IoTAC PILOTS

SMART HOME

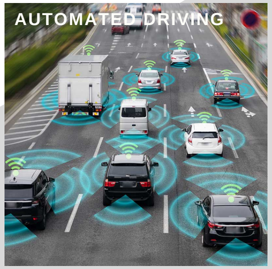
The Smart House of CERTH provides various innovative smart IoT-based technologies through its sensors, actuators, smart home devices and intelligent robots. It has the ITI Smart Home Platform, which acts as a complete monitoring and control framework, just like a management system. Through the main web dashboard, the user can interact with the IoT Infrastructure of the Smart Home. The pilot will validate the new IoTAC architecture through user and access management, energy, and healthcare related services.

PROSUMER CELL

Prosumer cells are the key elements of the future smart grid. A prosumer cell is capable to behave either as a producer or as a customer in the grid. It usually contains small local plants, switches to change between producer, consumer or off-line states, energy storage, and intelligent controller(s) with sensors and actuators. The pilot's objective is to improve the security and confidence of the prosumer cell system by implementing the IoTAC solutions. Key issues are identity and access management as well as the protection of the bidirectional information flow both internally between the local units of the cell and externally with the remote command interface.

DRONE OPERATION

The operation will focus on the vulnerability of Unmanned Air Systems and the vulnerability of fixed sensors that are in remote locations without human protection. A model of the system will be established with the user workstations, a ground control station (GCS) for UAVs, access points, and nodes. The system will be built around a hybrid communication network that combines fixed lines and wireless segments.. The pilot will consist of testing the runtime monitoring features implemented by the project and solutions to counter the possible attacks on the system.



AUTOMATED DRIVING

The connected and automated vehicle pilot will provide scenarios, where (V2X) data exchange enables cooperative manoeuvres integrating decision-making algorithms. The pilot will consist of Platoon driving and Platoon Merging. These cooperative scenarios require the use of real-time low latency communication with other vehicles in order to precisely complete the manoeuvre in its correspondent route This low latency communication channel poses a challenge to protect and guarantee its integrity, without incurring in significant overhead for the control of the manoeuvre.

The IoTAC Consortium:

Atos

Co-ordinator

CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

ITIS

MŰEGYETEM 1782

QUANTAG IT SOLUTIONS

Fraunhofer FOKUS

INTRASOFT INTERNATIONAL

tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

kaspersky

T · · LIFE IS FOR SHARING.

Technische Universität Berlin

SAFEPAY

AIRBUS

Visit our website:
https://iotac.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952684.
The contents of this document reflect only the project Consortium's view and the Commission is not responsible for any use that may be made of the information it contains.

IoTAC

Security By Design IoT Development and Certificate Framework with Front-end Access Control

Objectives:

- Implement all components of a secure IoT architecture based on a secure gateway integrating runtime protection modules and a real-time monitoring system.
- Define and implement methodologies, processes and technologies from design to certification to assure that all elements of the proposed architecture will be safe and reliable.
- Validate the new secure architecture and security assessment framework in four, close to real life demonstrations with various IoT use cases.
- Gain industry wide recognition for IoTAC as a future-proof direction for new IoT design, development methodology and related operation concept

IoTAC

CONCEPT:

The IoTAC project aims to deliver a secure and privacy-friendly IoT architecture that will facilitate the development of more resilient IoT service environments.
Our system, comprising of a secure gateway, runtime security applications and cloud-based service platforms, will provide comprehensive protection for service environments of various industry domains. The technology will not only protect new deployments but can also enhance the security level of legacy operations.
In the IoTAC architecture we deploy a combination of state-of-the-art technologies and extend them with new inherently secure processes and workflows. Security countermeasures are implemented both at hardware- and at software-level, which treat privacy and data security as topmost priorities.

6 MODULES

FRONT-END ACCESS CONTROL (FEAC)

FEAC introduces a novel approach using a secure chip card with a user cardlet and PKI for user authentication and authorisation. The solution detaches transaction management from credential control thus supports a truly decentralized operation. The authentication and authorisation functions are delegated to the front-end, to the user secure application, while at the access points only the integrity of the capability tokens need to be checked. This simple architecture at the endpoints allows the highest-level security even for resource constrained devices.

AI BASED ATTACK DETECTION

Within IoTAC, a novel technique using the Auto-Associative Random Neural Network (AARNN) is developed and tested to provide highly accurate attack detection of major Botnet attacks. The additional value of this technique lies in its training protocol which relies on normal traffic patterns, not requiring data regarding the possible attack patterns that the network may encounter.

IoT ENABLED HONEYPOTS

HONEYPOTS will be introduced with the purpose to attract the attention of potential attacker to specific environments that are not part of the actual system. The honeypots will comprise of two layers, one visible to the attackers, and another one that will be dedicated for analysing the attackers' behaviour.A critical element of the IoTAC IoT-enabled honeypots will be the novel anomaly detection algorithms. Both lightweight and advanced anomaly detection techniques will be developed supporting the early detection of behavioural changes of IoT devices, as well as the identification of potential intrusions and the conduction of root cause analysis for attack patterns.

The **RUNTIME MONITORING SYSTEM (RMS)** will collect security-related data real-time from monitored IoT systems and will store them for further processing. The collected data will be used to drive analytics algorithms that detect patterns of abnormal behaviour. The system will feature lightweight monitoring probs that will be responsible for the data collection and publishing to the monitoring platform. The RMS will provide appropriate configuration and management mechanism over the monitoring probes as well as appropriate data models and data transformation engines that will enable the discoverability and reusability of the collected data.

SECURE SOFTWARE DEVELOPMENT (SSD) enables the development of more secure IoT software applications by treating security at each phase of the overall Security by Design Life Cycle. More specifically, SSD will allow developers of an IoT software application to (i) ensure the correct definition of the security requirements, (ii) ensure the adherence of the produced IoT software application to the originally defined requirements, (iii) evaluate the security level of the IoT software application, and (iv) provide recommendations for security improvement. Hence, SSD is expected to enable the continuous monitoring and improvement of the security level of software applications running on IoT platforms throughout their overall development cycle.

KASPERSKY IOT SECURE GATEWAY (KISG) consists of the KasperskyOS operating system with a preconfigured set of application software. Kaspersky IoT Secure Gateway is intended for installation on a built-in Advantech UTX-3117-S6A1N computer. The KISG is designed to serve as a secure gateway for the Internet of Things in an enterprise network. It protects data at the gateway level by receiving, verifying and distributing sensor messages received over the MQTT protocol, and by relaying control commands to actuators. The KISG will be used as a platform to integrate the IoTAC runtime protection modules and to provide multi layer protection in diverse IoT domains.