Trusted Computing Group Members to Share Wide Variety of Solutions for Securing Enterprise, Internet of Things, Automotive and Industrial Control Systems Environments During RSA Conference 2015

Association Session Will Help Attendees Understand How to Implement Trusted Computing Across Wide Range of Applications

RSA Conference USA 2015

April 17, 2015 12:00 PM Eastern Daylight Time

PORTLAND, Ore.--(BUSINESS WIRE)--Next week at the RSA Conference 2015 Trusted Computing Group association session, members will showcase more than 20 examples of trusted computing for enterprise, IoT, network, embedded and mobile computing security – the widest variety and largest number of trusted computing demos ever shown at RSA.

RSA attendees can see the demonstrations during the half-day session "Should We Trust Mobile Computing, IoT and the Cloud? No, But There Are Solutions" in Moscone West 2002/2006, 9 a.m. – 1 p.m. Pacific on Monday, April 20.

Solutions include:

- Management of self-encrypting drives (SEDs) for compliance and data protection: Absolute Software and Seagate
- Securing data with the TPM in an archiving appliance to prevent attacks or unauthorized access: Artec IT
- Securing IoT sensors and actuators managed by a cloud application over the public network with TCG TNC standards and the TPM: Cisco, HSR, Infineon, Intel
- Protection of corporate data from insider threats with a cross-platform data loss prevention and mobile device management solution: CoSoSyS
- Near real-time network security with an IF-MAP-based SIEM to enable various components to monitor, evaluate and visualize the network state: Decoit and the University of Applied Science Hannover
- A host cryptographic accelerator integrated with the TPM for protection of encryption keys: Dell
- Establishing trust in embedded systems in the IoT with a TPM 2.0 and TPM Software

Stack 2.0 to determine firmware and software state: Fraunhofer SIT

- A remote firmware update with integrity enabled by the TPM for automotive electronic control units: Fujitsu Limited
- Trusted computing in a network device using the TPM for measured boot for detection of tampering of software: Huawei
- Managed IoT security from silicon to cloud with separation of hardware, software and data security capability from operational applications: Intel
- Trusted device lifecycle management for IoT devices, using enterprise key management structures for industrial controllers and vehicles: Integrated Security Services
- TPM Software Stack for the TPM 2.0 that includes a test application, system code for TPM commands and a Linux device driver: Intel
- A cloud data security gateway appliance for secure data access to and from common cloud storage services protected by the TPM: Intel
- Remote platform attestation with the TPM for protecting users and networks with BYOD and cloud computing environment: JWSecure
- Trusted I/O for IoT devices: Microsoft
- Standards-based mobile security including automation detection of out of compliance devices, data aggregation, intrusion prevention and data visualization based on TCG IF-MAP standards: DECOIT, Trust at HSH and PulseSecure
- A BYOD and NAC solution to provide intelligent, dynamic detection and remediation of compromised systems: PulseSecure and Rebasoft
- Secure boot and remote attestation for infrastructure security in cloud computing environments: Swisscom and Intel
- A secure overlay network for M2M connectivity and communications, including process control networks: Tempered Networks and PulseSecure
- Two-factor authentication using a virtual smart card with the TPM: Wave Systems
- A cloud-based service for managing self-encrypting drives, BitLocker and OSX FileVault: Wave Systems
- Solid-state self-encrypting drives with a TCG-standardized management interface supporting multiple software vendors for management: Samsung and Wave Systems
- Management of self-encrypting drives with pre-boot authentication using the TPM embedded on a laptop: WinMagic and Micron

Panels will address the concepts of “do I know you, can I trust you?” with an emphasis on the rapidly growing amount of sensor data, personally identifiable information, financial transactions and health data, and intellectual property going

through a variety of networks and touching a variety of devices.

Attendees will have the opportunity to win a one terabyte SSD 850 EVO self-encrypting drive from Samsung; a Raspberry Pi 2 IoT development kit with a TPM 1.2 daughterboard from Infineon; and a Microsoft Surface Pro 3 tablet, including Infineon TPM 2.0, also from Infineon.