Demo: Secure Inventorying and Lifecycle Management of IoT Devices with DLT

Armin R. Veres[1], Daria Schumm[1], Thomas Grübl[1], Katharina O. E. Müller[1], Bruno Rodrigues[2], Burkhard Stiller[1]
[1]Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH
Binzmühlestrasse 14, CH—8050 Zürich, Switzerland
[2]Institute of Computer Science in Vorarlberg ICV, University St.Gallen HSG
Hintere Achmühlerstrasse 1b, AT—6850 Dornbirn, Austria
E-mail: [schumm,gruebl,mueller,stiller]@ifi.uzh.ch, armin.veres@hotmail.com, bruno.rodrigues@unisg.ch

2024 IEEE 49th Conference on Local Computer Networks (LCN) | 979-8-3503-8800-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/LCN60385.2024.10639716

***Abstract*—Security management of Internet-of-Things (IoT) infrastructures encompassing the entire lifecycle of products and their continuous certification are fundamental functions to guarantee a high level of security. This paper demonstrates a DLT-based platform enabling secure inventorying and management of IoT devices and sensors distributed across multiple stakeholders. This work makes use of the Hyperledger framework, Decentralized Identifiers (DID), and Manufacturer Usage Description (MUD) files for IoT device inventorying and the identification of critical software updates.**

I. Introduction

Countless Internet-of-Things (IoT) devices connect to the Internet daily, gathering and processing an immense volume of information from the real world [1]. The advent of the 5th Generation (5G) mobile communications network, allowing for massive information exchange, is a game-changer in IoT. The enhanced connectivity and widespread adoption of IoT incite cyberattacks (*e.g.*, ransomware and Distributed Denial-of-Service (DDoS) attacks [2]), thus, affecting among others also IoT-related infrastructures, raising security and privacy concerns for consumers and businesses. The Cyber Security Act (CSA) developed by the European Union Agency for Cybersecurity (ENISA) further highlights the need for comprehensive device management and ongoing certification across the entire IoT lifecycle to ensure high-security standards [3]. Similarly, the Network and Information Security (NIS2) directive advocates for a pragmatic security framework that fosters collaboration among IoT stakeholders [4]. However, managing security in IoT devices is challenging due to device heterogeneity, limited hardware capabilities, the dynamism of the security landscape, and the large number of stakeholders [1]. An entire system can be potentially compromised by a single vulnerable device.

Thus, this paper demonstrates a novel IoT device inventorying and lifecycle management platform, leveraging Hyperledger Aries for identity management and Hyperledger Orion for information sharing. The platform provides secure bootstrapping of IoT devices, dynamic reconfiguration in response to evolving security threats, and customized device management, while enhancing security and operational efficiency in IoT systems.

II. Background

The key technical facets of this platform include DLT, DID, VC, and MUD:

1) Distributed Ledger Technology (DLT): A DLT enables the decentralized management of data between various stakeholders through a peer-to-peer network. A DLT can be either permissionless (public) or permissioned (private). In a permissionless DLT anyone can join the network to read and write data to the ledger, while in a permissioned DLT, only pre-approved nodes are allowed to participate [2].

2) Decentralized Identifiers (DID): DIDs determine a unique identifier that allows for decentralized and verifiable digital identities that are globally resolvable and manageable independently by its owner [5]. DIDs remove the need for centralized identity providers and certification authorities.

3) Verifiable Credentials (VC): To guarantee tamper resistance, a claim or a statement about the subject (*e.g.*, a device), is wrapped in a verifiable credentials (VC) container. That is a cryptographic proof of a claim that enables verifiers to check its correctness [6].

4) Manufacturer Usage Description (MUD): MUD is a standardized framework for manufacturers to specify the intended behavior of IoT devices in a network [7]. The Threat MUD defined by NIST [8] provides a flexible and dynamic alert mechanism for new threats and mitigations to apply until an update or patch is released.

III. Related Work

[9] describes the use of public Ethereum blockchain and smart contracts to manage and configure IoT devices. The proposal does not utilize DID, VC or MUD, and is not suitable for private instances of the blockchain. [10] proposes a framework for managing and monitoring IoT devices, that is based on now deprecated Hyperledger Composer private blockchain. The authors store device configuration files history in the blockchain and enable devices to download new configurations once there is a modification. Similarly to [9], the framework does not use

DID, VC, or MUD. DIAM-IoT [11] is a framework that incorporates DIDs and VCs into the lifecycle of the IoT devices, while utilizing blockchain to connect IoT data silos. The system is not suitable for private deployment and does not support network segmentation or MUD.

IV. Overview

The general idea is to operate with two main conceptual domains. One refers to the *manufacturer* domain and the second is the *sensor* domain. In a supply-chain scenario, utilising DLT and DIDs enables transparent visualization of the device's sensor configurations and lifecycle management.

Figure 1 provides an overview of the infrastructure. The domain includes the manufacturer/maintainer that provides new devices and bootstraps them to the network. The maintainer within the manufacturer domain may apply changes to devices and, thus, has the capabilities of an administrator. In this sense, the DLT is permissioned, because the *Manufacturer* (or Maintainer) is the one entity authorized to enter and modify device and sensor information. For example, the Configuration and Management Database (CMDB) maintains data, and determines which stakeholders may be granted permission to observe the configuration of a set of sensors (*i.e.*, used in transport), but not to modify. Another use case is secure firmware upgrading, where the maintainer may push an image to a vulnerable set of devices. The update is pushed to the end device(s), and the credential can be reinstated in an updated version with up-to-date components. Such updates may concern software, firmware, or hardware. Further components of the *Manufacturer Domain* comprise other DLT-based services, including a database, identity management service, and a MUD server.

Within the *Sensor Domain* (Figure 1), sensors can be deployed to track the conditions of goods in a supply chain. For example, during an aircraft transportation by a logistics company, sensors ensure that goods are transported adequately. To minimize the computational load on devices, a *Central Controller* manages the identities of *Function Controller* and *Edge Nodes*. Additionally, an *Auditor* is introduced, which notifies the Manufacturer and the DLT of a vulnerability, prompting an update and providing necessary software updates to the end devices. Communication between the Sensor Domain and Manufacturer Domain is managed through a shared network, which in the demonstration uses a zero-trust network.

V. Demonstration

The demonstration was implemented[1] through a hardware configuration, including a central administrative server based on x86-64bit architecture, which holds all necessary infrastructure from the Manufacturer Domain (*cf.* Figure 1).

[1]https://github.com/arminveres/iot-inventory-management

A. Use Case — Connected Cabin System

This demo builds on a scenario with an aircraft connected cabin system (CCS) developed by Collins Aerospace[2]. Nowadays, more IoT devices are being deployed within aircraft cabins to improve in-flight entertainment and aircraft systems, and enable improved flight maintenance. In this demonstration, the Sensor Domain represents CCS installed in the aircraft. The main configuration of the network is the edge nodes connected to a Central Controller that manages the edge nodes as a subnet. The following components are within the hardware setup:

- Sensor Nodes: low-end devices, including actuation, sensing, or Human-Machine Interface (HMI) capabilities, with limited room for hardware and software-based cybersecurity requiring offloading to a more capable instance.
- Manufacturer Controller: devices with the ability to host security functionality.

External communication occurs through an aircraft gateway, offering services for data repository, data loading, and connectivity with the external environment. The airline operations center, product owner, and airplane maintainer can interact through the airport infrastructure. A technician can access the aircraft directly if necessary.

B. Hardware in Use

Three Raspberry Pi 4B devices, each with 4 GB of RAM, act as Central Controllers and sensors. The server, here the Manufacturer (or Maintainer), and all devices are set up inside a Zero-Trust ZeroTier[3] network, configured to be 172.24.0.0 (/16). Furthermore, it allows for a careful onboarding of singular nodes, hindering communication with devices outside the network with enforceable flow rules.

Additionally, a laptop can interact with the server to issue commands, such as registering devices in the DLT, visualizing their status and identifiers, and modifying their configuration. The demonstration can be run using the laptop as an interface to the audience or an external screen to guide participants through the operation process.

C. Operations

1) Onboarding: Assuming the software infrastructure was initiated on the server and the Central Controllers (Figure 3), the Manufacturer can proceed to onboard a single or a predefined list of devices. Upon initiating the onboarding, the server sequentially instantiates a connection to each device using the Hyperledger Aries protocol[4], which issues a VC and notifies the device. The credential is stored on the Hyperledger Indy ledger[5]. The server additionally stores it inside the Hyperledger Orion CMDB [12], concluding the onboarding process.

[2]https://www.collinsaerospace.com/
[3]https://www.zerotier.com/
[4]https://www.hyperledger.org/projects/aries
[5]https://www.hyperledger.org/projects/hyperledger-indy

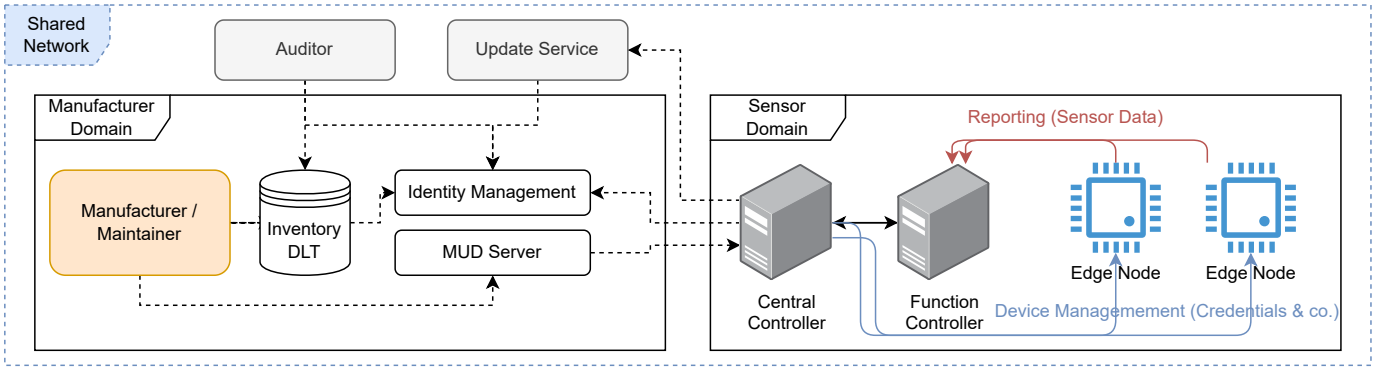

Fig. 1: Overview of System Components

Fig. 2: Hardware Setup of Central Controllers

```
Created auditor account
Options:
  [2]: Remove an onboarded node from the infrastructure
  [3]: Onboard node with public DID
  [4]: Mass Onboard fleet
  [5]: Query all nodes from Database
  [6]: Query single node from Database
  [h]: Print help
  [x]: Exit
> 3
Enter Node Name: node_raspi
Enter Node DID: 841WViQ5YzUbmThziMV7Pw
Maintainer.agent set connection id 35713d81-ecab-4a00-ba31-3dcde422ee4d
Maintainer.agent | 2023-12-10 14:36:33,440 aries_cloudagent.connections.base_m
nd for sender verkey: 59jDnmGypLhjCp4fo7rkYLppfGGUy3cYW99NKcNk2AZB
Maintainer.agent | 2023-12-10 14:36:33,442 aries_cloudagent.connections.base_m
nd for recipient verkey: DsQ8j7i37cM6v89J8muMAzJnNMtU9AmDcnivK6rpMeFr
Maintainer.agent | Connected

# Issuing credential offer to node_raspi
Maintainer.agent | Credential: state = offer-sent, cred_ex_id = b1916974-e22d-
Maintainer.agent | Credential: state = request-received, cred_ex_id = b1916974
Maintainer.agent | Revocation registry ID: 8BJ4EjbZM87wCasqjE1kt:4:8BJ4EjbZM87
troller_id_schema:CL_ACCUM:0978d6a9-0e1d-404e-86e2-e6bd1656bbb2
Maintainer.agent | Credential revocation ID: 1
Maintainer.agent | Credential: state = credential-issued, cred_ex_id = b191697
Maintainer.agent | Credential: state = done, cred_ex_id = b1916974-e22d-4aae-8
Options:
  [2]: Remove an onboarded node from the infrastructure
  [3]: Onboard node with public DID
  [4]: Mass Onboard fleet
  [5]: Query all nodes from Database
  [6]: Query single node from Database
  [h]: Print help
  [x]: Exit
>
```

Fig. 3: Onboarding a Central Controller

2) Auditing: To test the case of devices containing vulnerable components, the Auditor inspects each device in a given inventory, and initiates the auditing sequence. Upon finding a vulnerability, the server is notified, revoking a credential on the DLT and the inventory. When these devices are reachable (*i.e.* online), they receive a notification, and if the concerned component is software-based, then an update is initiated with the *Update Service*. Further auditing operations may involve security monitoring, including patching and configuration management maintenance, authentication, intrusion detection, risk assessment and mitigation, and compliance with standards and guidelines.

VI. Preliminary Conclusions and Future Work

This demonstration shows the functioning of a multi-stakeholder platform to monitor reliably and in an auditable manner the secure lifecycle of connected devices and sensors, generally IoT devices. The prototype is based on three Raspberry Pi devices and a laptop that showcases key functionality, especially registering and onboarding devices, tracking any status changes, and revoking their access (*i.e.*, decommissioning devices and sensors). The use of a DLT allows for a selective disclosure of information on a collaborative platform and maintains the management control of devices (*e.g.*, secure firmware updating) for their maintainers. At the same time, partner stakeholders can selectively receive permission to read or edit respective information.

This prototype is considered a foundation for a framework managing sensors in a multi-stakeholder scenario, which eventually will become part of the CERTIFY project's testing platform. As future work, it is planned to expand this demonstrator to a full support of MUD and Threat MUD, to enhance the device security itself, and to restrict their access areas. In addition, constrained devices without resources for running an Embedded Linux OS may also be considered as a future opportunity to expand such an approach to.

ACKNOWLEDGEMENTS

This paper was supported partially by *(a)* the University of Zürich UZH, Switzerland, and *(b)* the Swiss State Secretariat for Education, Research and Innovation (SERI) under grant agreement number 22.00165 within the context of the EU CERTIFY project.

REFERENCES

[1] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet of Things Journal*, Vol. 7, No. 1, p. 16–32, Jan. 2020.

[2] B. Rodrigues, E. J. Scheid, C. Killer, M. Franco, and B. Stiller, "Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks," *Journal of Network and Systems Management*, Vol. 28, No. 3, pp. 1–27, August 2020. [Online]: https://doi.org/10.1007/s10922-020-09559-4

[3] E. Commission, "The EU Cybersecurity Act." [Online]: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[4] "Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)." [Online]: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[5] W. W. W. Consortium. (2022) Decentralized Identifiers (DIDs) v1.0. [Online]: https://w3c.github.io/did-core/

[6] M. Sporny, D. Longley, D. Chadwick, and O. Steele, "Verifiable Credentials Data Model v2.0," Apr. 2024. [Online]: https://www.w3.org/TR/vc-data-model-2.0/

[7] E. Lear, R. Droms, and D. Romascanu, "Manufacturer Usage Description Specification," RFC 8520, Mar. 2019. [Online]: https://www.rfc-editor.org/info/rfc8520

[8] D. Dodson, D. Montgomery, W. Polk, M. Ranganathan, M. Souppaya, S. Johnson, A. Kadam, C. Pratt, D. Thakore, M. Walker *et al.*, "Securing Small-business and Home IoT Devices: Mitigating Network-based Attacks Using Manufacturer Usage Description (MUD)," National Institute of Standards and Technology, Tech. Rep., 2021. [Online]: https://www.nccoe.nist.gov/publication/1800-15/

[9] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 464–467.

[10] K. Košťál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, "Management and monitoring of iot devices using blockchain," *Sensors*, Vol. 19, No. 4, p. 856, Feb 2019.

[11] X. Fan, Q. Chai, L. Xu, and D. Guo, "Diam-iot: A decentralized identity and access management framework for internet of things," *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*. Taipei Taiwan, ACM, Oct 2020, p. 186–191. [Online]: https://dl.acm.org/doi/10.1145/3384943.3409436

[12] IBM, "The Orion blockchain database: Empowering multi-party data governance." [Online]: https://www.ibm.com/blog/the-orion-blockchain-database-empowering-multi-party-data-governance/