PRESS RELEASE

Trusted Objects expert on lightweight cryptography gives a presentation to the NIST

Alexandre Adomnicai, cryptography expert at Trusted Objects will give a presentation on his current research at the next NIST Lightweight Cryptography Workshop that will take place on October 17-18, 2016 at NIST (US National Institute of Standards and Technology) Headquarters, in Gaithersburg, Md., USA.

ROUSSET, FRANCE, October 17, 2016 – Trusted Objects, a specialist in Security for the Internet of Things (IoT), focuses on developing security solutions fully adapted to the specificities of the IoT environment.

Typically, a connected object has limited computing resources, is always on, can be physically accessed by attackers and needs to stand a very long lifecycle (up to 20 years). At the same time, a connected object needs to be secure, making lightweight cryptography a perfect candidate for the specific requirements of this new industry.

Alexandre Adomnicai, Trusted Objects cryptography expert, will discuss his paper "On the importance of considering physical attacks when implementing lightweight cryptography" at the next NIST Workshop on Lightweight Cryptography. His presentation will focus on the fact that as lightweight cryptography is designed for devices deployed in hostile environments (*i.e.* physically accessible to attackers), it has to be particularly resistant to physical attacks. The presentation will introduce two such attacks (a side channel and a fault one) that have been successfully demonstrated, analyze their complexity and actual feasibility, and discuss possible countermeasures.

This presentation takes place in a context where the NIST has launched its lightweight cryptography project to study the performance of the current NIST-approved cryptographic standards on constrained devices and to understand the need for a dedicated lightweight cryptography standard. The NIST has now decided to create a portfolio of dedicated lightweight algorithms through an open process similar to the selection of modes of operation of block ciphers.

Sami Anbouba, CEO Trusted Objects, declares: "We are very proud to see our research conducted by Alexandre Adomnicai recognized by the NIST. As experts in IoT security, we know that innovation in cryptographic algorithms and their implementations is of the utmost importance in order to bring the required level of security to the IoT world."

Alexandre Adomnicai is currently undertaking a CIFRE (Convention Industrielle de Formation par la REcherche - Industrial Agreement of Training through Research) thesis under the supervision of Jacques Fournier (CEA LETI), Assia Tria (CEA Tech) and Laurent Masson (Trusted Objects) titled "Secure implementation & integration of lightweight cryptography for the internet of things". He previously graduated from Université Denis Diderot (Paris VII) with a Master's degree in Mathematics and Computer Science applied to Cryptology.

About Trusted Objects

Trusted Objects is a leading independent player in the Secure IoT market, providing innovative embedded firmware and services to dramatically enhance the security of connected devices. The IoT world is so large and fragmented that it requires security solutions to be scalable, configurable, easy to integrate and cost effective. Trusted Objects solutions include embedded Secure Elements, firmware and software. They are customizable by firmware and cost effective, they are scalable and can be implemented easily from low volumes to mass production.

Trusted Objects also delivers a set of services including security assessment, personalization engine, keys and certificates management, fast prototyping to accelerate the deployment of comprehensive solutions that meet the highest security requirements.

More information at www.trusted-objects.com

Contact
Hervé ROCHE, VP Marketing, contact@trusted-objects.com