particular instance in the training set of a target model [2]. Adversaries can be e.g., a compromised or malicious aggregator, or someone stealing models during client-server communication.

Approaches for mitigating security and privacy risks in federated learning often still lag behind attacks, but are increasingly in the focus of research activities.

Regarding privacy risks, several approaches can be employed. Differential privacy (DP) aims to bring uncertainty into the model outputs to hide personal contributions to the model; clients can add noise to shared model parameters or train a differentially private machine learning algorithm. The main downside of this approach remains that noise degrades models performance, thus there is a trade-off between privacy and utility.

Secure Multi-Party Computation (SMPC) provides a cryptographic protocol that allows joint computation of a function while keeping its inputs private. In federated learning, this can replace a central aggregator. However, SMPC poses high computational costs, therefore limiting the scalability of federated learning.

Homomorphic Encryption (HE) allows mathematical operations to be performed on encrypted data. Clients can encrypt their model parameters, and the coordinator could aggregate them but not understand them. Like SMPC, HE greatly increases computational costs.

Detecting attacks on the integrity and availability of the machine learning process is even more difficult. Defences like anomaly detection and robust aggregation aim to discover potentially harmful models and eliminate their malicious influence on the global model. Yet they fail to detect targeted backdoor attacks, as poisoned models look and behave similarly to models that were trained without backdoor [3].

There has been a dramatic increase in interest in federated learning in recent years. Many companies, including Apple and Google, are already using federated learning for their services. Interest in this technology is especially high in medical applications and smart cities, where personal data is processed, and data privacy is a major concern. However, there are still challenges to address in federated learning. Mitigation of security and privacy risk is especially important for building trust in the technology. Further investigation of defence mechanisms is therefore critical for the successful application of federated learning.

This work has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826078.

References:

[1] P. Kairouz, H. Brendan McMahan, et al.: “Advances and Open Problems in Federated Learning”, Foundations and Trends in Machine Learning: Vol. 14: No. 1–2, pp 1-210, 2021.

[2] A. Pustozerova and R. Mayer: “Information leaks in federated learning”, in proc. of the Workshop on Decentralized IoT Systems and Security (DISS), 2020.

[3] N. Bouacida and P. Mohapatra: “Vulnerabilities in Federated Learning”, in IEEE Access, vol. 9, pp. 63229-63249, 2021.

Please contact:

Anastasia Pustozerova
SBA Research, Austria
apustozerova@sba-research.org

Considering Cybersecurity with Trustworthy IoT in Smart Cities

by Christoph Klikovits (Forschung Burgenland), Clemens Gnauer (Forschung Burgenland), Patrik Abraham (Fachhochschule Burgenland)

In today’s smart cities, the question remains how to securely integrate a multitude of different and constantly changing Internet of Things (IoT) devices and services. This is where we propose the combination of an identity provider (e.g.: ID-Austria [L3]) and the Arrowhead framework [L2] to verify sensors by matching them with a known legal identity. By providing an application that assures a secure authentication and trustworthy communication for people, sensors, and services in a smart city.

A variety of technological innovations have changed the characters of cities in recent years. There are millions of devices with sensors and actuators dispatched with an upward trend in cities (weather, water and gas metering, traffic lights and controls, waste management, etc.). Applying and using evermore of these in the context of interconnected IoT systems raises the challenge of providing trust and security in this context. The Center for Cyber Security of Forschung Burgenland [L1] deals with this topic and researches an approach to increase the trustworthiness and security of IoT devices. The aim of this approach is to link existing IoT devices or services with a known legal identity. An identity provider (ID-Austria) and an additional support service of the Arrowhead framework are combined through an integrated approach. Arrowhead was created for the orchestration of large scale IoT data. It offers strong security mechanisms and in combination with the admission ticket, cities can rely on secure and trustworthy IoT data. Furthermore, the Arrowhead project is implementing more and more support services like the on-boarding procedure [2] which is used for the autonomous integration of devices into the service-oriented arrowhead ecosystem. This procedure strengthens the secure and trustworthy integration of devices or services. A proof of concept could be developed in the EFRE project (FE07) “Civis 4.0 Patria” and presented in the FIP / IEEE

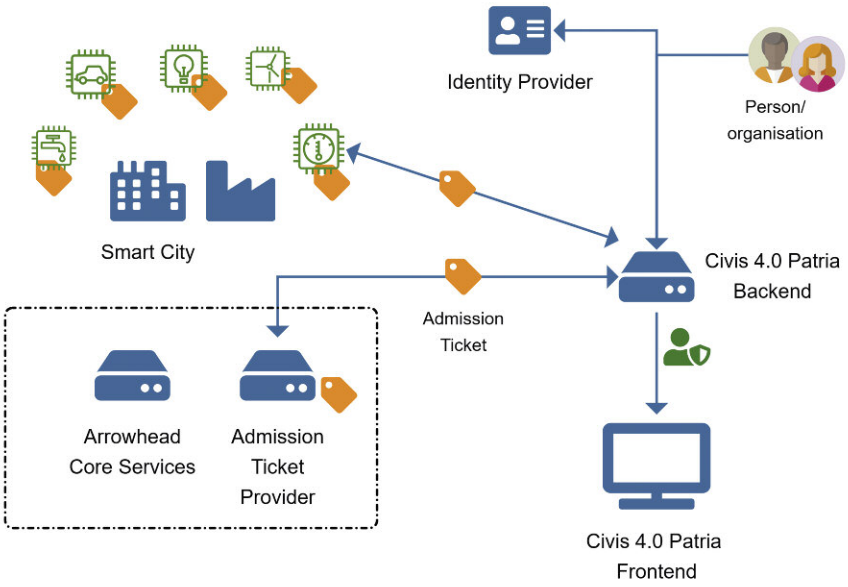

Figure 1: Architecture of trustworthy IoT in smart cities.

International Symposium on Integrated Network Management (IM) workshop [1].

As shown in Figure 1, various techniques and tools are used to create a digital admission ticket, which is created based on several parameters (IP, MAC address, etc.). In addition to the parameters listed, the electronic proof of identity from an identity provider is integrated into the creation of the digital admission tickets. Three instances and steps linked in an integrated approach are required for the creation of an admission ticket. Step 1: Firstly, a person or organization is involved in the proposed proof of concept shown in Figure 1. This natural person or corporate body requires an electronic proof of identification from an identification provider (e.g., ID-Austria [L3]). While logging into a backend layer (e.g., Civis 4.0 Patria backend), the login data is verified by the identification provider using an interface. By using the interface to the identification provider, the person or organisation does not need any additional login data for the backend layer. Step 2: In the verification process the identification provider determines an unique personal identifier, called bPK [L4], in two steps: Firstly, a character string is formed from a master number (central register or association register, commercial register entry) and the procedural area. Secondly, a specific hash algorithm calculates a secure one-way cryptographic derivation from this character string and encodes the bPK with the Base64 standard. Step 3: After the bPK has been transmitted from the identification provider to the backend layer, the person or organization is verified and clearly identified. The identified person or organization can use their identification (bPK) to register various devices or services in the backend layer. When registering, various additional parameters (IP-Address, Mac-Address, device ID, etc.), related to the device or service can be specified. These parameters, including a legal identity (bPK), are forwarded to the Arrowhead framework. Additionally, to the core services of the Arrowhead framework, a further service called the Admission Ticket Provider (ATP) was developed. The ATP is responsible for generating a hash (admission ticket) by combining the received device or service parameters (e.g., IP address or Mac-address), the unique personal identifier (bPK) and using the SHA-256 function. This delivers a string with 64 characters which will be stored in the ATP-database and transmitted to the backend for further use. Afterwards, the person or organization who registered the device or service will receive the admission ticket and must store it on the device (e.g., sensor, Raspberry Pi or smartphone) or service-platform.

The certified hash (admission ticket) created by the ATP is stored on both the respective device or service and in the ATP database. An implemented backend process automatically forwards the respective payload including the supplied admission ticket to the ATP in the Arrowhead framework every time a device or service transmits data. Furthermore, the admission ticket of the device or service is compared with the stored admission ticket in the ATP. After a successful verification of the admission ticket, the backend is informed by the ATP and allowed to publish the payload into the frontend. If an admission ticket is invalid or does not exist, the frontend release of the payload is not permitted and is discarded. As applied in a proof of concept, it shows trustworthy and secure communication in smart cities, where smart devices or services are increasingly used. Matching a unique personal identifier with devices or services enables to link a person responsible with e.g., IoT sensors, whereby trustworthiness, acceptance and security of devices and services in a smart city can be strengthened.

Links:
[L1] https://www.forschung-burgenland.at/cybershysecurity/
[L2] https://www.arrowhead.eu
[L3] https://kwz.me/h7J
[L4] https://kwz.me/h7M

References:

[1] C. Klikovits, P. Abraham and R. Rambacher: “A Framework to identify People, Devices and Services in Cyber-physical system of systems,” 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021, pp. 914-919.

[2] A. Bicaku, et al.: “Interacting with the arrowhead local cloud: On-boarding procedure”, 743-748. 10.1109/ICPHYS.2018.8390800, 2018.

Please contact:

Christoph Klikovits
Forschung Burgenland, Austria
christoph.klikovits@forschung-burgenland