



Trusted Computing Group to Address Industrial Security

Posted: Sep 27, 2017 9:16 PM CEST
Updated: Sep 27, 2017 9:16 PM CEST

New Sub Group to Develop Guidance Documents and a TPM Profile for Security of Industrial Equipment

PORTLAND, Ore. --(BUSINESS WIRE)

Members of [Trusted Computing Group](#) (@TrustedComputin) today announced new efforts to provide foundational security for industrial systems in increasingly connected factories and other industrial environments facing growing security threats.

"The connection of manufacturing, critical infrastructure and other industries to the Internet brings many benefits, but the associated potential for ransomware and malicious attacks presents major risks that can cause chaos for businesses and their customers and partners," said TCG Embedded Systems Work Group and Industrial Sub Group Chair Steve Hanna, Infineon Technologies. "TCG members offer deep experience in embedded security that can be applied to industrial security, whether connected or not, to protect the systems, data and networks that we all rely on daily."

The [Industrial Sub Group](#) will develop guidance for securing industrial equipment and a profile for using TPM 2.0 in industrial equipment. TCG members have contributed to the development of the Industrial Internet Consortium (IIC) [Internet Security Framework](#), which recommends using the TPM to secure endpoints.

Noted Monty Wiseman of GE and various TCG work groups, "Security has become the leading consideration for industrial networks connected to the wide variety of things. The work TCG has done around trust and security in for non-industrial systems such as PCs and servers has direct application to the industrial market, and we can provide specific guidance, specifications and how-to."

"TCG is playing a significant role in bridging the gap between specification and application of embedded security best practices specifically for Industrial," said Chetan Khona, industrial IoT strategy and business manager at Xilinx. "This is a critical step in the mainstream adoption of robust security for these systems."

The TPM also is noted as a hardware security approach to protect authenticators, such as cryptographic keys, in IEC/ISA [62443](#). The [Industrial Sub Group](#) will be looking at further development and engagement in this standards effort as part of its scope.

On Tuesday, Oct. 3 at the [IoT Solutions World Congress](#), TCG members GE, Infineon, Microsoft, OnBoard Security and Wibu-Systems will host a session about the group's efforts to secure industrial equipment.

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](#). To join the effort to secure industrial systems, go to <https://trustedcomputinggroup.org/membership>.

Brands and trademarks are the property of their respective owners.

Tweet this: @TrustedComputin forms subgroup to tackle industrial equipment security
<http://ow.ly/767k30frYME>

View source version on businesswire.com:

<http://www.businesswire.com/news/home/20170927006045/en/>

PR Works, Inc.

Anne Price, +1-602-330-6495

anne@prworksonline.com

Twitter: [@TrustedComputin](#)

Copyright Business Wire 2017

Information contained on this page is provided by an independent third-party content provider. Frankly and this Site make no warranties or representations in connection therewith. If you are affiliated with this page and have questions or removal requests please contact pressreleases@franklyinc.com