TCG Announces DICE Architecture for Security and Privacy in IoT and Embedded Devices

Members to Discuss Foundational Trust and Security for the Industrial IoT at Oct. 3 Session, IoT Solutions World Conference

September 18, 2017 01:00 PM Eastern Daylight Time

PORTLAND, Ore.--(BUSINESS WIRE)--Trusted Computing Group (@TrustedComputin) has released the Device Identifier Composition Engine (DICE) Architecture for securing resource-constrained devices that make up the Internet of Things.

The DICE Architecture provides critical security and privacy benefits to IoT and embedded systems where traditional Trusted Platform Modules (TPM) may be impractical, while also enabling support for those devices with a TPM for additional security benefits.

Security capabilities this new approach enables include strong device identity, attestation of device firmware and security policy, and safe deployment and verification of software updates, which often are a source of malware and other attacks. The DICE Architecture, with its hardware root of trust for measurement, breaks up the boot process into layers, and creates unique secrets and a measure of integrity for each layer. This means if malware is present, the device is automatically re-keyed and secrets are protected.

To make it simpler for device makers and vendors, there is no requirement to retain or store databases of unique secrets. The DICE Architecture integrates easily into existing infrastructure, and the architecture is flexible and compatible with existing security standards.

TCG members Microsoft, Micron and STMicroelectronics are providing info and resources on using DICE, and other member announcements will follow.

At the IoT Solutions World Congress, Tuesday, Oct. 3, 09:30-13:00 p.m. in Fira Barcelona, hall CC5, room 5.1, TCG members GE, Infineon, Microsoft, OnBoard Security and Wibu-Systems will host a session about how to implement DICE and the group's efforts to secure the industrial IoT.

Speakers from the companies will talk to attendees about deploying techniques to better secure the industrial Internet of Things, how to ensure identity and security of very constrained "things," and using available APIs for encryption, authentication, device identity and integrity.

TCG session attendees must have a conference or expo pass to the congress event and can save 500€ on a Full Conference Pass with code 526E24AF or get a free Expo Pass with code 111B9B47. http://www.iotsworldcongress.com/visit/passes-and-prices/

About TCG

TCG (@TrustedComputin) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. More information about TCG is available at www.trustedcomputinggroup.org. Follow TCG on Twitter and on LinkedIn

Tweet this: @IOTSWC secure #IIOT session Oct 3. free expo pass 111B9B47 http://ow.ly/oUbj30eLftt

Contacts

PR Works, Inc.
Anne Price, +1-602-330-6495
anne@prworksonline.com
Twitter: @TrustedComputin

Tweets by @TRUSTEDCOMPUTIN