e.g., users, auditors, and manufacturers), as pointed out by the Network and Information Security (NIS) directive [2].

Therefore, providing access to cybersecurity information is crucial to foster the realization of a more homogeneous perspective on cybersecurity. CSA and NIS promote strategic cooperation among the stakeholders to support and facilitate information sharing. This approach

helps to respond to large-scale incidents by creating synergies, which can act more effectively against cybersecurity vulnerabilities.

2. Description of Work

This thesis will develop a service to support security information sharing between stakeholders to support the continuous security assessment throughout the IoT device lifecycle. In this thesis, we will consider Distributed Ledger Technology (DLT) as a promising approach to enable a trustworthy and transparent platform for sharing cybersecurity information among stakeholders without a trusted third party [3]. There is a need to integrate the presence of several entities owing different responsibilities and roles in sharing cybersecurity knowledge. While performing security monitoring activities, the user may detect vulnerabilities that will be shared with the manufacturer for further investigation and prompting mitigations or resolutions. Therefore, the device could be reconfigured throughout its lifecycle according to the changing threat landscape, according to device manufacturers publishing secure updates (i.e., patches) and device profiles.

Several standardization organizations have devoted efforts toward the progress of secure IoT deployment and bootstrapping. However, all the established approaches have significant challenges. On the one hand, using the same pre-shared credential for every device is the most straightforward approach, but it does not identify each device, nor does it give devices a way to verify that they are connecting to the correct network. This thesis will develop a bootstrapping service to provide a lightweight bootstrapping protocol, supporting different authentication methods depending on the device's characteristics and providing key management [4].

Due to the developed bootstrapping mechanism, the infrastructure will enable IoT inventorying. The infrastructure will keep track of all embedded IoT devices. The infrastructure should store security levels associated with each device. Furthermore, IoT devices' secure updating/patching process will be developed to ensure security throughout their lifecycle. Manufacturers and software providers will need to update the device's software to fix a security issue after an attack or vulnerability detection.

Most upgrading proposals are based on centralized models using client-server architectures. In contrast, this thesis will design a scalable and secure approach for disseminating software updates in scenarios with selected IoT devices. The upgrading process developed in this thesis shall be decentralized, robust, and efficient, bringing the upgrading functionality closer to the end devices. Blockchain technologies will be leveraged by providing a transparent ledger to manage the different versions of software elements composing an IoT device or system and share other relevant security aspects (e.g., vulnerabilities and device information). As interoperability is crucial, this thesis will analyze the use of Bifröst [5]/interledger [6] approaches to interconnect different blockchain implementations. Finally, this thesis will consider mitigations for IoT devices using the notion of threat Manufacturer Usage Descriptors (MUDs) proposed by the NIST [7] provides a flexible and dynamic way to alert about a new threat and the mitigations to apply before an update or patch is released. Threat MUD is intended to complement MUD files, dynamically reconfiguring the device when a new vulnerability is detected.

3. Bachelor Thesis Goals

This thesis will take advantage of a hyper ledger technology employed for device inventorying and identifying the required software patches/updates that must be installed on selected IoT devices. The hyper ledger technology between stakeholders (i.e., device manufacturer, consumer, auditor, and authorities) will allow enhanced device lifecycle management.

Designing device inventorying (to store and gather information about devices) and secure firmware upgrading is the critical component of this thesis. In the design of the system, several components of a modern IoT device, such as SE (i.e., cryptographic support providing cryptographic primitives of high performance) and the Trusted Execution Environment (TEE), such as commercially available ARM TrustZone, have to be taken into account [8]. Those features will enable secure functions such as

authentication, enrolling, inventorying, data authentication, and storage. Secure Over-The-Air (OTA) upgrade on the IoT device will also be provided. Furthermore, the device should verify the runtime integrity utilizing open attestation solutions leveraging the underlying hardware/firmware level security primitives. Finally, the deployment domain should obtain relevant security information about the newly onboarded IoT device (ID, behavioral profile, security policies, certificates). Those profiles should be used to appropriately configure the IoT infrastructure, i.e., allowing only legitimate use of the IoT device according to a given security requirement of the environment.

4. Activities and Milestones

Based on the description of the work, the following tasks targeting the critical milestones need to be accomplished:

Milestone 1: The definition of use cases completed, incl. actors, requirements, and functionalities

Milestone 2: Functional architecture developed

Milestone 3: Target IoT device selected

Milestone 4: Target hyper ledger platform selected

Milestones 1-4 need to be addressed by the end of the first month, and the output has to be presented as the initial version of the report.

Milestone 5: Specification & implementation of the DLT-based Configuration / Management Database (CMDB)

Milestone 6: Specification & implementation of the device onboarding

Milestone 7: Initial experimentation with the platform accomplished

For milestones 5-7, which need to be done in the second and third months, the student has to hand in the intermediate version of the report and present the progress in the first half of the thesis.

Milestone 8: Specification & implementation of the OTA Upgrading

Milestone 9: Specification & implementation of the MUD threat mechanism

Milestone 10: Experimentation of the integrated prototype completed

Milestone 11: Evaluation of the results focusing on different use cases

Milestone 12: Documentation of the developed approach and Final presentation. Note that documentation has to be done continuously during the project and always after having reached any of the above stated milestones. The completion of the thesis includes the full version of the thesis report in terms of introduction, motivation, final implementation, summary, bibliographic references, and lists of tables, figures, and other material needed within appendices.

5. General Notes

- **Schedule/Time Planning**: the student has to provide a written schedule for his/her full study steps within the first two weeks of his/her work. Clarify details with your supervisor and finalize the schedule of tasks, basically in a weekly fashion. Include the intermediate/public presentation(s), too.
- **Intermediate Presentation**: prepare an intermediate and internal presentation (20 min max plus Q&A) after half time of your study (date to be set) and discuss this with your supervisor. At the end (date to be set) a final public and self-containing presentation (20 min max plus Q&A) has to be given.
- **Report**: final written report will document all work undertaken and remember that this report must be self-contained. Major technical basics are to be included and detailed knowledge obtained during the work must be documented. Assumptions, design decisions, configuration choices, and results are part of the report as well as design details and usage information. Correct bibliographic references and a list of papers, recommendations, and descriptions used must be added, including those ones given below.

- **Period Meetings with Supervisors**: establish periodic meetings with the supervisor to report on progress, discuss current problems and request assistance when required.
- **Interaction**: the students involved in this thesis must participate actively and respond within 1 - 2 days. If needed, a more frequent interaction will determine a better basis for supervision and progress.

6. Formal Results

Besides the intermediate and final oral presentations, the following documents need to be handed-in to the supervisor before the final deadline:

- **Report Printed Copies**: double-sided report in a soft cover binding and in 3 copies (in English or German): the report must cover the milestones, a table of content and figures (including tables), a valid list of bibliographic references, and optional appendices as required is part of the report, too. The official acknowledgment section is mandatory, a personal one optional, however recommended, as usually a number of people took part in the process of finalizing the study. The text processing shall be done in LaTeX (preferred) or FrameMaker and in rare cases in Word.
- **Source-Code and Documentation**: A documentation of the design/configured system, covering the system's view point, a description, a use and installation manual, a documentation of all program and data structures developed or utilized is essential. All of this may be part of the report above, however, in case it will not be included, it must exist in a separate document.
- **Digital Copy**: a dedicated CD has to be produced containing (1) a collection of all program sources, software components, protocol design utilized, and documentation in PDF; (2) the written report in PDF or full HTML pages, a directory description if needed, figures in source file and JPG or EPS and a full printable PS as well as PDF file; (3) the set of slides for the final presentation in PPT (PowerPoint); and (4) all further material used, if available in electronic form, such as all existing and documented tested scenarios, plans, and results.
- **German Summary**: maximum of 2 pages (in case the report is written in German, the summary needs to be in English), which will enable a quick and clear overview of the work, tasks and results. The summary will be part of the bound report, and is included after the front page and before any other following text. It includes four short sections: 1. Einleitung/Introduction, 2. Ziele/ Aims and Goals, 3. Resultate/Results, and 4. Weitere Arbeiten/Further Work.
- **Hand-in**: The complete set of copies of the report, the CD, and the talk must be completed and handed in to the supervisor in time before the study will change into the "submitted" status. Note that failures of delivering those information and data after the formal hand-in time may result in a "non-passing" state of this work.

7. References

The following list of references addresses key aspects and serves as a starting point for the work. Further papers, scenarios, and document research is a must! It is more than highly recommended and may be essential for a successful completion of the work. The papers indicated in bold provide the essential information about this topic. Other references provide the background information as well as links to standards, hardware components, and implementation.

[1] The EU Cybersecurity Act, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act. Last accessed: May 25, 2023.

[2] Directive on measures for a high common level of cybersecurity across the Union, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. Last accessed: May 25, 2023.

[3] Ricardo Neisse, Gary Steri, and Igor Nai-Fovino. 2017. A Blockchain-based Approach for Data Accountability and Provenance Tracking. In Proceedings of the 12th International Conference on

Availability, Reliability and Security (ARES'17). Association for Computing Machinery, New York, NY, USA, Article 14, 1–10. https://doi.org/10.1145/3098954.3098958.

[4] Trusted IoT Device Network-Layer Onboarding and Lifecycle Management. https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management. Last accessed: May 25, 2023.

[5] E. J. Scheid, T. Hegnauer, B. Rodrigues and B. Stiller, "Bifröst: a Modular Blockchain Interoperability API," 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrueck, Germany, 2019, pp. 332-339, doi: 10.1109/LCN44214.2019.8990860.

[6] Siris, V. A., Nikander, P., Voulgaris, S., Fotiou, N., Lagutin, D., & Polyzos, G. C. (2019). Interledger Approaches. IEEE Access, 7, 89948-89966. [8755830]. https://doi.org/10.1109/ACCESS.2019.2926880.

[7] Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD), https://www.nist.gov/publications/securing-small-business-and-home-internet-things-iot-devices-mitigating-network-based. Last accessed: May 25, 2023.

[8] Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, Burkhard Stiller, Landscape of IoT security, Computer Science Review, Volume 44, 2022, 100467, ISSN 1574-0137.

Zürich, May 25, 2023

Prof. Dr. Burkhard Stiller