End-to-end Security and Privacy in a Heterogeneous Multi-platform Environment

C. Kassapoglou Faist, D. Vizár, P. Dallemagne

The Internet of Things opens new perspectives for aging well, enabling remote health monitoring and assistance. However, interconnecting IoT devices and offering large-scale services over publicly available infrastructures poses serious security and privacy concerns. CSEM and its partners carried out security risk analyses and data protection Impact assessments enabling us to propose targeted protection measures.

Adjusting the living-room temperature from the workplace, or measuring a patient's medical condition remotely, have become common-place actions, thanks to the Internet of Things. By 2025, market analysts predict over 20 billion interconnected devices worldwide, enabling new services and enhancing the quality of life. But what guarantee do we have with respect to the authenticity and the integrity of the data that we receive? And how can we be sure that confidential information has not leaked or is not available to unauthorized parties? These and other security and privacy concerns have been raised and IoT solution providers have started addressing requirements identified by customers or regulatory bodies by, *e.g.*, encrypting the data. However, efficient solutions require a global, end-to-end (E2E) perspective and must be tailored to the needs of the application.

CSEM and its partners are studying this problem in the context of the H2020 EU Large-scale Pilot project ACTIVAGE. The project enables IoT services for Active and Healthy Aging, supporting independent living of older adults in their living environments and responding to the needs of caregivers, service providers and public authorities. The project's main objective is to build a European IoT ecosystem across nine deployment sites in seven European countries. The idea is to reuse and scale up several existing IoT platforms (based on frameworks such as Fiware, Sofia, SensiNact, Universaal, openIOT), providing interfaces for interoperability.

Although inter-dependent, security and privacy were handled separately. Security deals with confidentiality, integrity and availability. Since security measures are costly and may also hinder performance, special care must be taken in their design. Adopting the reference architecture shown in Figure 1, the methodology described below was applied to the design.

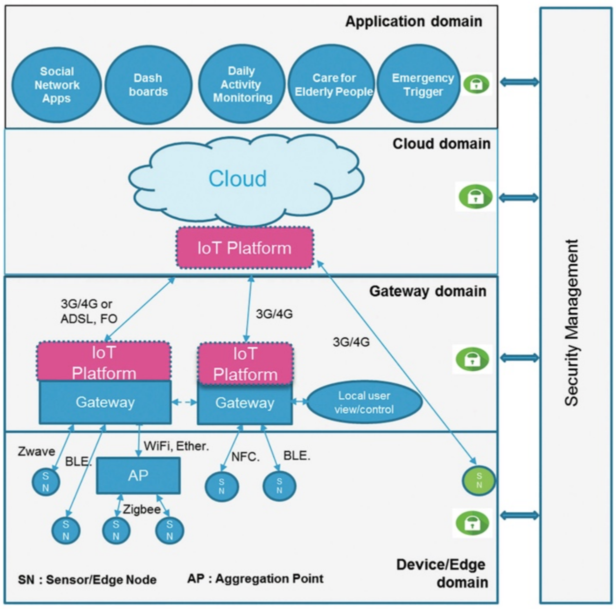

Figure 1: Reference architecture for security risk analysis.

First, a reference, E2E security risk analysis was performed. Using the Microsoft STRIDE method, we identified threats and vulnerabilities for the system assets, within each domain and across the IoT domains (Device, Gateway, Cloud and Application). The threats were categorized, and their risk was quantified taking into account criteria such as probability of occurrence, damage extent, population affected etc. At the same time, security countermeasures were identified, to be proposed as the threat risk demands.

In a second step we assessed the current status of each deployment site through questionnaires that reflected the risks identified in the reference study. In this effort, publications and guidelines by the IoT Security Foundation and the Open Web Application Security Project were highly valuable. Based on the answers, security recommendations were made, tailored to each of the nine deployment sites in the project.

The third step dealt with the identification and high-level specification of the overall, cross-platform security services in an E2E perspective. As in the case of the oneM2M specification, the security services were defined to be Authentication and Authorization (which includes Access Control and Consent Handling), E2E Security Association, Sensitive Data Handling and Security Provisioning, along with underlying functions, such as Identity Management and a Public Key Infrastructure. In particular, in order to guarantee confidentiality across any data path, a scheme similar to Transport Layer Security was proposed for E2E encryption, to be integrated at application layer.

With the emergence of Big Data technologies, the European General Data Protection Regulation (GDPR) came into force; responding to the growing public demand for privacy. The GDPR defines who the data owner is and it requires, *e.g.*, privacy by design and by default in a data system. Typical approaches to comply with the GDPR rely on existing frameworks and processes, such as the Data Protection Impact Assessment (DPIA), put in place by consultancy companies, national agencies (such as the French CNIL) and standardization bodies. A DPIA guides the designer through the following steps: description of the use and processing of all personal data in the system, assessment of the necessity of processing and the risks with respect to a person's rights, documentation of the measures taken (*e.g.*, security mechanisms) and demonstration of compliance. DPIAs were carried in the project deployment sites.

Implementation of security and privacy in ACTIVAGE, which largely relies on existing, widely accepted tools and frameworks is under way. In addition, CSEM has defined a framework providing Consent Management and Personal data management services, to be enriched in the future with several tools for privacy-preserving data analytics, such as multi-party computation and homomorphic encryption. These tools will be supported by security and cryptography functions designed for low-end platforms (*e.g.*, an environmental sensor or a wearable device) as well as for high-end ones (*e.g.*, cloud), allowing the deployment of E2E private computations.