Celtic-Plus
Smart Connected World

Project Achievements

CRITISEC

Project ID: C2018/1-1

Start Date: 1 December 2018

Closure date: 31 March 2022

Partners:

Applio Tech AB, Sweden

HITEC Luxembourg S.A., Luxembourg

III CSTI, Taiwan

Itrust consulting, Luxembourg

Kraftringen Energi AB, Sweden

RISE Research Institutes of Sweden AB, Sweden

Sensative AB, Sweden

Sony Nordic (Sweden), Filial till Sony Europe B.V., Sweden

Tyréns AB, Sweden

University of Luxembourg, Luxembourg

Co-ordinator:

Harold Linke

HITEC Luxembourg

E-Mail: harold.linke@hitec.lu

Project Website

www.celticnext.eu/project-critisec

https://critisec.hitec.lu

Critical Infrastructure Security

The CRITISEC project developed security services and standards for edge networks in critical infrastructures allowing to connect edge networks to control and production systems in a secure way. Use cases focused on are Energy distribution, Smart cities, Critical communication, Critical Logistics and Identity Management.

Main focus

The core idea of the CRITISEC project was to develop novel security products, services and standards for edge networks in critical infrastructures, where the edge networks are a heterogeneous set of networks connected to the edge of a core production network.

The challenges that CRITISEC addressed were:

1. the heterogeneity of the edge networks and of the systems they are connected to;

2. the resource-constrained nature of devices (e.g., battery power) and even of networks as a whole (packet loss, low bandwidth);

3. the scale of the edge networks, that can be composed of huge numbers of (resource-constrained) devices, so requiring efficient and highly scalable security solutions;

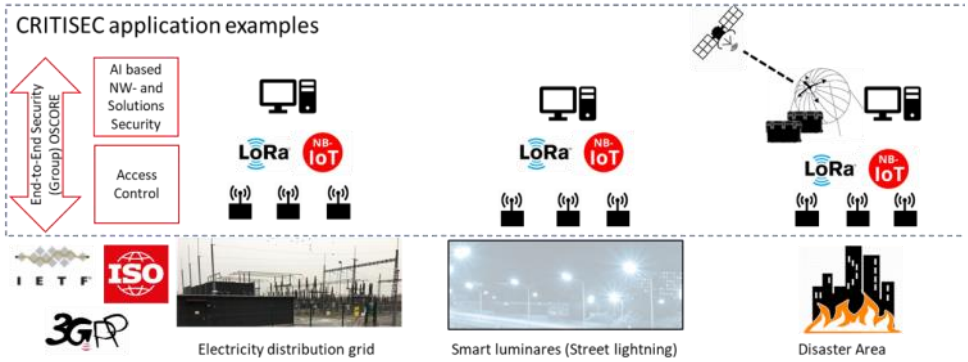
4. the predominant presence of open/shared platforms, where multiple applications share access to a common network of edge devices;

5. the presence of legacy devices and platforms, for which secure update procedures are often scarce, if any.

Approach

The CRITISEC project performed research in the several novel technology areas related to security in critical infrastructures, and developed corresponding innovative security mechanisms and solutions:

- The use of AI for threat analysis, and mitigation strategies.
- End-to-end security and application isolation in open platforms.
- Identity and fine-grained Access Management for constrained devices (e.g., sensors and actuators) connected to critical infrastructures via edge networks.
- Secure end-to-end (group) communication methods efficiently supporting large-scale deployments, together with authorized provisioning of group keying material.
- Security Lifecycle Management, including secure automated enrolment of IoT devices and secure distribution of software/firmware updates.



(LoRa = Long Range mobile IoT standard – NB-IoT = Narrowband IoT)

These areas are of strategic relevance for infrastructure providers, since their production systems are exposed to increasing threats, especially through Advanced Persistent Threat (APT) actors and criminal elements looking for cyber-blackmailing opportunities. Such attackers have a potential to significantly disrupt core production systems, both affecting the economic viability of the provider and disrupting important societal services.

Achieved results

The main achievements of the project are contributions to security standards (especially the Group OSCORE security protocol as well as the access control ACE framework and its profiles) and 7 new or updated products (Sensative Yggio 3.0, Applio Free and Sense, CSTI DTM, itrust CyberJayBox, ARIANA, CryptoCeVerif).

Other important achievements are new concepts such as the AI based anomaly detection using application log analysis, and a combination of AI-based methods and deep packet inspection, as components of a monitoring system for anomaly and intrusion detection.

The results were demonstrated in 5 demonstrators:

Energy Distribution demonstrator - integration and operation of sensors in critical infrastructures for energy distribution, in order to increase the monitoring and control, achieve a more flexible and efficient use of the infrastructures, and facilitate adoption in new customer services.

Smart Cities demonstrator - smart city operation in multiple applications, using a unified infrastructure and platform including for instance street lighting and air quality monitoring.

Critical Communication demonstrator - improving the security of critical communication infrastructures composed of a set of smaller edge networks. The communication flows and networks are monitored by AI-based anomaly/intrusion detection solutions.

Secure End-to-End Group Communication - demonstrating a secured group communication model, where network nodes acting as clients can send a single message protected end-to-end to multiple recipient servers, e.g., over IP multicast.

Secure and Automated Device On-Boarding - demonstrating the onboarding of IoT devices as a fundamental, early step in their lifecycle, where first crucial steps are taken to ensure that following communications are properly secured.

Impact

The 7 new or updated products Sensative Yggio 3.0, Applio Free and Sense, CSTI DTM, itrust CyberJayBox, ARIANA and CryptoCeVerif will have a significant impact on the business of the partners. This helps improving the security of IoT networks in critical infrastructures.

The approved IETF standard proposals comprising the ACE framework and its profiles enable fine-grained access control for the IoT. The new IETF standard proposals comprising Group OSCORE and the ACE-based provisioning of group keying material enable secure end-to-end group communication for the IoT.

The AI based anomaly detection using application log analysis and the combination of AI-based methods and deep packet inspection will allow more flexible and easier to use anomaly detection solutions and an enhanced protection against new cyber threats.

About Celtic-Plus

Celtic-Plus is an industry-driven European research initiative to define, perform and finance through public and private funding common research projects in the area of telecommunications, new media, future Internet, and applications & services focusing on a new „Smart Connected World“ paradigm. Celtic-Plus is a EUREKA ICT cluster and belongs to the intergovernmental EUREKA network. Celtic-Plus is open to any type of company covering the Celtic-Plus research areas, large industry as well as small companies or universities and research organisations. Even companies outside the EUREKA countries may get some possibilities to join a Celtic-Plus project under certain conditions.

Celtic Office

c/o Eurescom, Wieblinger Weg 19/4

69123 Heidelberg, Germany

Phone: +49 6221 989 138

E-mail: office@celticnext.eu

www.celtinext.eu

EUREKA