RSA® CONFERENCE 2014

Get Proactive with Security:

A SESSION ON USING TRUSTED COMPUTING TO FREE SECURITY RESOURCES FOR THE DAY-TO-DAY FIRES

TRUSTED COMPUTING GROUP™

SESSION SCHEDULE

10:00AM Welcome and Introduction to the Trusted Computing Group (TCG)

Dr. Joerg Borchert – President, Trusted Computing Group

10:15AM Panel: Endpoint Compliance and Security Automation

Moderator:

Jon Oltsik – Senior Principal Analyst, Enterprise Strategy Group (ESG)

Panelists:

Steve Whitlock – Chief Security Architect, The Boeing Company

Dan Griffin – Founder, JW Secure & Microsoft Enterprise Security MVP

David Waltermire – Security Automation Architect, NIST

11:00AM Demonstration Showcase

11:30AM Panel: Will the Real Trusted Platform Module (TPM) Please Stand Up?

Moderator:

Paul Roberts – Editor-in-Chief & Founder, The Security Ledger

Panelists:

Monty Wiseman – Security Architect, Intel Corporation

Dustin Ingalls – Partner Group Program Manager, Windows Security, Microsoft

Gal Shpantzer – Security Consultant & Analyst, SANS

12:15PM Lunch and Demonstration Showcase

1:00PM Panel: Mobile Device Security: Fact or Fiction

Moderator:

Victor Wheatman – Global Information Security Market Analyst & Enterprise Advisor

Panelists:

Rick Doten – Chief Information Security Officer, DMI, Inc.

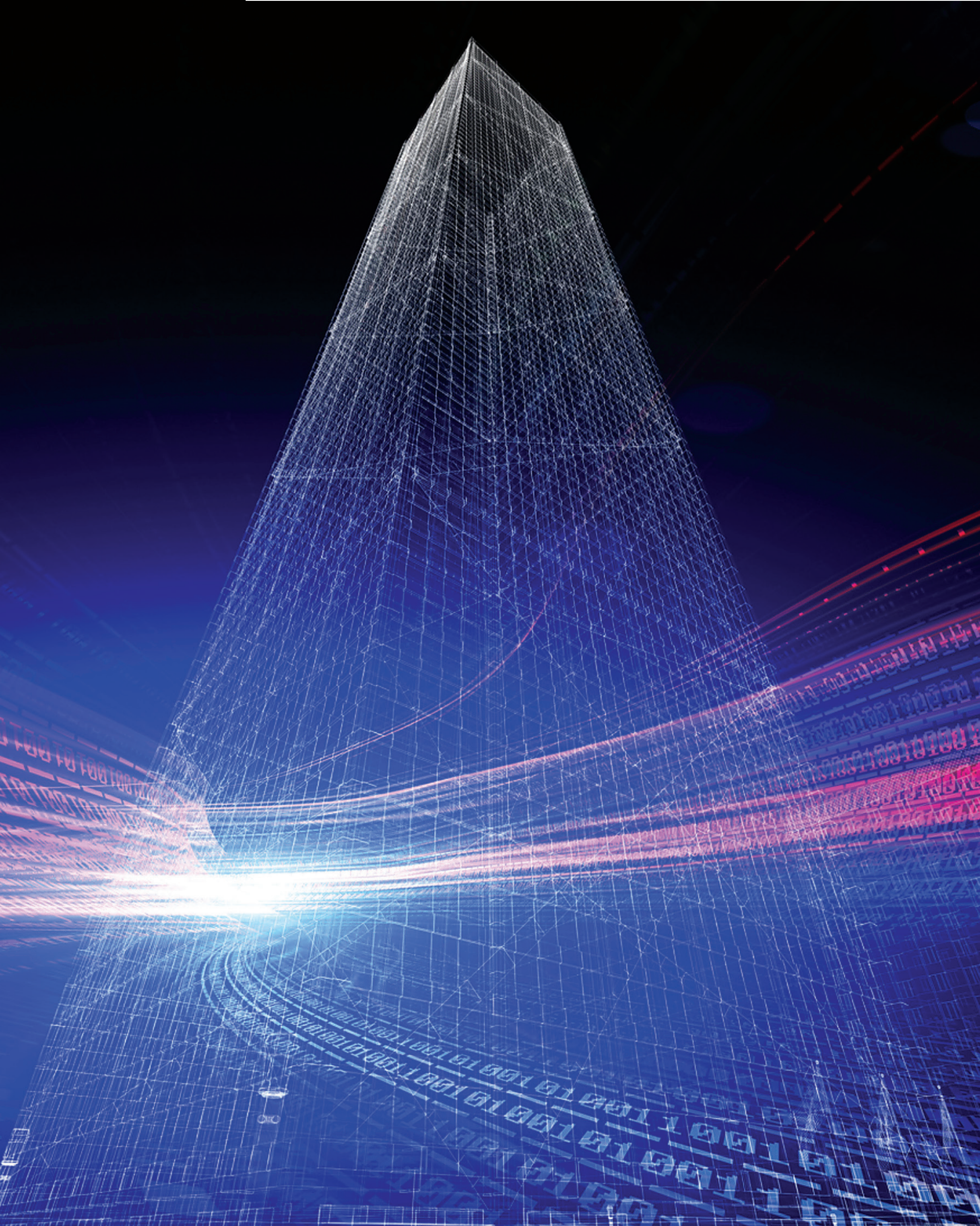
Jason Conyard – Information Technology Vice President, Juniper Networks

Eric Green – SVP, Business Development, Mobile Active Defense & Program Director, SC World Congress

1:45PM Closing Remarks

End of Session Live Drawing

DEMONSTRATION SHOWCASE



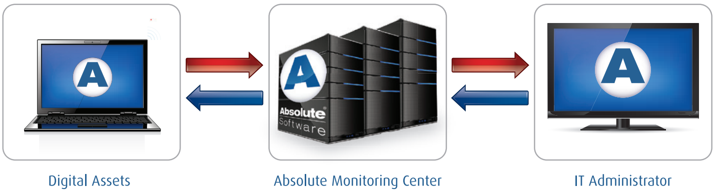
AbsoluteSoftware | Seagate

Endpoint Compliance with Self-encrypting Drives

Trusted Computing Technologies supported: Opal-standard Seagate self-encrypting drives

Absolute Software & Seagate will demonstrate the management of Seagate Opal-compliant self-encrypting drives (SED) using Absolute Secure Drive. Additionally, compliance will be highlighted via Absolute's Encryption Status report, a cloud based report available within Absolute Computrace, which alerts on the encryption status of endpoints across a wide range of software encryption platforms.

Regardless of whether or not a device is on or off-network, in Timbuktu or Toledo, the Encryption Status report alerts on the endpoint's compliance with the organization's encryption policies, and informs administrators if a device is at risk. If a device is equipped with a Seagate drive, the report will also indicate if the drive is an SED, and the drive's management status.



Asguard Networks | JUNIPer NETWORKS

Practical Network Segmentation for Industrial Control System Security

Trusted Network Connect (TNC) IF-MAP and Metadata for Industrial Control Systems Security enable dynamic protection for critical infrastructure networks interconnecting with enterprise and public networks.

Integration of Industrial Automation and Control Systems (IACS) with enterprise IT and shared public networks is increasing, driven by considerations from cost to monitoring to the introduction of new products and services. With this increased connectivity comes increased risk: trust relationships and boundaries are weak or undefined, poorly managed systems are exposed to infection from shared networks, and protocols and devices never designed for security are accessible to attackers and susceptible to misconfiguration.

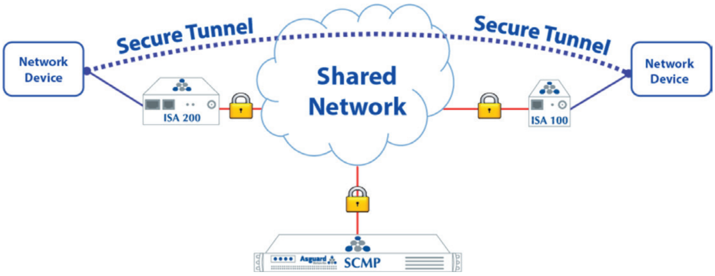
In the demonstration, an industrial automation device is controlling the operation of local control system inputs and outputs. A Human Machine Interface (HMI) is used to monitor and control the automation device for providing Supervisory Control and Data Acquisition (SCADA). The Asguard Networks SimpleConnect™ Industrial Security Appliances (ISA) and Management Platform (SCMP) implement TNC standards to provide dynamic protection for the ICS.

TCG Technology Supported

A TNC interface underlies this protection of the interconnection between a process control network and an enterprise network:

- IF-MAP enables coordination of configuration, behavioral, location, and policy information between provisioning and network management applications, policy management and enforcement devices, and network intelligence and visibility components.

- IF-MAP Metadata for Industrial Control Systems Security specifies the pattern of IF-MAP usage for the various components providing enhanced security and management of control system networks.



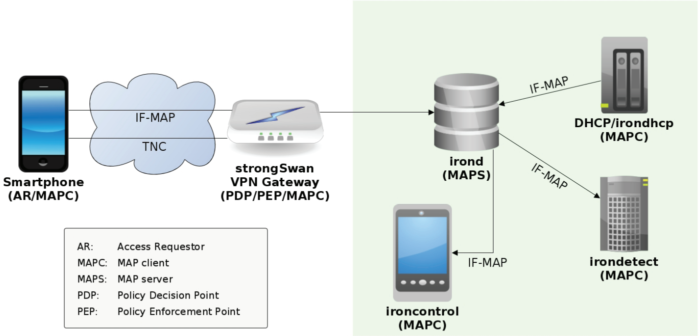
The SimpleConnect™ product line from Asguard Networks implements TNC standards to simplify the management of multiple independent private overlay networks and restrict connectivity within these networks. SimpleConnect™ uses the IF-MAP Metadata for ICS Security specification, using IF-MAP clients, to strengthen the security of ICS communicating over shared networks. Juniper Networks implements the IF-MAP Server, which provides a centralized coordination service for the SimpleConnect IF-MAP Clients.

Near Real-time Network Security with Open Source Tools

Trusted Computing Technologies supported: IF-MAP, TNC

The demonstration intends to illustrate how Trusted Network Connect (TNC) Open Source tools of multiple vendors can be combined to smartly address the complex scenario of securing a Bring Your Own Device (BYOD) scenario. The example scenario integrates the strongSwan (www.strongswan.org) VPN solution, developed by the University of Applied Sciences in Rapperswil (Switzerland), with several iron* (github.com/trustathsh) tools by the Trust@HsH research group at the University of Applied Sciences and Arts in Hanover (Germany), and the Android-IF-MAP-Client (github.com/decoit/Android-IF-MAP-Client) by DECOIT GmbH, a SME company from Bremen (Germany).

The combination of those tools allows implementing a network security solution which responds to security incidents in near real-time. The scenario is set in a Bring Your Own Device (BYOD) environment where employees use their own smartphones for enterprise tasks. Different TNC IF-MAP tools are combined to enforce corporate policies affecting the employees' Android cell phone devices on initial network connection and to continuously monitor policy conformity if behavioral changes of the devices occur.

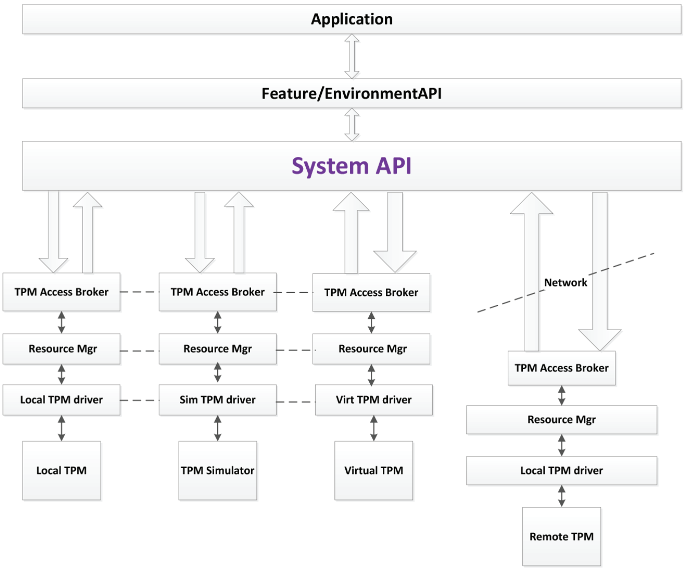


AR:	Access Requestor
MAPC:	MAP client
MAPS:	MAP server
PDP:	Policy Decision Point
PEP:	Policy Enforcement Point

TCG's TPM Software Stack (TSS) System API

Trusted Computing Technologies supported: TPM, TSS

The TSS, TPM Software Stack, for TPM 2.0 is an industry application programming interface being developed by TCG to enable the TPM 2.0 industry. This demonstration showcases the lowest level of the stack, the system API, which is nearing completion. This level of the stack enables "bare metal" access to all the TPM 2.0 functionality and will form the basis of the final complete TSS stack. The demo shows a test application sending and receiving TPM 2.0 commands to the TPM 2.0 simulator. This demo is an Intel sample implementation of the TCG TSS 2.0 System API specification in development.



The diagram above shows where the TPM 2.0 device fits in the TSS stack.

Data Protection in a BYOD World: Security Automation

Trusted Network Connect (TNC) enables consistent data protection & secure access across a wide range of endpoint devices - including BYOD - through security automation.

Organizations are increasingly seeing staff using their laptops, smartphones, and tablets in the office, at home, and on the road. The traditional desktop is no longer at the center of the end-user's universe. With the trend toward employees bringing their own devices to work and accessing corporate resources, data protection in a BYOD world means organizations must manage access to corporate networks to minimize risk to the organization while maximizing value to employees, contractors, and even guests.

The problem of an organization's data residing on unmanaged or less-trusted devices presents a set of risks, both in terms of data protection as well as for compliance with business, regulatory, and audit policies. In order to make the trust decisions that provide users access to corporate resources needed to get their jobs done, IT must find simple, low-impact ways to gather required information about these devices.

This demonstration presents a multi-layered approach to creating a profile of an unmanaged device that a user brings to the corporate network. Through the use of TNC standards-based technology enabling multi-vendor interoperability, this solution presents a comprehensive view of the endpoint and its expected behavior/profile, which can be used for informed, automated access control decisions.

TNC standards underlie this integration of endpoint identification, device profiling, and network access control:

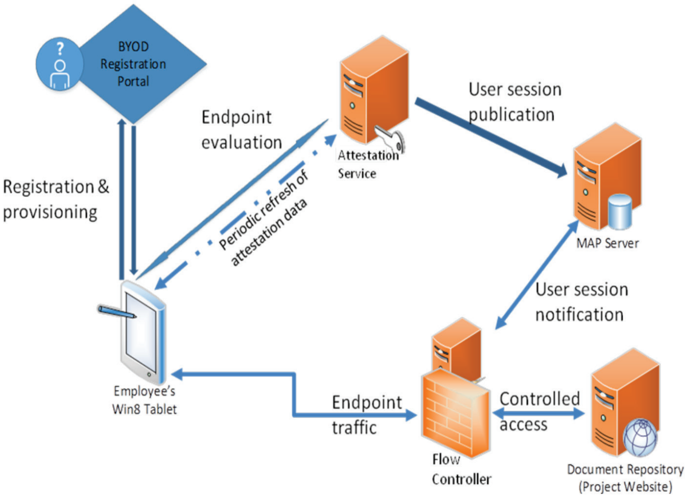
- The BYOD Attestation Service acts as a TNC Metadata Access Point (MAP) Client, identifying and health checking BYOD devices, issuing SAML tokens, and publishing session information to the TNC MAP Server; other network devices can use that information to apply appropriate resource and network access controls.

- The Microsoft SharePoint server acts as a resource provider, consuming SAML information and providing appropriate access to resources.

- The Juniper Networks Junos Pulse Access Control Service + SRX Series Services Gateway acts as a Flow Controller MAP Client, consuming the user session information from the MAP Server and enforcing resource access policy.

- The Infoblox Orchestration Server acts as a MAP Server, providing a clearinghouse for information about connected endpoints.

The TNC IF-MAP interface enables integration of network intelligence among disparate security systems to enable automated enforcement of enterprise security policies.



Solid-State Drives with Self-encryption: Solidly Secure

Solid-State Drives (SSD) supporting TCG's Self-Encrypting Drive (SED) technology provide robust protection of stored data using hardware-based encryption built directly into the drive hardware and electronics, protecting sensitive data from loss or theft or during re-purposing, warranty work, or end-of-life.

Solid-state drives (SSD) offer many advantages over rotating magnetic media such as better reliability and performance, remarkable ruggedness, less weight, no noise, and significantly lower power consumption. Compared to a hard disk drive (HDD), the SSD's booting and application loading times are 50% less and file copy time is 60% less. The current price differential between SSDs and HDDs is steadily declining and the superior advantages of SSDs make that price difference even less consequential. The important cost comparison is not the initial cost, but the life cycle costs of using an SSD versus an HDD. Time savings in doing every task significantly reduces the "wait" time for active users and provides a more productive work experience. Ruggedness and longer life save on repair and replacement.

National and international breach notification laws typically contain encryption 'safe harbors', which exempt stolen or lost data from public notifications. The penalties for notification have been tabulated and are significant. Add self-encryption to the list of SSD superlatives, which is a quantifiable business requirement for protecting stored data. Self-encryption offers faster performance, better security, standards-based, and is "always on", operating transparently, when compared to software-based encryption. The Trusted Computing Group has standardized self-encryption and all major drive manufacturers are providing interoperable products. Solid-state and self-encryption provide an unbeatable combination.

The TCG-standardized management interface allows multiple ISVs to manage SEDs, including Wave, WinMagic, and others.

Solid-State Drive + Self-Encrypting Drive

SIMPLE SOLUTION

- Reduced TCO
- Increased productivity
- Better Performance
- More shock resistance
- Better reliability
- Less power use
- Approaching price parity re: HDD

- Simplified Management
- Robust Security
- Compliance "Safe Harbor"
- Cut Disposal Costs

- Scalable
- Interoperable
- Integrated
- Transparent

TRUSTONIC

Endorsement Credential For TPM Mobile

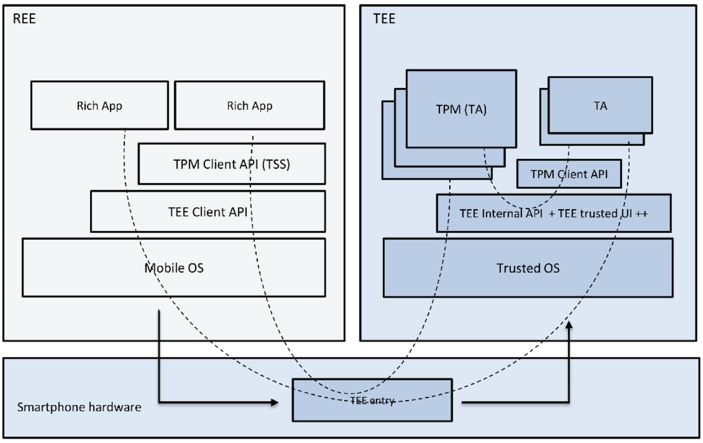
Trusted Computing Technologies supported: TPM Mobile

Trusted Computing Group is driving the deployment of the Trusted Platform Module (TPM) also on mobile platforms, where one instantiation of a TPM is a deployment in a Trusted Execution Environment (TEE). In such an environment, the processor hardware and accompanying firmware set up a programmable, isolated execution environment for which credential software and other security-critical software, so called Trusted Applications (TAs) can be developed. This architecture is illustrated in the figure.

For a TPM, implemented as a TA in a TEE, there are trust anchors that need to be provided by the TEE infrastructure. One such hardware-derived anchor is the endorsement (key) credential, i.e. a digital certificate signed by an external authority that attests the presence of a TPM signing key in the TPM-enabled device. Such a binding is necessary for TCG-defined services such as remote attestation.

In the demonstration, we use a proof-of-concept TPMv2 implementation, implemented as a TA on Trustonic <t-base - a GlobalPlatform™ (GP) enabled TEE. We highlight the process for setting up an endorsement key using standard TPMv2 mechanisms.

In our TPMv2 implementation, we add attestation data to the outSideInfo attribute in the creationData, returned by the TPM2 CreatePrimary function. The attestation data element, which is in a proprietary format, binds the generated endorsement key both to the physical device on which it was generated, and the TA (the TPM2 application) used. A Certification Authority (CA) receiving the public components of the endorsement key and the corresponding attestation data element can connect to Trustonic back-end infrastructure to confirm the attestation binding as one constraint in the generation process of the endorsement credential. In our demonstration, attestation validation is done locally in the CA for the physical devices being demonstrated, and the resulting x.509 certificate is returned to the device requesting the endorsement credential.



Our associated poster explains the protocol flows and the attestation function in more detail. We show the proof-of-concept both with a development board, where protocol details can be explored, as well as with an application and TA on an off-the shelf Samsung Galaxy Tab. Both of these devices are equipped with the Trustonic <t-base TEEs.

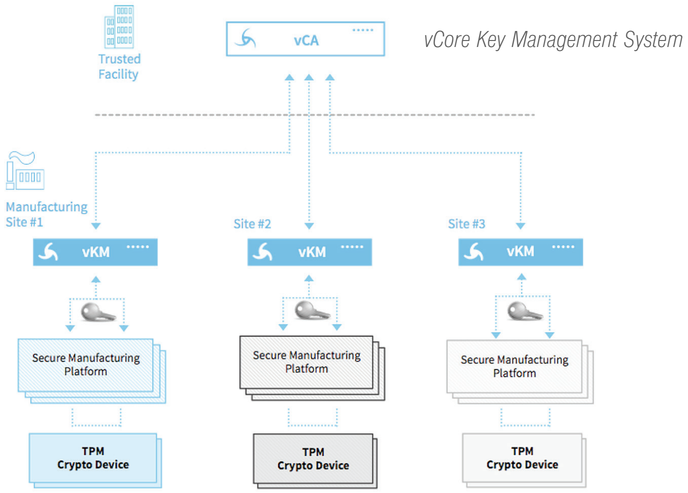
VALICORE technologies | infineon

Enhanced Embedded Security Solutions Using TPMs

Trusted Computing Technologies supported: Embedded TPM enrollment

Embedded system TPM use remains limited despite being a secure and cost effective solution. Latest chips, such as the Infineon Optiga 9645, expand compatibility with the addition of an i2c bus, however lack of support continues to be a barrier. In smaller systems that don't include a BIOS, enrollment must be performed by software during the manufacturing process where traditional manual configuration isn't feasible.

Valicore Technologies is pleased to demonstrate automated TPM enrollment enabling embedded security solutions. The vCore Key Manager is used to easily generate TPM keys and certificates, signed by a common root. The resulting TPM-based cryptographic module is a platform for the development of enhanced security functionality, including: hardware-based key protection, secure boot verification, mutual-authentication, secure communication, and remote attestation.


Trusted Facility
vCA
vCore Key Management System
Manufacturing Site #1
Site #2
Site #3
vKM
vKM
vKM
Secure Manufacturing Platform
Secure Manufacturing Platform
Secure Manufacturing Platform
TPM Crypto Device
TPM Crypto Device
TPM Crypto Device

wave®

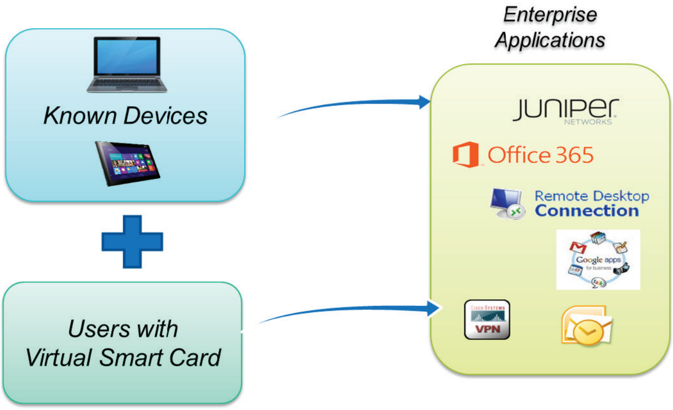
User and Device Identity Solutions: Virtual Smart Cards

Trusted Computing Technologies supported: TPM, TSS

Smart cards and tokens have long been the authentication method of choice for security-minded organizations. By adding "something you have" (i.e. a smart card or token) to the traditional "something you know" (i.e. a user password), tokens and smart cards provide stronger assurance that whoever is accessing the network is who they say they are.

Virtual smart cards provide these security advantages, but are also easier and less expensive to deploy and manage. Virtual smart cards are part of the endpoint hardware itself, so they can't be lost or separated from the user. That means you don't have to buy extras and re-deploy constantly.

This demo shows how Wave takes advantage of the Trusted Platform Module (TPM) to provide enterprises a more secure, less expensive multi-factor authentication solution on Windows 7 and Windows 8.



SED Management with HP Drive Encryption

Trusted Computing Technologies supported: SED, Opal, TPM

Through this demonstration, WinMagic will leverage an HP laptop with an Intel® SSD Pro 1500 SED to showcase how easy it is for business users to take advantage of the security provided by HP Drive Encryption to manage an Intel SED and leverage the built-in TPM as part of the authentication process and recovery process.

WinMagic has worked with HP to develop HP Drive Encryption which is capable of supporting and managing SEDs. Through this demonstration we will show how standalone business users can use a SED to secure their HP laptop and how HP Drive Encryption can manage the security and integrate with pre-boot authentication and the TPM embedded on the device.

This demonstration takes advantage of WinMagic/HP Software, HP Laptops and Intel® SSD Pro 1500 SEDs and will leverage TCG Technologies including Opal 2.0 and TPM.

WINMAGIC DATA SECURITY | Seagate

Security Automation Made Easy with Enterprise Drives

Trusted Computing Technologies supported: SED, Enterprise, Opal

WinMagic along with Seagate will demonstrate the benefits and easy of management of TCG Enterprise drives using WinMagic's SecureDoc data encryption solution combined with Seagate FIPS140 validated Enterprise Drives.

Leveraging WinMagic's new SecureDoc OSA for Servers we will show how enterprises can easily control and manage TCG Enterprise drives provided by Seagate for a server that requires regular administration with minimal physical intervention. Leveraging technology such as PBConnex auto-boot, we'll show how administrators can easily re-boot servers running enterprise drives leverage our Opal based unique pre-boot network authentication with auto-boot to seamlessly perform regular maintenance and overall drive management.

The ability of SecureDoc OSA for Servers relies heavily on the fact the boot drives are TCG OPAL compliant as that allows us to do all administrator authentication, staging etc. in the pre-boot environment leveraging the MBR Shadow to manage the TCG Enterprise drives.

DMI

DMI Mobile Trusted Computing Solutions

Trusted Computing Technologies supported: Samsung KNOX, Bitlocker / TPM, Smartcard Solutions

Secured mobile trusted computing solutions using TPM, Manufacturer and Smartcard technologies to leverage mobile capabilities while maintaining security requirements. The solution will provide a range of industry leading technologies and solutions that are currently being deployed as well as in development. The demonstration provides a set of various solutions that are customizable for individual security and mission requirements. The solutions leverage TPM, device root of trust, as well as two factor authentication mechanisms to secure devices.

The TPM solution will provide two separate mobile apps specifically designed for the Windows / TPM tablets, each utilizing Bitlocker and TPM / PTT. Both apps have consumer-grade user interfaces and user design and leverage advanced mobile platform features.

Samsung Knox enabled devices will show duel persona operational constructs while providing device root of trust through Knox as well as over the air device management. The solution also provides Data at Rest and in Transit security as well as VPN technologies.

The Smartcard solution will illustrate two-factor authentication leveraging Common Access and PIV Cards while remaining platform and reader agnostic.

Welcome and Introduction to the Trusted Computing Group (TCG)

Dr. Joerg Borchert

President and Chairman, Trusted Computing Group

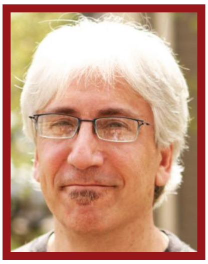
Vice President, Chip Card & Security ICs, Infineon Technologies North America Corporation

Joerg Borchert was born in Hamburg, Germany. He studied Mechanical Engineering and Business Administration at the Technical University of Darmstadt, Germany. He achieved his PhD in Economics before he joined Siemens AG in 1988. Initially Joerg was on the staff of the Corporate Board of Directors handling Mergers & Acquisitions in Munich, Germany. In 1992 he joined Siemens Semiconductor which became Infineon Technologies in 1999.

Joerg moved to the US in 1998 when he was appointed Vice President. He worked for three years in the wireless division and has more than 10 years' experience in the security and chip card semiconductor area. He was instrumental for the roll out of the German Payment Smart Cards in 1996 and the success of the world's largest electronic Passport program in US. In 2008 he became VP and General Manager for the Business Line Government ID. The major success has been the business win of the German National ID card system in fall 2010.

Joerg took over in September 2010 the responsibility for Chip Card and Security for the region Americas. He resides in the US HQs in Milpitas, CA. Currently he and his team are involved in semiconductor security solutions for the smart grid and mission critical embedded systems. He contributed to four patent filings in this area.

Endpoint Compliance and Security Automation

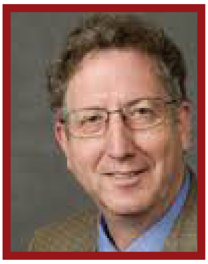


Jon Oltsik - Moderator

Senior Principal Analyst

Enterprise Strategy Group (ESG)

Jon Oltsik is an ESG senior principal analyst and the founder of the firm's Information Security and Networking services. With 25 years of technology industry experience, he is widely recognized as an expert in threat and security management as well as all aspects of network security. Recently, Oltsik has been an active participant with cybersecurity issues, legislation, and technology within the U.S. federal government. Prior to joining ESG, he was the founder and principal of Hype-Free Consulting. He has also held senior management positions at GiantLoop Network, Forrester Research, Epoch Systems, and EMC Corporation.



Steve Whitlock - Panelist Speaker

Chief Security Architect

The Boeing Company

Chief Security Architect Steve Whitlock provides strategic support for Boeing's long-term information security capabilities. This includes the tracking of emerging technologies and the changing threat landscape, as well as helping to influence the direction of the information security industry in support of Boeing's global presence. With more than twenty-five years of research in information security and cryptography, Whitlock has provided strategic input to numerous global agencies, and has served on writing and steering committees for the Intelligence and National Security Association, Internet Security Alliance, Defense Information Base Technology and Architecture Working Group, Trans-global Secure Collaboration Program, and Enduring Security Framework Activity. He has served on the Program Committee for the annual ID Trust conference sponsored by NIST, ACM, OASIS and Internet 2 for eight years. He currently serves on the Jericho Forum Board of Management and was Vice Chair of the Open Group Security Forum for many years. Steve has a master's degree in software engineering from Seattle University.

Dan Griffin - Panelist Speaker

Founder and Microsoft Enterprise Security MVP

JWSecure

Dan is the founder of JW Secure and is a Microsoft Enterprise Security MVP. He previously spent seven years working on smart cards and cryptography for Microsoft while on the Windows Security development team. He is the author of two books, Cloud Security and Control and The Four Pillars of Endpoint Security: Safeguarding Your Network in the Age of Cloud Computing and the Bring-Your-Own-Device Trend. He has also published numerous articles on security software development, as well as on IT security, and is a frequent conference speaker. Dan holds a Master's degree in Computer Science from the University of Washington and a Bachelor's degree in Computer Science from Indiana University.

David Waltermire - Panelist Speaker

Security Automation Architect

National Institute of Standards and Technology (NIST)

David Waltermire is the specification architect for the Security Automation Program at the National Institute of Standards and Technology. Waltermire has been a significant contributor to the Security Content Automation Protocol (SCAP) and CAESARS-FE Continuous Monitoring projects. Prior to joining NIST, he worked as a security consultant where he focused on the advancement of security automation capabilities within the government sector. He comes from an operational background, having managed systems and network operations for internet service providers and also working as a software engineer pioneering the first standards-based configuration assessment tool. His research experience includes computer viruses, vulnerability/misconfiguration identification, categorization and remediation.

Will the Real Trusted Platform Module (TPM) Please Stand Up?

Paul Roberts - Moderator

Editor-in-Chief and Founder

The Security Ledger

Paul Roberts is the Editor-in-Chief and founder of The Security Ledger (securityledger.com), an independent security news website that explores the intersection of cyber security with business, commerce, politics and everyday life. Roberts has spent the last decade covering hacking, cyber threats and information technology security, including senior positions as a writer, editor and industry analyst. Before founding Security Ledger, he was editor of Threatpost.com and a Security Evangelist for Threatpost's corporate parent, Kaspersky Lab. Prior to that, he spent three years covering the enterprise IT security space as a Senior Analyst in The 451 Group's Enterprise Security Practice. He has held positions as an editor and senior writer for Infoworld.com and Ziff Davis' eWeek.com and was a U.S. Correspondent for IDG News Service on the security beat. He also has worked with a number of companies doing technical writing and has spoken and written extensively on security topics.

Monty Wiseman - Panelist Speaker

Security Architect

Intel Corporation

Monty is a Security Architect for Intel's Data Center Group (DCG). His current projects include architecture for TCG, Intel's TXT(R) Technologies, Boot Guard(R) and other security initiatives. Monty has participated (for chair of) the TCG PC Client working group, Security Evaluation working group and is Intel's representative in the TCG Technical Committee. Monty has 20 years' experience in Desktop, Network and Mainframe environments holding security related and other engineering positions at Novell, Fujitsu, and Control Data. Monty has been developing hardware and software for computers ranging from mainframe to microcomputers since 1975.

Dustin Ingalls - Panelist Speaker

Partner Group Program Manager, Windows Security

Microsoft

Dustin Ingalls is the Group Program Manager for the OS Security team in the Operating Systems Group(OSG). His team has responsibility for security & identity features in Windows, such as PKI, authentication, cryptography, BitLocker, AppLocker, smartcards, biometrics, TPM, secure boot, and others. Dustin has been at Microsoft for 19 years. Prior roles include General Manager of MS IT Global Operations with responsibility for Microsoft's corporate network & data centers worldwide, Product Unit Manager for System Center Configuration Manager, and General Manager of the SoftGrid/App-V product unit.

Gal Shpantzer - Panelist Speaker

Security Consultant and Analyst

SANS

Gal Shpantzer has 13 years of experience as an independent security professional and is a trusted advisor to CSOs of large corporations, technology and pharma startups, Ivy League universities and non-profits/NGOs specializing in critical infrastructure protection. He has been involved in multiple SANS Institute projects, including co-editing the SANS Newsbites, revising the E-Warfare course and presenting SANS@Night talks on cyberstalking, CAPTCHAs and endpoint security. In 2009, he founded and led the privacy subgroup of the NIST Smart Grid cybersecurity task group, resulting in the privacy chapter of NIST IR 7628. He is a co-author of the Managing Mobile Device Security chapter in the 6th ed. Vol 4 of the Information Security Management Handbook (2010) with the late Dr. Eugene Schultz. Shpantzer collaborated with Dr. Christophe Veltsos to present the ongoing Security Outliers project, focusing on the role of culture in risk management at RSA, CSI, BSides and Baythreat conferences. Most recently, he was involved as a subject matter expert in the development of the U.S. Department of Energy’s Electric Sector Cybersecurity Capability Maturity Model (ESC2M2) in 2012. He is currently involved in the Infosec Burnout research project and co-presented on this topic at BSides-Las Vegas (2011) and RSA (2012), and leads the PACS-WG for EnergySec.

Mobile Device Security: Fact or Fiction

Victor Wheatman - Moderator

Global Information Security Market Analyst and Enterprise Advisor

Victor (Vic) Wheatman is an Independent Global Information Security Market Analyst and Enterprise Advisor. Prior to becoming independent, he was a Managing Vice President at Gartner Research for the Security and Privacy team where he worked for over twenty years. Wheatman also chaired and programmed Gartner's worldwide security conferences. Earlier, Wheatman was vice president in Gartner's Electronic Commerce/Electronic Business research area. He served as President of the northern California EDI/EC Users Group for seven years. Prior to joining Gartner, Wheatman was a program manager at Input, a market research firm, specializing in electronic data interchange. Earlier in his career, he worked as a public radio producer and station manager. He created the award-winning National Public Radio program "Car Talk."

Rick Doten - Panelist Speaker

Chief Information Security Officer
DMI, Inc.

Rick has over 24 years of experience in the IT industry, the last 17 focused on cyber security Before DMI, Rick was a Risk Management Consultant at Gartner. He was Chief Scientist at the Lockheed Martin Center for Cyber Security Innovation (CCSI). Rick was Managing Principal for Verizon Business's East Coast Professional Security Services practice. Through most of his career, Rick ran penetration testing, forensics and incident response teams, and risk management professionals across all industries and the US federal government. Rick has been quoted in dozens of security articles such as Dark Reading, SC Magazine, Infosecurity Professional magazine, Kreb's on Security, and Mashable, on the topics of cyber security and mobile security. Rick has appeared on CNN, TechTV, and the National Insider as a cyber security expert. Rick is on the Intel Corp. Enterprise Board of Advisors, and the Council on Cyber Security Critical Security Controls Editorial Panel. Rick also holds a Patent for Wireless Intrusion Detection technology.

Jason Conyard - Panelist Speaker

Vice President, IT, End User Services
Juniper Networks

As Vice President of Information Technology, Jason Conyard is responsible for delivering Infrastructure, desktop, mobile, and collaboration solutions to ~9600 Juniper employees globally. With 20+ years of experience directing global IT strategy & operations, Conyard previously held senior management roles at Barclays Global Investors, Global Communications Partners and Symantec.

Eric Green - Panelist Speaker

SVP, Business Development and Program Director

Mobile Active Defense and SC World Congress

Eric is both SVP of Business Development and board member at Mobile Active Defense who have an industry leading smartphone security product.

In that role he's been consulting as a subject matter expert (SME) with primarily the FORTUNE 500 and Federal Agencies on the subject of mobile security and management. This includes serving as an SME for both the NSA's National Information Assurance Partnership (NIAP) in developing the requirements for the mobile device management protection profile used to create a Common Criteria for mobile device management as well as for CompTIA in the creation of a mobile security management certification.

Outside of that role, he has been involved in the security industry for over a decade. Past experience also includes running a technology book division publishing 12 books with a wide variety of industry luminaries, primarily in security.

Eric is also program director for SC Magazines SC Congress events and for the last 6 years have also produced, hosted and syndicated the SecureIT Live podcast show, available online at www.secureitlive.com.

GET INVOLVED

Trusted Computing Group Mission

The Trusted Computing Group (TCG) is a not-for-profit organization that defines, develops and promotes open, vendor-neutral, global industry standards that are supportive of a hardware-based root of trust. Since its formation in 2003, the organization has been leading the industry with open standards that drive the creation of customizable security solutions for mobile, PC client, server, storage and network applications.

Why Join Trusted Computing Group?

Membership in the Trusted Computing Group (TCG) allows you to participate in the development and promotion of vendor-neutral technical standards that drive trusted computing technologies.

Network and collaborate with industry experts, contribute to technical specifications through various technology Work Groups, and influence both developers and enterprise end-users of trusted computing technology, all in a neutral environment that fosters the creation and adoption of open, interoperable standards.

Learn more at http://www.trustedcomputinggroup.org/join_now

Contact Information:

Trusted Computing Group Administration
3855 SW 153rd Drive
Beaverton, Oregon 97006 USA
Phone: +1.503.619.0562
Email: admin@trustedcomputinggroup.org
Web: www.trustedcomputinggroup.org

Notes:

Notes:

TRUSTED
COMPUTING GROUP™

www.trustedcomputinggroup.org/resources/rsa_conference_2014_get_proactive_with_security