PROJECT PROFILE

17004

AI and privacy-enhancing -technologies to enhance internet interoperability, resiliency and security for business and industry

[SunRISE]

The SunRISE project will implement a comprehensive security solution, concentrating on aspects and issues critical to future systems related to the internet of things (IoT). Advanced digital technologies, such as artificial intelligence (AI), machine learning and privacy-enhancing technologies (PETs), together with security-data sharing, will be deployed to implement such system-security features as intrusion and anomaly-detection.

In recent years, the internet of things (IoT) revolution has been transforming our world, as we move towards one where everything is interconnected, everything is smart, and everything is – or should be – secure. Sensors, actuators, processors, networks and radios are crucial in building smart connected-devices enabling real-time sensing, contextual understanding, environment manipulation, and communication. Today, 2.9 billion people are online, 40% of the world's population. And by 2020 we expect about 50 billion devices to be connected.

While delivering clear benefits, these devices also increase the risk of data manipulation, data theft and cyberattacks. In 2015, European enterprises had at least a one-in-five chance of losing data through a targeted cyberattack. There is a severe risk that the European economy is falling behind in exploiting opportunities in emerging IoT markets. The lack of trust by businesses and consumers in smart connected-devices is a clear barrier to growth and jobs. At this point, it is no longer sufficient to provide ad hoc 'semiconductor' responses to these issues. Essentially, we need well-structured, interoperable and resilient secure solutions and systems.

AI and machine learning crucial to comprehensive IoT security

The SunRISE project will deal with one of the major challenges for the digital industry, namely IoT security. To obtain a comprehensive security solution, this project will address the following critical aspects in future IoT systems:

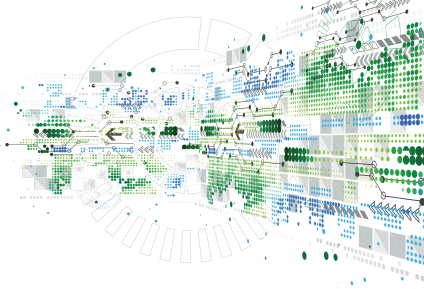
- Design of intrusion and anomaly-detection: by using machine learning (and the latest results) on IoT edge nodes;
- Sharing of security intelligence data (from IoT nodes to cloud back-ends): by creating a community with reference structures. Based on the larger dataset, machine learning can be accelerated and overall system security increased. This should result in security turning into a shared responsibility, interest and effort, but also into improved efficiency, cost and resource usage;
- Lack of trust by fearing the loss of confidential data: can be overcome by using privacy-enhancing technologies (PETs), like homomorphic encryption and secure multi-party computation (MPC);
- Efficient and cost-effective introduction of PET: by designing and manufacturing hardware which supports and accelerates AI specific to IoT end-nodes.

SunRISE activities will result in the following deliverables:

- A reference cloud-based platform for sharing security intelligence;
- Novel homomorphic encryption hardware accelerators and secure multi-party computation PET technologies;
- Efficient hardware for PET technologies and machine learning;
- A reference platform for secure IoT device identity and life-cycle management;
- Highly secure and cost-efficient root-of-trust hardware for IoT devices.

Crucially, this project will be guided by PENTA's three key objectives:

1. To reinforce existing strengths in Europe: SunRISE will use existing European expertise and experience in AI and machine learning to monitor the security of IoT devices and detect anomalies, thus preventing attacks or further shortcomings. The project will also develop tools capable of fixing detected errors and/or bringing the entire IoT system operation into a safe mode;
2. To close gaps across the European value-chain: To meet the high technological risk posed by this project's approach, SunRISE brings together experienced partners from three countries, all experts in their specific field.



KEY APPLICATION AREAS

- Health & Well-Being
- Digital Industry

ESSENTIAL CAPABILITIES

- Connectivity & Interoperability
- Safety, Security & Reliability
- Computing & Storage

PARTNERS

Ancud IT Beratung GmbH
AnyWi Technologies
Cloud&Heat Technologies GmbH
Delft University of Technology
Eindhoven University of Technology
ENGIE – Laborelec
Fraunhofer IIS/EAS
NXP Semiconductors Belgium NV
NXP Semiconductors Germany GmbH
Philips Electronics Nederland B.V
Philips Medical Systems
Sandgrain
SIRRIS HET COLLECTIEF CENTRUM VAN DE TECHNOLOGISCHE INDUSTRIE
Stichting IMEC Nederland
Technical University of Munich
Technolution BV
University of Ulm

COUNTRIES INVOLVED

- Belgium
- Germany
- Netherlands

PROJECT LEADER

Christopher Nigischer
NXP Semiconductors GmbH

KEY PROJECT DATES

August 01, 2019 to July 31, 2022

The innovation strength for novel solutions will be enhanced by the cooperation between application owners (like smart grids, industry, eHealth) and leading-edge providers (of secure IC and sensors, security, AI/ machine learning);

3. To identify and develop new European market-leadership opportunities: SunRISE's use of disruptive security-oriented technologies (such as homomorphic encryption, lithography, AI and machine learning) in IoT-related domains (like intrusion-detection mechanisms) will improve European strengths. These technologies, together with the project's disruptive approach to business and markets, will also help the micro and nanoelectronics industry and associated sectors create and support future European champions.

The project will be executed by partners from the entire market value-chain. Significantly, they will offer a balanced effort between industry and academia, working towards a shared, integrated security-solution by contributing in such essential areas as security technology and related tools; secure IC and sensor component-building; and IoT systems.

Spreading the news

Effective dissemination, vital in ensuring results are well-tailored to various target-groups, will take place throughout the duration of the project. SunRISE will undertake a series of dissemination initiatives to ensure the sustainability of deployment actions. These will include organising special sessions at major European and international events to maximise the impact and reach the community at large. Project partners will publish in the most representative journals and participate in important conferences. And thanks to the interdisciplinary nature of the project, they will also ensure that they cross the different research domains and communities. In addition, white papers, workshops and presentations will be used to communicate results and findings – including those from participating PhD and Master's candidates – to other relevant industry, scientific and academic players and communities.

A thriving IoT

Gartner Inc. predicted in 2017 that 8.4 billion connected things will be in use worldwide in 2017 and this number will be increase to 20.4 billion by 2020. Based on this forecast, the total spending on endpoints and services could reach almost US$2 trillion in 2017. Regionally, Greater China, North America and Western Europe are the main drivers of connected things and these three regions are predicted to represent 67% of the total IoT in 2017.

Global investments in IoT security was estimated at US$703m for 2017 and is predicted to grow at a CAR (compound annual rate) of 44% to a US$4.4 billion by 2023. These forecasts are based on IoT-security-relevant revenue of major technology companies across 12 industries and 21 technologies.

Importantly, McKinsey & Company reported in 2017 that IoT lacks well-established, overarching standards that describe how the different parts of the technology stack should interact. In other words, there is no standard approach for ensuring the security of critical IoT applications and large players and industry organisations all use their individual approaches. Some segments, such as industrial, still use a small set of proprietary, incompatible technology standards originating from major players. In other segments, such as automotive or smart buildings, standards for interoperable devices are very rudimentary, leading to high security risks and costs.

These are typical issues SunRISE is already anticipating. The best way of ensuring various international standards are implemented is through regular contacts with such regulatory, standards and certification organisations as ECSO, Eurosmart, AIOTI and ENISA.

Aeneas Office
44 rue Cambronne
F-75015 Paris - France
Tel. +33 1 40 64 45 80
Fax +33 1 40 64 45 89
Email penta@aeneas-office.org
www.penta-eureka.eu

Penta (E! 9911), the EUREKA Cluster for Application and Technology Research in Europe on NanoElectronics, will bring about technological leadership for a competitive European information and communications technology industry.