CELTIC-NEXT
eureka Cluster

Project Information

CISSAN

Project ID: C2022/1-3
Start Date: 1 May 2023
Closure date: 31 May 2026

Partners:

AddSecure Smart Grids, Sweden
Affärsverken Karlskrona, Sweden
Arctos Labs AB, Sweden
Bittium Biosignals Ltd., Finland
Bittium Wireless Ltd., Finland
Blekinge Tekniska Högskolan, Sweden
Blue Science Park, Sweden
Cibernos, Spain
Clavister AB, Sweden
Councilbox, Spain
Geodata Ziviltechnikergesellschaft mbH, Austria
Mattersoft Ltd., Finland
Mint Security Ltd., FInland
Netox, Finland
Nodeon Finland Oy, Finland
Savantic, Sweden
ScopeSensor Ltd., Finland
Techinova AB, Sweden
University of Jyväskylä, Finland
Wirepas Oy, Finland

Co-ordinator:
Alexey Kirichenko
University of Jyväskylä
E-Mail: alexey.l.kirichenko@jyu.fi

Project Website
www.celticnext.eu/project-cissan

Collective intelligence supported by security aware nodes

In its recent publication [1], the European Cyber Security Organisation observes that cyberattacks targeting IoT networks are expected to have high impact on all sectors from smart home appliances to smart cities and connected cars. To address the IoT cybersecurity challenges, CISSAN builds new methods and technologies for integrating collective security intelligence to IoT networks. CISSAN-powered networks will be able to collaboratively identify tampered and adversarial devices, detect malicious activities, and select effective countermeasures. For IoT network owners and operators, this will help ensure higher resilience of their networks accompanied by the resource efficiency of the security functionalities intelligently distributed across the network nodes.

Main focus

The proliferation of Internet of Things (IoT) with its *smart devices* has fundamentally changed how different environments, such as homes, offices, factories, smart buildings, and smart grids, are used and operated. However, as stated in [1], security is a major concern for IoT networks and environments, where the risks of physical device tampering, injection of malicious devices, and unpatched vulnerabilities are higher than in traditional networks. This is nicely captured in the Hyppönen's law [2]: "If it's smart, it's vulnerable." Following "when everything is connected, everything must be protected" [2], CISSAN proposes and implements algorithms for mitigating IoT security threats (good reviews of which can be found in [1] and [3]) through collective decision-making and with a reduced impact on the limited resources of IoT devices. These algorithms are based on research and innovation in optimizing the distribution of security capabilities and aggregating the intelligence in IoT network nodes. Three industrial use cases, which nowadays heavily rely on the use of IoT, inform the project developments and are used for validating and demonstrating the project results: (i) public transportation; (ii) smart energy grids; (iii) mining and tunnelling operations.

Approach

CISSAN researches and implements algorithms for distributed security monitoring, attack detection and response in IoT networks. Such algorithms combine machine learning-based methods, more traditional AI techniques (e.g., decision-making based on formal knowledge representation and expert systems, fuzzy logic-based approaches, or genetic algorithms), and attack-specific rules. Since increasing the level of autonomy in IoT network defence is one of the high goals of the project, we develop mechanisms for collective decision-making by CISSAN "security agents", which are essentially security functions placed to IoT network nodes. Blockchain-based consensus protocols are one possible type of such mechanisms to be considered in the project. To enable communication between the security agents

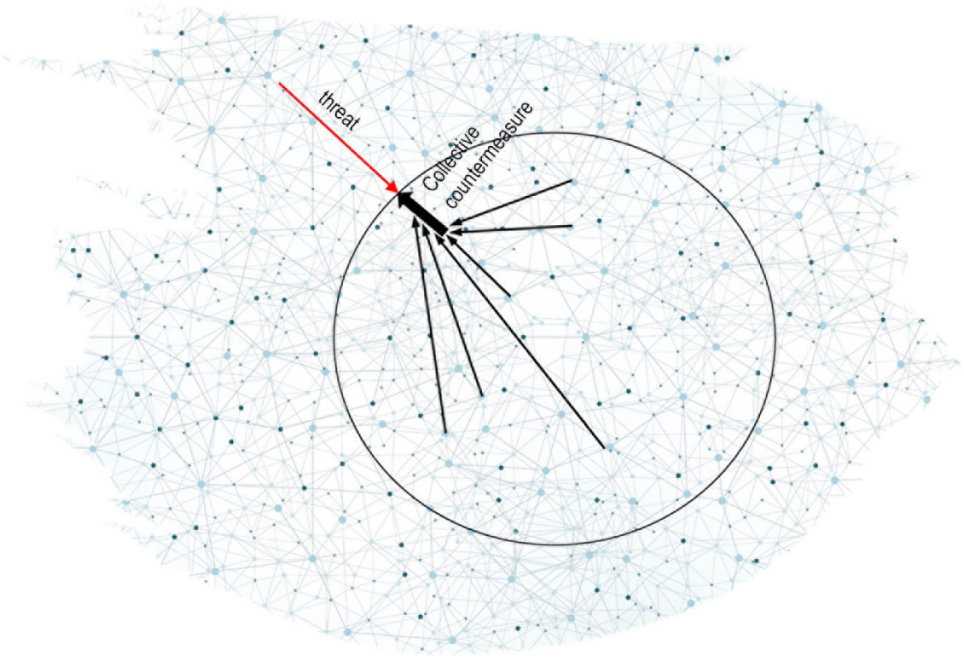

Figure 1: IoT nodes collectively defending against a cyberthreat

(collective intelligence traffic), CISSAN prototypes and evaluates a light overlay networking solution. Also, methods and tools are developed for verifying the quality of data sets used in the project for building machine learning models and supporting other data-driven technologies.

IoT devices are usually resource-constrained, and instrumenting each of them with the full set of security functions required for detecting and countering cyberattacks may not be an optimal strategy. Instead, we work to propose network context-aware algorithms for distributing the security functions among the IoT devices, edge devices, and possibly cloud backends to achieve a suitable balance between the network resilience and the resource utilization.

The technical efforts in CISSAN are accompanied by defining and investigating potential business models around the project results and their business impact analysis. We take into account regulatory and compliance considerations, including the ENISA's work on certification schemes.

Main results

The set of methods and interconnected technology components built by CISSAN, which can be viewed as the CISSAN platform, will be used for integrating collective security intelligence to IoT networks.

For a future IoT network at the design stage, the CISSAN platform can serve a foundation to build upon, by selecting CISSAN-powered devices, integrating CISSAN code to native network nodes, edge devices and cloud backend components, and using CISSAN tools for configuring and managing the IoT network security as appropriate. For IoT networks at later stages in their life cycle, the CISSAN results can be used in adaptive ways to bring network resilience improvements with the maximum impact possible. In addition to this, subsets of the CISSAN technology will be exploited by the project partners, their customers and other third-party organizations. For instance, a planning and optimization tool for distributing security functionality across IoT network devices is expected to bring value to several partners in their future applications, while a tool for blockchain-based integrity protection of sensor data and a cloud service for quality verification of such data are planned to be offered in selected markets.

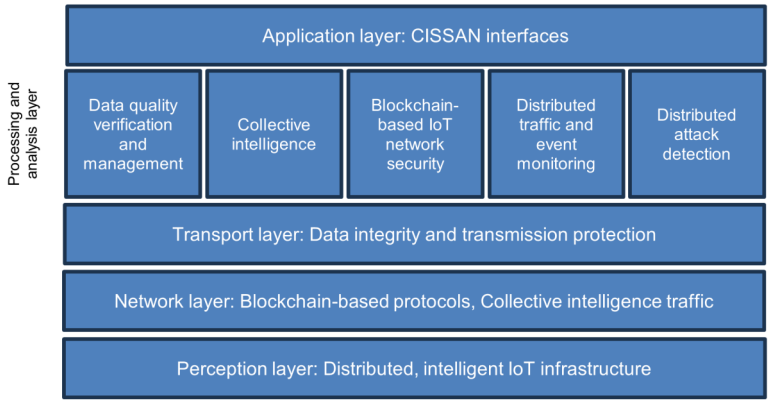

Figure 2: Initial CISSAN architecture

Impact

By integrating the full range or suitable subsets of the CISSAN results, we expect the users to achieve significant security improvements in their IoT networks while minimizing the human expert supervision costs (increasing the level of autonomy in IoT network defence) and the resource consumption for running security functions. The reduction in the number of security incidents and the cost of handling those will make IoT networks exploiting CISSAN methods and technology more trustworthy for their stakeholders and users, which is critical from the business point of view. We also expect that CISSAN-powered IoT networks will be better prepared to security reviews and evaluations in the scope of existing and upcoming regulation, certification schemes, and – possibly – cyber insurances, and we consider this a major business benefit.

[1] European Cyber Security Organisation (ECSO) Technical Paper on Internet of Things (IoT). Available online: https://ecs-org.eu/?publications=technical-paper-on-internet-of-things-iot (accessed on 15 January 2024).

[2] Hypponen's Law: If it's smart, it's vulnerable. Available online: https://blog.f-secure.com/hypponens-law-smart-vulnerable/ (accessed on 15 January 2024).

[3] Wheelus, C.; Zhu, X. IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework. IoT 2020, 1, 259-285. https://doi.org/10.3390/iot1020016

About CELTIC-NEXT

CELTIC-NEXT is the EUREKA Cluster for next-generation communications enabling the digital society. CELTIC-NEXT stimulates and orchestrates international collaborative projects in the Information and Communications Technology (ICT) domain.

The CELTIC-NEXT programme includes a wide scope of ICT topics based on new high-performance communications networks supporting data-rich applications and advanced services, both in the ICT sector and across all vertical sectors.

CELTIC-NEXT is an industry-driven initiative, involving all the major ICT industry players as well as many SMEs, service providers, and research institutions. The CELTIC-NEXT activities are open to all organisations that share the CELTIC-NEXT vision of an inclusive digital society and are willing to collaborate to their own benefit, aligned with their national priorities, to advance the development and uptake of advanced ICT solutions.

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