Project Information

CRITISEC

Project ID: C2018/1-1
Start Date: 1 December 2018
Closure date: 31 March 2022

Partners:

Luxembourg

HITEC Luxembourg S.A.

Itrust Consulting

University of Luxembourg

Sweden

Applio Tech AB

Kraftringen Energi AB,

RISE Research Institutes of Sweden AB

Sensative AB

Sony Nordic,

Tyréns AB

Taiwan

III-CSTI

Co-ordinator:

Harold Linke

HITEC Luxembourg

E-Mail: harold.linke@hitec.lu

Project Website

www.celticnext.eu/project-critisec

Critical Infrastructure Security

The CRITISEC project intends to develop 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, Identity Management and Distributed Ledgers.

Main focus

The core idea of the CRITISEC project is 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 will be addressing are:

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

2) 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;

3) The predominant presence of open/ shared platforms, where multiple applications share access to a common network of edge devices;

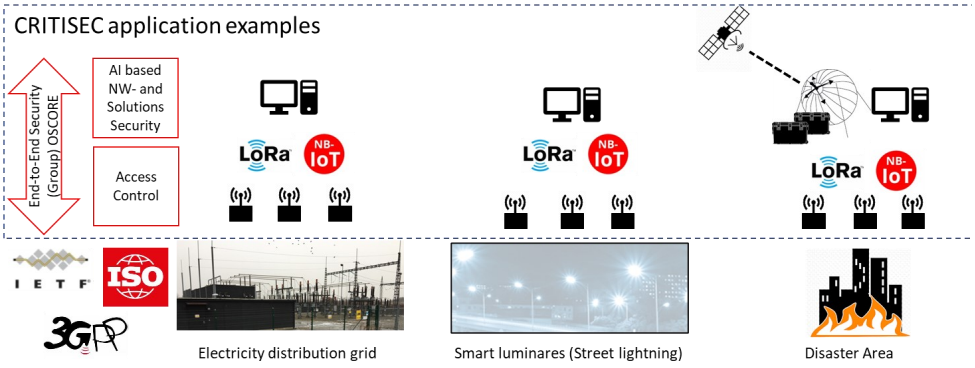
4) The presence of legacy devices and platforms, for which secure update procedures are often scarce, if any.

Approach

The CRITISEC project will perform research in the following novel technology areas related to security in critical infrastructures, and will develop corresponding innovative security mechanisms and solutions:

- The use of AI for threat analysis, and mitigation strategies.
- The use of open ledgers (blockchain) to confirm trustworthiness of sensor data in open networks.
- End-to-end security and application isolation in open platforms.
- Identity and 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.
- Security Lifecycle Management, including secure firmware upgrade and management.

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



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

have a potential to significantly disrupt core production systems, both affecting the economic viability of the provider and disrupting important societal services.

Currently attacks often go unnoticed under a long period of time, so worsening their effect. Moreover, attackers that penetrate some seemingly unrelated part of a company's IT system often have the possibility to move laterally into the core production system.

The use cases addressed are:

1. Energy distribution
2. Smart cities
3. Critical communication and Small IoT
4. IoT for Critical Logistics
5. Identity Management for IoT
6. IoT and distributed ledgers

The use cases will be demonstrated in three application examples:

- Electricity distribution grid (use case 1)
- Smart luminaries (use case 2)
- Disaster arey (use cases 3-6)

Main results

The main results of this project will be novel security standards, solutions, products and services that can be used by providers of critical infrastructures to secure edge networks connected to their production systems. This will reduce the risk of malicious service disruption and preserve availability, reliability and safety in provisioning of societal services.

The main results will include:

- IETF (Internet Engineering Task Force) standards and advanced standard proposals, concerning lightweight protocols for secure end-to-end communication and access control for IoT devices
- Integration and testing of the OSCORE (Object Security for Constrained RESTful Environments) protocol in several IoT platforms
- AI based application security for edge computing
- AI based network security
- Solutions to use blockchain and open ledgers for IoT device management
- A 5G security surveillance system

Impact

The CRITISEC project results will have a great impact on several areas in the IoT market.

First, the IETF standards proposed by CRITISEC - including OSCORE and Group OSCORE - will be implemented in several solutions from CRITISEC partners and used to improve the end-to-end security of critical IoT networks. The solutions will be implemented in several real world use cases by the project partners

The AI based application security module for edge computing is planned to be integrated into a disaster management solution to improve the application security but will also be available for general introduction into edge computing.

The AI based network security device will improve the security of IoT network and allow the early detection of 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 0
E-mail: office@celticnext.eu
www.celticnext.eu

EUREKA