HORIZON 2020

Securing the Internet of Things with a unique microchip fingerprinting technology

Results in Brief

Innovative identification methods secure IoT devices

IoT devices are so insecure that they threaten the entire internet. Now, millions of legacy devices can be individually identified and authenticated.

DIGITAL ECONOMY

SECURITY

© Blue Planet Studio, Shutterstock

The Internet of things (IoT) refers to simple hardware devices connected via the internet. Examples include doorbell cams, wearable health monitors, fire alarms and city traffic lights. By some estimates, the world may have 50 billion such devices by 2025, and 1 trillion by 2030.

Although they provide convenient services, IoT devices are very insecure and can be easily hacked. Hacked devices can be made to hack other devices. These situations threaten the reputations of businesses, and they can cause many kinds of real danger for people. The vulnerability occurs because the devices' memory and processing capacity are too low for sophisticated security.

Replacing billions of legacy devices with updated hardware is not feasible. However, the EU-funded INSTET project has developed a way to secure IoT devices that avoids such replacement. The current project improved device identification technology developed in an earlier SME Instrument Phase 1 feasibility study project of the same name. The new project confirmed the concept's commercial potential.

Every device physically identified

The innovative method first assigns an identifier to every IoT device, based on its unique physical characteristics. Physical identifiers are derived using special algorithms that measure random variations generated in hardware manufacturing process, via a physical unclonable function (PUF) developed by the project. This is known as silicon biometrics, and essentially fingerprints every IoT device in an unforgeable way.

Once each device has an identifier, before secure exchange of data is possible, the identifier must be authenticated. Otherwise, it cannot be guaranteed that devices are communicating with the correct party. The ability to verify device identity is what allows the simple IoT devices to be secured.

The PUF is a component of the INSTET security system. It enhances the entire security system with strong and unforgeable high-grade security services. “The main advantage,” says project coordinator Georgios Selimis, “is that you do not need to programme the root key from outside. So the key always stays inside, and then is always secure.”

Easy chip upgrades

Additionally, the PUF is based on the ubiquitous static random-access memory (SRAM) circuits. “Therefore, our approach is scalable to all IoT devices,” adds Selimis, “since SRAM is a component found in all microcontrollers, even the low-cost ones. As a result, we are able to retrofit those millions of IoT devices that are installed in the field, without requiring a redesign of the products.” This is the only solution on the market that provides strong hardware-based security, using only software that is easily deployed on IoT devices of limited processing power.

The system targets three separate IoT segments. INSTET Wearables provides end-to-end security for wearable devices. INSTET Medical supports binding of the software with medical device hardware. Finally, INSTET Critical Infrastructures supports IoT cloud connectivity. Researchers successfully created different software architectures for each application. The team also created and operated demonstrators for each market segment. Project staff developed detailed market analyses and exploitation plans.

Next, the consortium will focus on developing market-specific standards and regulations. The outcome will be the closing of a major security weakness affecting IoT devices.

Keywords

INSTET | IoT | security | Internet of Things | device identification | physical unclonable function | silicon biometrics

Discover other articles in the same domain of application

Pared-down system brings tracking closer to the mass market

9 April 2018

Middleware system utilises AI to coordinate building energy management

8 May 2020

Enabling interoperability and seamless data exchange in the energy sector

20 March 2025

Cloud-based GPS/GNSS tracks locations using a tiny amount of power

20 January 2023

Project Information

INSTET

Grant agreement ID: 811509

Project website

DOI
10.3030/811509

Project closed

EC signature date
30 May 2018

Start date
1 June 2018

End date
31 May 2020

Funded under
INDUSTRIAL LEADERSHIP - Innovation In SMEs

Total cost
€ 2 496 362,50

EU contribution
€ 1 747 453,75

Coordinated by
INTRINSIC ID BV
Netherlands

Last update: 6 November 2020

Permalink: https://cordis.europa.eu/article/id/422611-innovative-identification-methods-secure-iot-devices