TRUSTED OBJECTS

PRESS RELEASE

Trusted Objects demonstrates end-to-end security from IoT edge devices to Amazon Web Services

AIX EN PROVENCE, FRANCE, April 4, 2018 – Trusted Objects, a security expert for the Internet of Things (IoT), announces a new step in edge device to cloud security with a plug and play secure connection between a Secure Element running with its secure firmware TOSF and Amazon Web Services (AWS) IoT.

The growing demand for security in the Internet of Things is requiring a global end-to-end approach, as securing each part of the IoT chain separately cannot bring a satisfactory answer. For this reason, Trusted Objects is demonstrating that thanks to its TOSF embedded secure firmware, it is possible to set up a secure end-to-end connection between a Secure Element and Amazon Web Services (AWS) IoT platform.

Edge device-to-cloud seamless security is now facilitated for system integrators thanks to the projects Trusted Objects has just published on hackster.io website. These demonstrations are showing how to connect edge devices to AWS IoT, based on either LoRaWAN or TLS protocol. The projects objective is to securely provision edge device identifiers (LoRaWAN), digital certificates (TLS) and more generally various data related to each device to make them available in AWS cloud. With this solution, the edge device will be automatically authenticated by the AWS servers during its whole life cycle and will communicate data securely from end to end.

The first project demonstrates how to secure a LoRaWAN node using Trusted Objects secure firmware into a Secure Element (SE), with Kerlink gateway, Actility servers and AWS IoT backend. The SE is based on a secure hardware platform designed by Idemia StarChip and is the root-of-trust to achieve end-to-end security, first by providing strong authentication between the LoRaWAN node and the gateway and, secondly, by encrypting/decrypting applicative data up to the servers and using HTTPS protocol between servers and AWS.

The second project implements a TLS protocol for end-to-end security between a device embedding a SE running on Trusted Objects secure firmware and AWS IoT. Trusted Objects secure firmware is enabling the SE to handle the full TLS stack, which consists in certificate-based mutual authentication with AWS IoT, secure session key establishment and encryption/decryption of messages between the device and AWS IoT. In this context, a secure communication between the device and AWS IoT is automatically established, ensuring end-to-end security.

Sami Anbouba, CEO of Trusted Objects, declares: "End-to-end security is essential to create trust in the IoT ecosystem. Trusted Objects contributes to creating trust thanks to its global end-to-end approach based on its Secure Element and systems expertise."

Trusted Objects will present its projects on Avnet booth, during SIdO, a major international event dedicated to the Internet of Things taking place in Lyon, France on April 4 and 5, 2018.

About Trusted Objects

Trusted Objects is a leading independent player in the Secure IoT market, providing innovative embedded firmware, to dramatically enhance the security of connected devices.

The TOSF embedded secure firmware has been successfully ported into a Secure MCU designed by Idemia StarChip, leading to a family of Secure Element (SE) fully optimized for battery-powered devices, certified and being the root of trust to meet the end-to-end security needs of the IoT.

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

Contact

Hervé ROCHE, VP Marketing, contact@trusted-objects.com
More information at http://www.trusted-objects.com