

HORIZON  
2020

# Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience

## Results in Brief

### New tools help secure embedded devices

Simple computer chips can be hacked, and manufacturers develop protections, but fairly evaluating the defences is complex.



DIGITAL ECONOMY



SECURITY



© Hamik, Shutterstock

So called embedded devices are simple computer chips, designed for a single function, built into common products. Examples include credit card smart chips, or the chip in car keys that allows remote unlocking of a specific vehicle.

Although such devices use encryption, they are vulnerable to hacking. Conventional decryption (of intercepted emails, for example) relies on analysis of sent and received messages, making it difficult to derive the


encryption key directly. Yet, with an embedded chip, the hacker has physical access to the device. Given certain inputs and outputs, measurement of the amount of power consumed during processing can eventually reveal the cryptographic key.

These attacks are called [side channel attacks](#) . Since the 1990s, the banking smart card industry has developed numerous countermeasures that do not reveal cryptographic keys.

The problem is that such countermeasures are difficult to assess. No consensus

exists on the most suitable methods, and to date it has not been possible to compare various assessments. Assessments are generally complex (because attacks have been increasing in sophistication), and computationally intensive, which means expensive.

## Better protection


The EU funded [REASSURE](#)  project developed improved methods for evaluating countermeasures against the hacking of embedded devices. Internet of things (IoT) devices are now prime targets for attack; however, IoT manufacturers lack the expertise and equipment needed to evaluate countermeasures. To help manufacturers, the project developed automated code checking tools for IoT developers. Researchers also delivered a set of additional software tools, supported with training.

Engineers developed the tools specifically for companies developing embedded devices and countermeasures. Companies must internally assess the effectiveness of their countermeasures. Next, the company goes to an evaluation lab, which will independently evaluate the device's resistance to side channel attacks. "As this external evaluation is expensive," explains Dr Francois Koeune, project coordinator, "it is in the interest of both parties to make it as efficient as possible."

The new tools are more reliable than previous evaluation methods and more likely to find weaknesses. The tools also help the independent lab maintain its certification to conduct such assessments.

## Improved performance

Industrial partners implemented the tools developed during the project, often resulting in significant improvement. In the best cases, the tools reduced the number of traces needed for analysis by a factor of 10, and reduced necessary computing power by 16 times. The new tools also aided the product reassessments necessary after every detected security weakness. Using the tools, one partner was able to skip half the usual testing without loss of security. Finally, the tools proved more comprehensive, and in 10 % of internal validation cases, they detected security breaches not previously detectable at that stage.

"Also, there is an ISO standard in the field which entered its revision phase during our project," adds Koeune. "We issued documents highlighting what we considered to be significant weaknesses in this standard. The [International Standards Organisation](#)  acknowledged this and will open the standard for revision. REASSURE's tools, plus the training in their use, represent an important development in securing these ubiquitous devices".

# Keywords

- REASSURE
- tools
- countermeasures
- embedded devices
- security.
- evaluation
- hacking
- side-channel attack

## Discover other articles in the same domain of application



Pared-down system brings tracking closer to the mass market

9 April 2018  



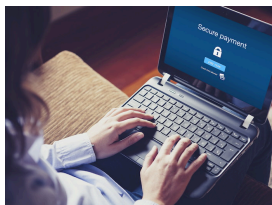
Enhanced situational awareness improves decision-making during extreme weather events

4 October 2019   



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

20 January 2023 



## An innovative approach to corporate payments fraud prevention

15 November 2019



### Project Information

#### REASSURE

Grant agreement ID: 731591

[Project website](#) 

#### DOI

[10.3030/731591](https://doi.org/10.3030/731591) 

Project closed

#### EC signature date

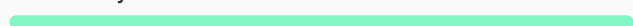
27 November 2016

#### Start date

1 January 2017

#### End date

31 March 2020



#### Funded under

INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

#### Total cost

€ 3 528 635,00

#### EU contribution

€ 3 478 747,50

#### Coordinated by

UNIVERSITE CATHOLIQUE DE LOUVAIN



Belgium

**Last update:** 7 September 2020

**Permalink:** <https://cordis.europa.eu/article/id/422031-new-tools-help-secure-embedded-devices>

European Union, 2025