Should We Trust Mobile Computing, IoT and the Cloud?

No, But There Are Solutions

Guide to TCG Seminar and Demonstration Showcase

RSA® CONFERENCE 2015

TRUSTED COMPUTING GROUP®

Seminar Schedule

9:00 – 9:20 WELCOME & INTRODUCTION TO TRUSTED COMPUTING GROUP®

	JOERG BORCHERT	*TCG President & Chairman*

9:20 – 9:45 20-STORY SNOW CASTLE:
Why We Need a New Foundation for the Internet of Things

	PAUL ROBERTS	*Founder & Editor in Chief, Security Ledger*

9:45 – 10:45 SECURITY AND THE ROOT OF TRUST:
Leveraging the Root of Trust and TPM in the Enterprise

MODERATOR:	**PAUL ROBERTS**	*Security Ledger*
PANELISTS:	**AMY NELSON**	*Engineering Technologist, Security Software Technical Planner, Dell*
	DAVID BOSSIO	*Group Program Manager, OSG Enterprise & Security R&D, Microsoft*

11:00 – 12:00 THE INSECURE INTERNET OF THINGS AND HOW TO SECURE IT

MODERATOR:	**RICH NASS**	*Executive Vice-President, Embedded-Computing.com, OpenSystems Media*
PANELISTS:	**STACY CANNADY**	*Engineer Technical Marketing Security & Trust Organization, Cisco Systems*
	DARIN ANDERSEN	*Founder, CyberUnited*
	CHUCK BENSON	*Assistant Director of IT, Facilities Service, University of Washington*

12:00 – 13:00 MOBILE IS KING, BUT SECURITY MUST BE A PRIORITY

MODERATOR:	**JAI VIJAYAN**	*Technology Editor/Writer*
PANELISTS:	**GIL BERNABEU**	*Technical Director, GlobalPlatform*
	LEE NEELY	*Senior Cyber Analyst, Lawrence Livermore National Laboratory (LLNL)*
	JON GEATER	*Chief Technology Officer, Trustonic*

13:00 CLOSING REMARKS/END OF SESSION LIVE RAFFLE DRAWING

RAFFLE DRAWING PRODUCTS DONATED BY:
INFINEON TECHNOLOGIES
SAMSUNG ELECTRONICS

WELCOME & INTRODUCTION TO TRUSTED COMPUTING GROUP®

DR. JOERG BORCHERT
President and Chairman
Trusted Computing Group
Vice President, Chip Card & Security ICs
Infineon Technologies North America Corporation

SECURITY AND THE ROOT OF TRUST:

Leveraging the Root of Trust and TPM in the Enterprise

PAUL ROBERTS, Moderator
Editor In Chief & Founder
The Security Ledger

AMY NELSON, Panelist
Engineering Technologist,
Security Software Technical Planner
Dell

DAVID BOSSIO, Panelist
Group Program Manager,
OSG Enterprise & Security R&D
Microsoft

THE INSECURE INTERNET OF THINGS AND HOW TO SECURE IT

RICH NASS, Moderator
Executive Vice-President,
Embedded-Computing.com
OpenSystems Media

STACY CANNADY, Panelist
Engineer Technical Marketing
Security & Trust Organization
Cisco Systems

DARIN ANDERSEN, Panelist
Founder
CyberUnited

CHUCK BENSON, Panelist
Assistant Director of IT,
Facilities Service
University of Washington

MOBILE IS KING, BUT SECURITY MUST BE A PRIORITY

JAI VIJAYAN, Moderator
Technology Editor/Writer

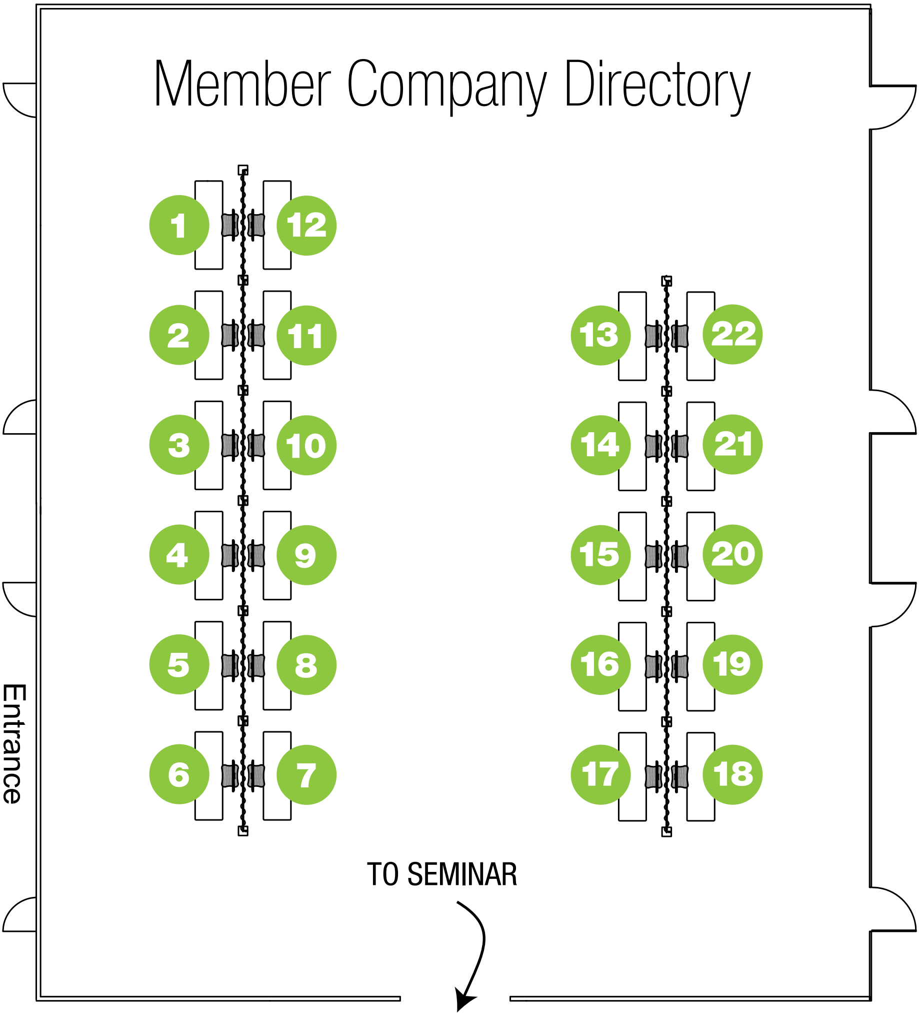
GIL BERNABEU, Panelist
Technical Director
GlobalPlatform

LEE NEELY, Panelist
Senior Cyber Analyst
Lawrence Livermore National Laboratory (LLNL)

JON GEATER, Panelist
Chief Technology Officer
Trustonic

Demonstration Showcase

Member Company Directory



1. **Swisscom | Intel**
2. **Fujitsu Limited**
3. **Microsoft**
4. **Tempered Networks | Pulse Secure**
5. **Intel**
6. **Cisco | HSR | Infineon | Intel**
7. **Intel**
8. **Dell**
9. **Huwaei**
10. **Wave**
11. **Wave | Samsung**
12. **Decoit | Univ. of Applied Sci., Hanover**
13. **Fraunhofer SIT**
14. **Pulse Secure | Rebasoft**
15. **Decoit | HsH | Pulse Secure**
16. **JWSecure**
17. **Intel**
18. **Integrity Security Services**
19. **WinMagic | Micron Technology Inc.**
20. **Artec IT**
21. **CoSoSys**
22. **Absolute Software | Seagate**

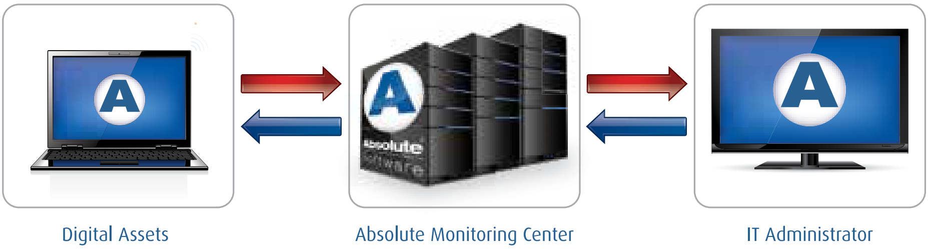
Absolute® Software

Seagate®

ENDPOINT COMPLIANCE WITH SELF-ENCRYPTING DRIVES (SEDs)

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

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



VISIT OUR DEMO #22

ARTEC® IT Solutions

SECURE YOUR DATA WITH TPM

Trusted Computing Technologies to Secure Your Data

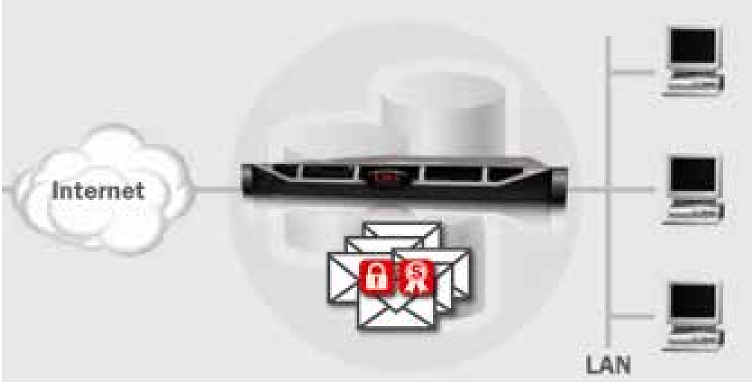
TPM IN COMBINATION WITH INFORMATION MANAGEMENT

Almost all applications used by organizations generate a large amount of data and information every day. Users in the network, partner communication, customers, and leads also serve as sources that constantly create new information that must somehow be coped with. But how to secure those Information and data sources?

Conventional systems and security mechanisms reveal a decisive weak-ness when examined closer: they are potentially open to attacks when third parties can gain direct access to the hardware. Trusted EMA® prevents such attacks by creating links to hardware characteristics that are unique to each device. This protects the appliance from unauthorized manipulation and constructs an unbreakable »safe« for your organization's archived data.

Trusted EMA® is based around a TPM chip (Trusted Platform Module), firmly anchored inside all EMA® appliances, which provides a smart extension to our existing secu-rity concept. Using the TPM chip and the groundbreaking Trusted EMA® feature, the appliance-specific data decryption key re-ceives even better protection against mali-cious hardware attacks. EMA® hardware and appliance software now truly combine and form an inseparable unit.

In short, we managed to make one of the most secure solution even more secure. Our latest innovation, called Trusted EMA®, takes the advanced security measures one step further. EMA® is now the world's first archiving appliance that is built according to the Trusted Computing standard (TC).



#20 VISIT OUR DEMO

cisco

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

infineon

intel

SECURING IoT WITH TRUSTED COMPUTING

Trusted Computing Technologies Supported: TPM and TNC

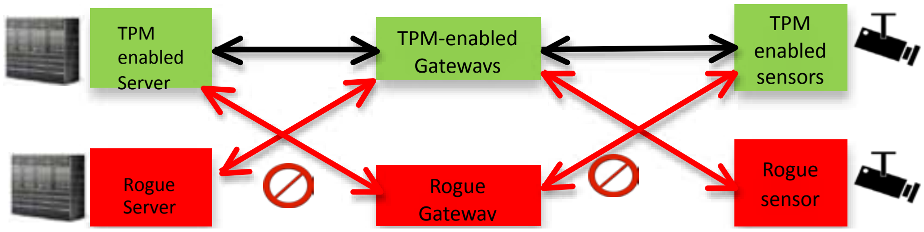
The Use Case for this demonstration is a deployment of IoT sensors and actuators (such as those found in a Smart Building) managed by a Cloud-based application that is remote to the sensors (such as the Building Management application). The server and the IoT devices are connected over the public Internet, using an OpenSSL connection. Mutual authentication of devices is required at session start.

TCG technology (TPMs to protect credentials and TNC to validate credentials) is applied to the use case by extending OpenSSL authentication. Instead of single factor, using certificates only, the enhanced Open SSL authentication process requires a certificate and an integrity report (both protected by a TPM on each device). Servers and gateways perform local validation of the integrity reports. If both credentials are validated, an OpenSSL session for data exchange is started. IoT devices validate the SSL certificate from the gateway in conventional, single factor OpenSSL authentication.

Several security threats are addressed by these protections. Fake servers, gateways, and sensors are detected and blocked by always performing mutual authentication. Infected components are similarly detected and blocked by checking integrity reports. Rooting these checks in a TPM prevents malware from stealing credentials or falsifying an integrity report. The security of the IoT system is grounded in hardware, ensuring uptime and maximizing reliability.

The demo includes an extensive GUI showing activity logs, credentials provided at session start and other logged information relevant to session start and device status.

OpenSSL and the TNC code are all Open Source. The IoT devices and gateways may be from a mix of vendors demonstrating the open nature of the protocols.



#6 VISIT OUR DEMO

ENDPOINT PROTECTOR | by CoSoSys

QUITTING THE GAMBLE OF TRUSTING INSIDERS WITH CORPORATE DATA

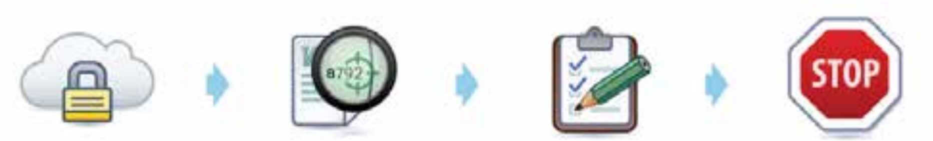
CoSoSys will showcase Endpoint Protector 4, a cross-platform Data Loss Prevention (DLP) and Mobile Device Management (MDM) solution as a tool to address insiders' threats and human error and prevent data loss, data theft and data leakage. The demonstration will be based on most common use cases and best practices to control transfers of confidential data in enterprises.

During the demo, there will be emphasis on DLP for Mac OS X, as a tool to support enterprises which integrate Macs into their networks and need data protection as much as Windows computers do.

Human error is tackled during by Endpoint Protector 4 by controlling access to removable devices and filtering the information that users are not allowed to transfer outside of the network. At the same time, a more profound level of security is shown with Content Aware Protection which scans documents being sent through online applications like Dropbox and decides whether to block the transfer or not.

MDM will be also demonstrated, as a part of Endpoint Protector 4, with innovative features like Geofencing – location-based policies.

Endpoint Protector 4 combines DLP and MDM within the same administration console in a user-friendly and intelligent way in order to protect information on all working stations, regardless if they are computers, smartphones or tablets. The DLP features work at the content level and not the data traffic level, offering to IT administrators highly flexible policies.



User attempts to upload a file to a cloud service

Content is inspected before upload to the cloud

If sensitive content is detected, violating a policy, the incident is reported and/or blocked

Data transfer is stopped to protect company information and logged for later auditing

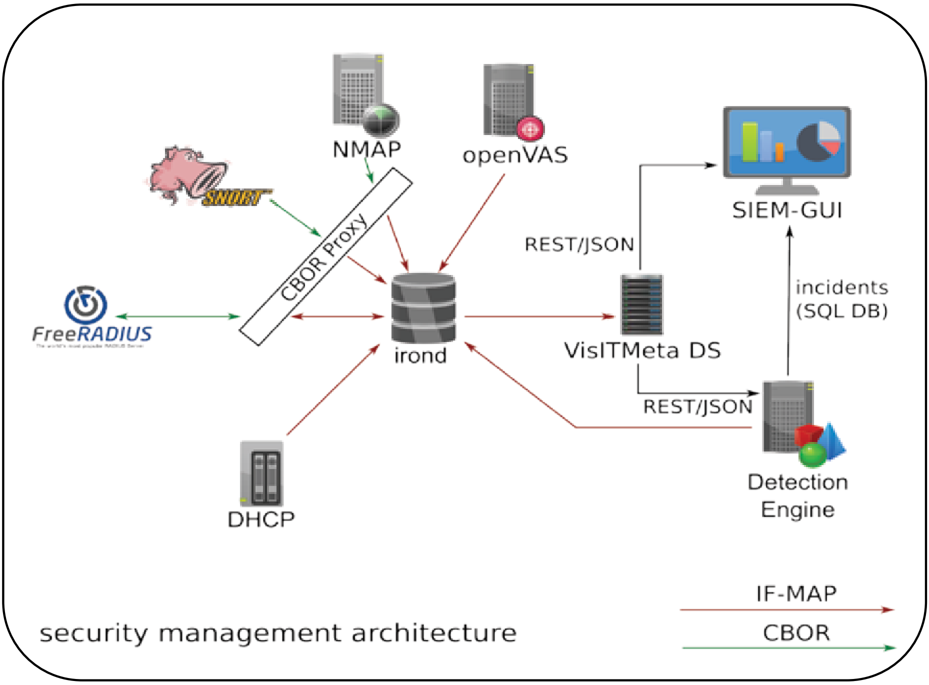
VISIT OUR DEMO #21

NEAR REAL-TIME NETWORK SECURITY WITH AN IF-MAP-BASED SIEM APPROACH

Trusted Computing Technologies Supported: Interface for Metadata Access Points (IF-MAP)

This demonstration intends to illustrate how IF-MAP open source tools of multiple vendors can be combined to smartly address the complex scenario of detecting and reacting to unwanted behavior involving the information of multiple sources. The example scenario integrates several components and IF-MAP-clients developed by DECOIT GmbH, a SME from Bremen (Germany), and the Trust@HsH research group from the University of Applied Sciences and Arts in Hanover (Germany).

The combination of these tools allows to identify threats in a detailed manner as well as a near real-time response to found incidents. The scenario is set in a medium-sized network, where an authenticated user is behaving in a malicious manner, while the different components monitor, evaluate and visualize the network state.



#12 VISIT OUR DEMO

DELL DATA PROTECTION I HOST CRYPTO ACCELERATOR (HCA) AND TPM INTEGRATION

Dell Data Protection I Host Crypto Accelerator (HCA) is a hardware option to provide FIPS 140-2 Level 3 certified encryption for internal storage mediums. DDP I HCA works with Dell's Data Protection Encryption Software and utilizes the TPM for protection of encryption keys such that they never transition through system memory in the clear.

DDP I HCA is a hardware-based, cryptographic engine maintaining an advanced level of tamper resistant security. It provides support for National Security Agency Suite B encryption and signing algorithms and is available exclusively on select Dell commercial devices as a hardware expansion card.

Dell Data Protection I Hardware Crypto Accelerator:

- Delivers enterprise class pre-boot authentication for enterprise deployment
- Drive agnostic hardware encryption with performance similar to an SED
- Offers the highest level of Federal Information Processing Standards (FIPS) certification (FIPS 140-2 Level 3) commercially available for a system disk encryption solution
- Provides superior encryption key protection in hardware with automatic key deletion in case of an attack

VISIT OUR DEMO # 8

Fraunhofer SIT

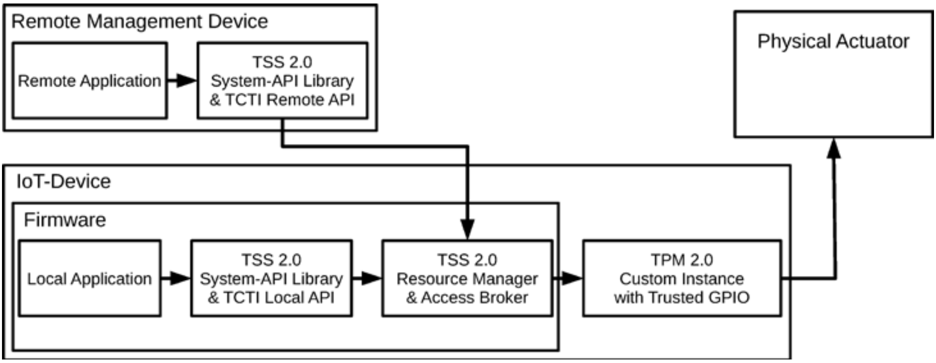
ESTABLISHING TRUST WITH EMBEDDED ACTUATORS IN THE IoT

Trusted Computing Technologies Supported: Trusted Platform Module (TPM) Library Specification 2.0, TPM Software Stack (TSS) 2.0

With the emergence of the Internet of Things (IoT) an increasing number of so-called smart objects are being deployed. These include cyber-physical systems that perform physical actions or collect sensitive data with potentially high security impact. Application range from motion sensors over door locks to industrial applications in smart factories, railway systems or the SmartGrid.

The Trusted Platform Module (TPM) 2.0 with an accompanying TPM Software Stack (TSS) 2.0 provides an effective way to determine the firmware and software state of such devices and detect manipulations. However, it can only detect but not protect the access to the sensor or actuator attached to such an embedded device.

This demonstrator highlights a custom TPM 2.0 module, extended with trustworthy GPIO capabilities in order to secure access to the attached actuator even in the case of firmware manipulations and to ensure remote management of this actuator even during an active attack. It utilizes a prototype of a TPM 2.0 implementation on a discreet chip and a prototype implementation of a TSS 2.0 locally as well as remotely.


Remote Management Device
Remote Application
TSS 2.0 System-API Library & TCTI Remote API
Physical Actuator
IoT-Device
Firmware
Local Application
TSS 2.0 System-API Library & TCTI Local API
TSS 2.0 Resource Manager & Access Broker
TPM 2.0 Custom Instance with Trusted GPIO

#13 VISIT OUR DEMO

REMOTE FIRMWARE UPDATE FOR VEHICLE ECU WITH A TPM

Demonstrate application of TCG Technology for Automotive area.

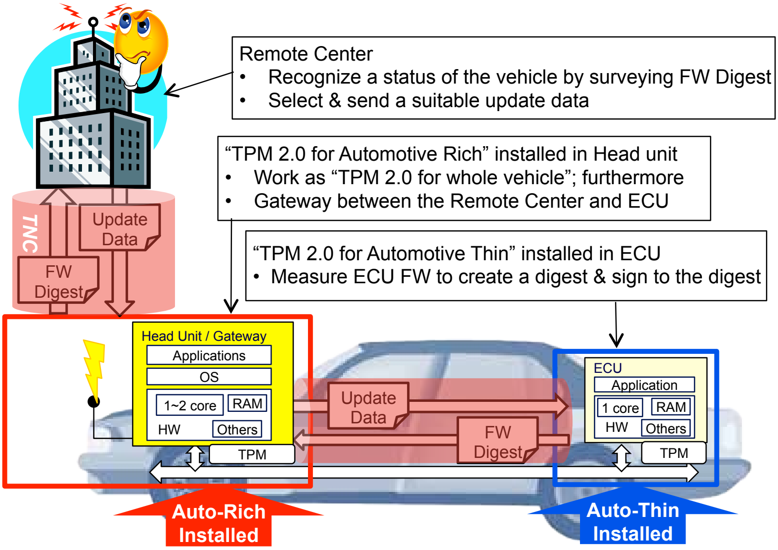
It shows remote firmware update demo for ECU in a car with integrity by TPM.

The secure update is implemented using the following three steps:

- Accurate remote determination of in-vehicle software and hardware configuration and integrity
- Verification of successsful completion of intended software updates
- Secure long-term storage of audit logs of the related updated operations and TPM measurement operations

This figure shows the concept of message flow for each component (Head Unit/Gateway or ECU) for remote maintenance. This is one of the figures which are contained in TPM 2.0 Automotive-Thin Profile v1.0 published by TCG.

http://www.trustedcomputinggroup.org/resources/tcg_tpm_20_library_profile_for_automotivethin



Remote Center

- Recognize a status of the vehicle by surveying FW Digest
- Select & send a suitable update data

"TPM 2.0 for Automotive Rich" installed in Head unit

- Work as "TPM 2.0 for whole vehicle"; furthermore
- Gateway between the Remote Center and ECU

"TPM 2.0 for Automotive Thin" installed in ECU

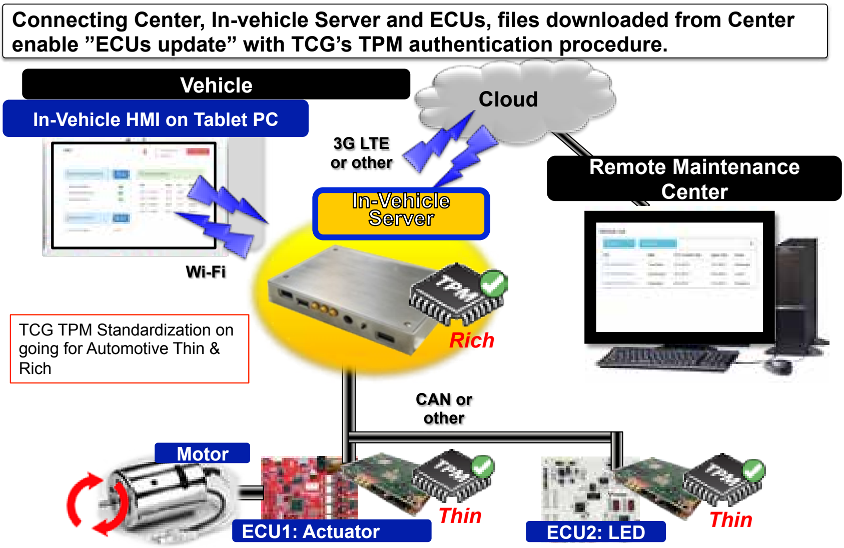
- Measure ECU FW to create a digest & sign to the digest

VISIT OUR DEMO # 2

Based on this concept, the demo system includes:

- A notebook computer representing the remote maintenance center
- Representation of a vehicle that requires remote update of firmware
- Several connected communications modules

The figure below shows the demo system diagram. The demo flow/procedure follows the three steps described above.


Connecting Center, In-vehicle Server and ECUs, files downloaded from Center enable ”ECUs update” with TCG’s TPM authentication procedure.
Vehicle
In-Vehicle HMI on Tablet PC
Cloud
3G LTE or other
Remote Maintenance Center
In-Vehicle Server
Wi-Fi
TPM
Rich
TCG TPM Standardization on going for Automotive Thin & Rich
CAN or other
Motor
ECU1: Actuator
Thin
ECU2: LED
Thin

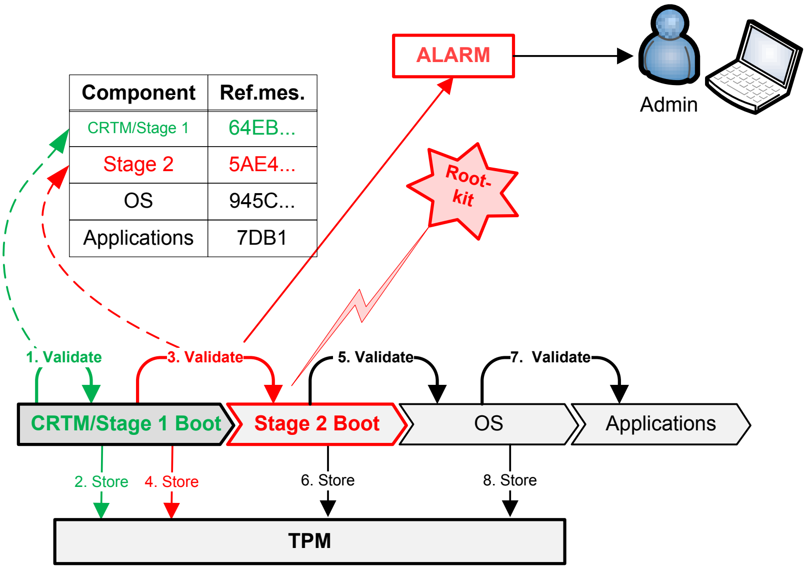
# 2 VISIT OUR DEMO

TRUSTED COMPUTING IN NETWORK DEVICE

Telecommunication operators have expressed serious concerns regarding the exposure of their infrastructure to the threat of equipment tampering and unauthorized data exfiltration. Network device vendors can support operators in their efforts to defend against such threats with solutions adapted to their particular requirements.

Huawei demonstrates how to use the Trusted Platform Module (TPM) and the measured boot process on telecom devices and successfully implement firmware and software tampering detection.

The demonstration will showcase an enhanced measured boot process, in which each boot component is not only measured, but also validated against reference measurements. The validation is performed locally, without requiring additional infrastructure.



Component	Ref.mes.
CRTM/Stage 1	64EB...
Stage 2	5AE4...
OS	945C...
Applications	7DB1

VISIT OUR DEMO #9

INTEL SECURITY CRITICAL INFRASTRUCTURE PROTECTION (CIP) – FOR MANAGED IoT SECURITY

The Intel Security CIP (IS-CIP) demonstration leverages an innovative defense-in-depth approach to monitor and manage IoT deployments from silicon to cloud. The IS-CIP solution is a virtualized security-architected platform optimized on Intel Architectures that manages HW, SW, and data security capability separately from operational applications hosted in secured unmodified guest OS partitions. This separation of concerns between operational applications and platform monitoring and management capabilities enables IS-CIP to host and protect new and legacy software with little or no changes to these operational applications, thereby enabling rapid advancement of security awareness and controls to new and existing infrastructure.

IS-CIP provides controls to harden the device, secure the communications between devices, and to manage and monitor connected devices in a policy-driven and closed-loop remediation environment. The IS-CIP software stack implements cyber security controls, physical security controls, and a hardware-based embedded identity. Each device is securely measured and validated during the boot process and during software execution to ensure the integrity of the hardware, firmware, and software. The communications security leverages the embedded identity to enable mutual authentication between devices and to authenticate traffic streams. In addition, the confidentiality and integrity of the communications can be remotely configured and managed on a stream-by-stream basis. Finally, all devices have a consistent security management and monitoring capability which decouples the security processes and policies from the physical device and OS characteristics.

In IoT deployments, management and monitoring of devices and data are critical. The IS-CIP demonstration will show how to monitor security status and event data in near real-time with automated, policy-driven management capabilities that enable orchestration of responses to security anomalies. This allows for an automated reactive security response based on the nature of the attacks on the device, creating a dynamic security response that inhibits the script-based attacks that depend on a known environment. In addition, by altering the policy, proactive security orchestration is enabled such that devices not yet under attack can begin to mitigate against a particular threat, thereby inhibiting the ability of threats to propagate within the environment after compromise.

The IS-CIP platform demonstrates how to protect new and existing (greenfield and brownfield) operational software deployments, including consolidation or redundant/backup deployment strategies for control systems and other critical infrastructure applications, with a comprehensive intelligent managed protection strategy.

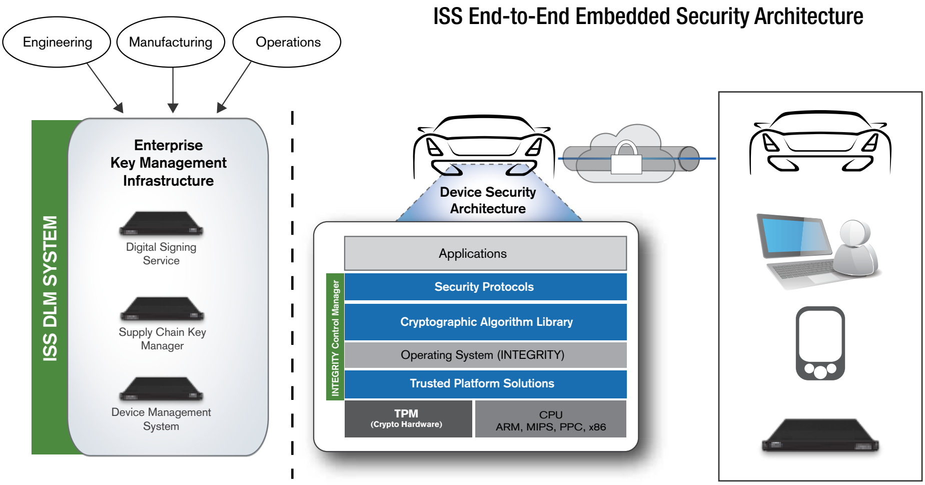
#5 VISIT OUR DEMO

INTEGRITY™
SECURITY SERVICES

TRUSTED DEVICE LIFECYCLE MANAGEMENT FOR END-TO-END SECURITY

While the Trusted Platform Module is the foundation of an IoT device's security architecture, the benefit of enhanced key protection is only realized through an Enterprise Key Management Infrastructure to securely produce the proper keys, certificates, and digital signatures required for trusted computing.

The Device Lifecycle Management (DLM) System provides IoT system developers with a PKI certificate authority, digital signing service, and supply chain key management solution, scalable across a variety of distributed manufacturing environments. DLM is available today and currently deployed in a variety of applications including semiconductor high-speed key injection, protection of intellectual property in industrial controllers, and automotive security credential management systems.



ISS End-to-End Embedded Security Architecture

VISIT OUR DEMO #18

INTEGRITY™ SECURITY SERVICES

INTEGRITY Security Services (ISS) will demonstrate the automated enrollment of a TPM within a typical embedded IoT device using the DLM System to generate and sign Attestation Identity Key (AIK) certificates. AIKs are used to authenticate devices and securely inject trust anchors into the TPM. The resulting device is able to authenticate all software, identities, and data, used in the design of value-added features including:

- Remote Software Updates
- Protection of Intellectual Property
- License Management & Content Protection
- Feature Control (“In-app purchases”)

INTEGRITY Security Services is a proud member of the Trusted Computing Group. To learn more about DLM and integration of TCG technology in end-to-end embedded security solutions, please visit us in the Green Hills Software booth (South Expo #S1933).

#18 VISIT OUR DEMO

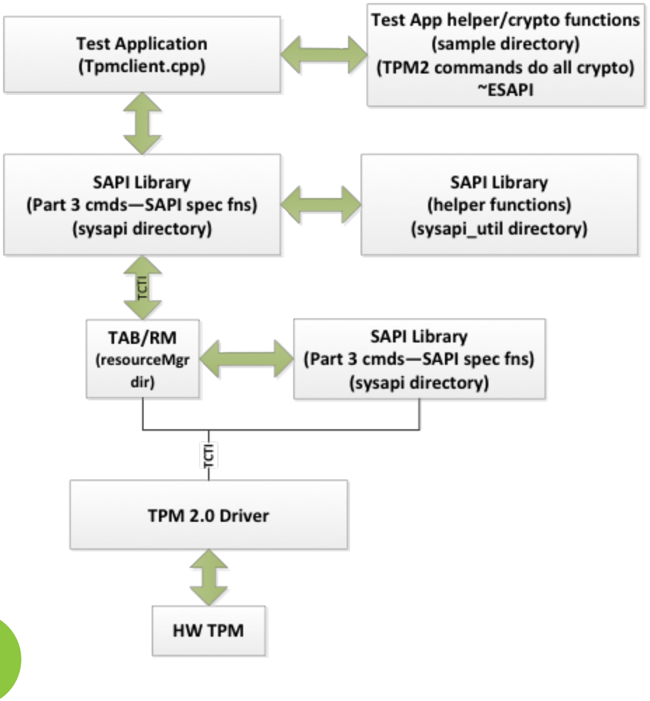
TPM 2.0 FAMILY ENABLING FOR LINUX

TPM 2.0, TSS System API, TSS Trusted Access Broker/Resource Manager, Linux Device Driver

FULL LINUX STACK FOR TPM 2.0

TPM 2.0 enables security in a wide range of deviced from embedded/IOT, to PCs and servers. Giving these applications access to TPM 2.0's full set of feature requires a software stack. We are demonstrating a TPM 2.0 software stack consisting of:

- A test application that exercises TPM 2.0 commands
- TSS System API code for sending and receiving the TPM 2.0 commands
- A TSS TAB/RM (TPM access broker/resource manager) for coordinating multi-process access to the TPM and for managing the TPM's resources
- A Linux device driver for sending and receiving the raw byte streams to the TPM and provides the system resources as was done for TPM 1.2



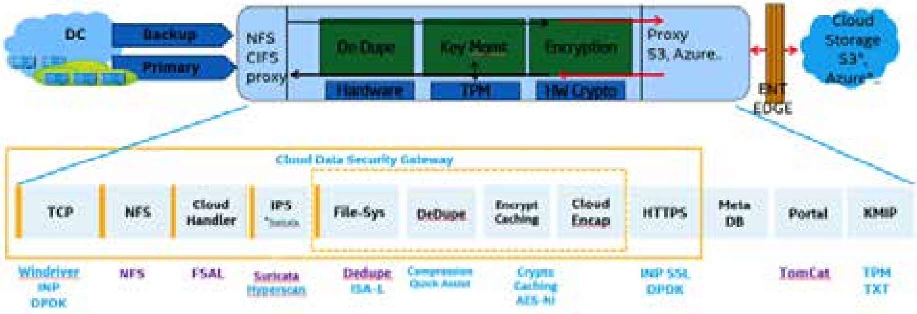
VISIT OUR DEMO #17

CLOUD DATA SECURITY GATEWAY

As enterprises increasingly move application workloads and data into external clouds – one of the biggest concerns is security and how do I securely transfer my app/data to the cloud, how do I gain visibility into my app/ data and the infrastructure on which they run, how do I ensure that only I can access my app/ data and only I have the keys to encrypt / decrypt my data, thus protecting privacy of data owners.

Cloud Data Security Gateway Appliance (CDSA) enables enterprise users to route application/backup data from the enterprise network to public/private cloud based storage services (like Amazon S3, Google Cloud, Microsoft Azure, Openstack Swift etc.) in a secure way and with optimized latency. CDSA achieves this performance by leveraging Intel Architecture based accelerators like Intel QuickAssist, ISA-L, AES-NI, and DPDK in addition to performance enhanced data handling. Appliance and data integrity is protected by TxT/TPM enabled trust.

Openstack Cinder volumes store critical enterprise data which needs to be standards compliant. So, boundary control plays a very important role for Cinder based storage. The demonstration also focuses on boundary control of Cinder Volumes with the help of TPM/TxT assisted geo/asset tags.



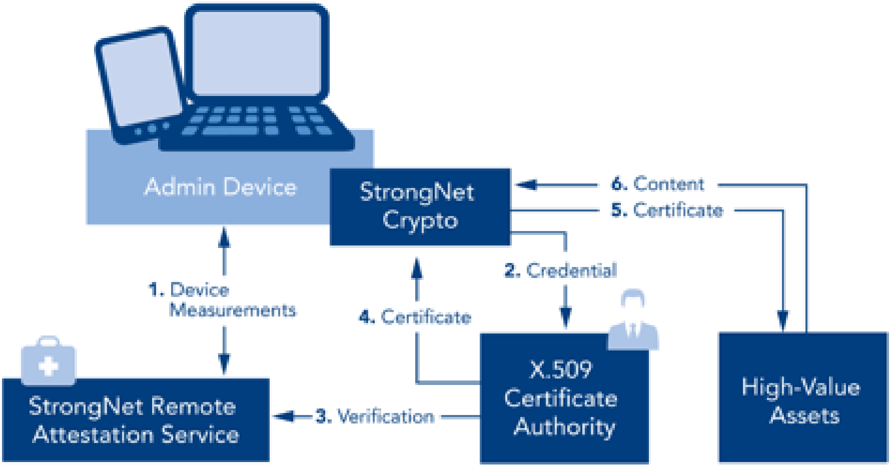
#7 VISIT OUR DEMO

JW SECURE STRONGNET™ SECURE ADMIN

Trusted Computing Technologies Supported: Remote Platform Attestation and Trusted Platform Module (TPM)

As a result of growing Bring Your Own Device (BYOD) and cloud computing trends, enterprise connectivity continues expanding exponentially. Not only that, but the DevOps movement has increased the number of accounts with system administrator access to servers and data. Together, the rising sophistication of Internet attacks and the potential for insider threats have seriously endangered enterprise data security.

The best way to administer your IT infrastructure is from locked-down, hardened workstations that enforce encryption, device-to-user association, and strong authentication. StrongNet with Measurement Bound Keys is designed to protect system administrator workstations and other devices by enforcing both user identity and device integrity, so every network resource that supports public key cryptography or public key infrastructure (PKI) can be protected. StrongNet uses hardware root of trust to deliver high-integrity user and computer credentials, and our proprietary Measurement Bound Keys can ensure that credentials will not be accepted unless the mobile device complies with security policies.



VISIT OUR DEMO #16

Microsoft

MICROSOFT WINDOWS INTERNET OF THINGS — TRUSTED I/O

#3 VISIT OUR DEMO

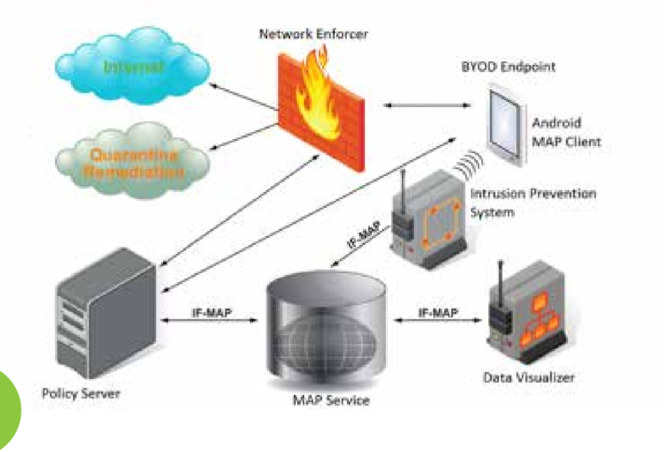
BYOD SOLUTIONS WELL IN HAND:

Standards-Based Mobile Security

BYOD security is a hot topic for the enterprise - end users want to work from their shiny new smartphones and tablets, and corporations desire the productivity gains and cost reductions associated with permitting them. But with greater flexibility comes increasing threat - mobile devices are at a higher risk of compromise than traditional desktop operating systems due to limited security software and exposure to web-based malware and malicious mobile applications. How do we ensure that these devices play well with others once we allow them on our networks?

TNC IF-MAP based interoperability for security automation enables a mobile security solution in which:

- A Pulse Secure Policy Secure policy server (TNC MAP Client) authorizes a BYOD device to connect to the network.
- A DECOmap Android client from DECOIT GmbH (TNC MAP Client) gathers data from the device and publishes it to the MAP service.
- A Snort intrusion prevention system, with TNC MAP Client functionality developed by DECOIT GmbH, monitors behavioral activity on the network.
- IF-MAP based security automation - coordinated by Trust@HsH's irond TNC MAP Server - enables the Snort IPS to signal the Pulse Secure policy server if the mobile device is out of compliance or misbehaving, so the policy server can isolate or restrict the mobile device.
- A Trust@HsH VisITMeta data visualizer (TNC MAP Client) enables a security administrator to investigate activity, and communications partners, of the offending mobile device.



VISIT OUR DEMO #15

Pulse Secure

Rebasoft
Revealing your network

BREACH CONTAINMENT:

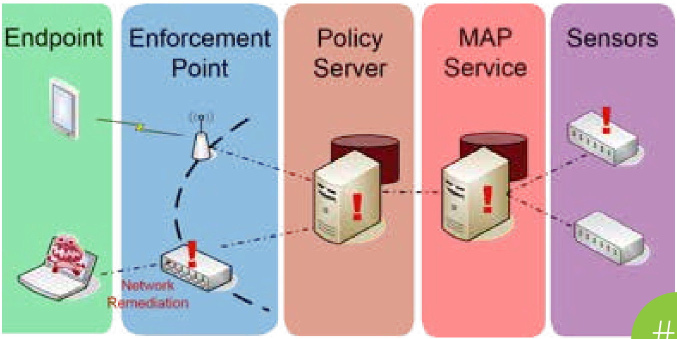
Standards-Based Security Automation for Coordinated Threat Control

As we learned from the JP Morgan breach, it only takes one compromised system to expose an entire protected network. The 2013 and 2014 Verizon Data Breach Incident Reports illustrate this problem: in 2012, 71% of attacks and breaches involved compromised end-user devices; in 2013, attacks on servers nearly doubled compared to the previous year. Identifying and isolating systems attempting unauthorized access is a critical enterprise-security defense mechanism.

Combining access control with threat protection technology reduces risks and costs associated with sophisticated attacks. Pulse Secure's Policy Secure provides a mobility-ready NAC and BYOD solution that protects enterprises with seamless enforcement of security policies for all users, devices, and applications accessing the network. The Rebasoft Threat Auditor is a flexible system that takes information from a wide variety of systems and makes decisions based upon what it finds, enabling organisations to link multiple systems together to improve post-admission security. Together, they leverage TCG standards to provide intelligent, dynamic detection and remediation of compromised internal systems.

TNC IF-MAP based interoperability for security automation enables a Coordinated Threat Control scenario in which:

- A Pulse Policy Secure policy server (TNC PDP & IF-MAP Client) authorizes an authenticated, compliant system to connect to the network.
- A Rebasoft Threat Auditor (TNC IF-MAP Sensor) detects unauthorized behavior from that system.
- IF-MAP based security automation - provided by the Pulse Secure MAP service - enables the Rebasoft sensor to signal to Pulse Policy Secure that the system is misbehaving.
- Pulse Policy Secure isolates the misbehaving system.



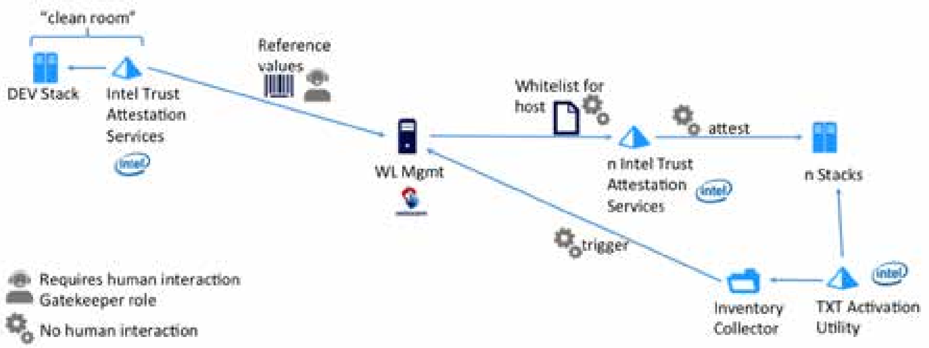
#14 VISIT OUR DEMO

USING TCG TECHNOLOGIES IN A REAL WORLD CLOUD SETUP

Security becomes a more and more important topic for everyone. Especially in the area of cloud computing, customers do request more privacy and security.

Up until now, infrastructure security was based on thick doors and locks in front of data centers. That changes with trusted computing technologies like Secure Boot and Remote Attestation. Those are a change of paradigm in the area of infrastructure security. In a close collaboration with Intel, Swisscom wants to use those technologies in its cloud.

The demo will show the general architecture based on Intel's Trusted Execution Technology (Intel® TXT). It will cover the provisioning of the infrastructure as well as the attestation of machines. You will also have the opportunity to discuss our learnings and challenges that we faced while implementing those trusted computing technologies in a real world environment.



VISIT OUR DEMO #1

TEMPERED NETWORKS

Pulse Secure

DYNAMIC OVERLAY PROTECTION FOR INDUSTRIAL CONTROL SYSTEMS

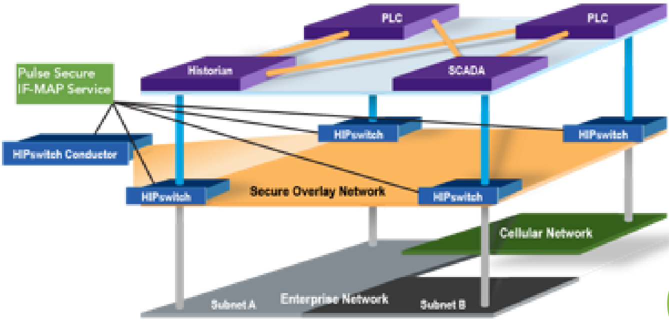
The adoption of M2M connectivity and communications over the Internet using IP-based networks is on the rise, but security has been an afterthought. The exponential growth of Internet-connected devices and systems–from water treatment plants to railway controls; energy plants to building control systems–have created more opportunities for bad actors to gain access to networks and sensitive information. The increased attack surface created by these critical assets leaves an organization exposed and vulnerable to cyber security threats.

The Tempered Networks solution allows organizations to create private overlay networks at unlimited scale--on top of shared network infrastructure--providing network segmentation. A Tempered Networks environment is comprised of a scalable orchestration engine (HIPswitch Conductor™), industrial and data-center grade security appliances (HIPswitches), and a management console and user interface (SimpleConnect™). HIPswitches are used to implement multiple private overlay networks, which can be individually orchestrated by the HIPswitch Conductor and managed by the SimpleConnect web-based user interface. Pulse Secure's Policy Secure server implements the MAP service, which provides dynamic, centralized coordination for HIPswitch MAP Clients.

TCG Technology Supports Critical Infrastructure Protection

Two TNC standards underlie 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.



#4 VISIT OUR DEMO

wave®

WAVE VIRTUAL SMART CARD 2.0:

Two-Factor Authentication with TPM

Wave Virtual Smart Card 2.0 provides strong two-factor user authentication, offering better security at less than half the cost of USB security tokens or physical smart cards. It can be used like a traditional smart card or token – but because it uses hardware already embedded in the endpoint, the user doesn't have to carry anything extra for secure authentication.

Typical use cases are for device login, secure VPN, web applications, cloud applications and other certificate-based applications, like wireless authentication (802.1x), remote desktop, or user login to a Windows tablet or laptop.

Additional Information:

END-USER BENEFITS

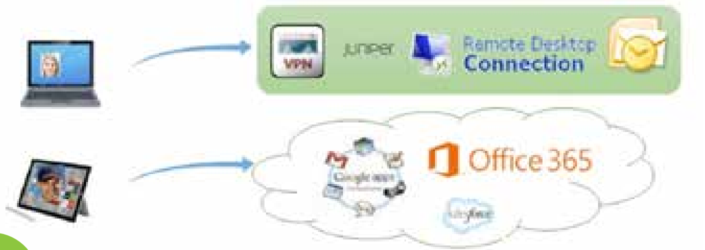
Better Security: Uses the industry-standard hardware Trusted Platform Module (TPM), so built to vendor-neutral, internationally-developed security standards. The keys are unique to each endpoint, i.e. it is not vulnerable to a centralized server hack.

Instantly mitigates the threat from compromised user credentials: By applying a strong, hardware-based second factor to the authentication process, it negates the huge risk posed by the compromise of user credentials and the potential to use those credentials for unauthorized entry into sensitive IT systems and applications.

Convenient: Built into the endpoint, so there's nothing extra to carry or lose.

Cost-effective: Typically greater than 50% lower total cost of ownership than USB token solutions, in some cases up to 65% less. Leverages pre-existing hardware for lower capital expenditure and eliminates replacement costs for lost tokens and smart cards.

Works right now: The only enterprise-capable virtual smart card that works on Windows 7. Available today on Windows 7, Windows 8 and Windows 8.1, and will work with Windows 10.



VISIT OUR DEMO #10

wave®

THE FAST, RISK-FREE WAY TO DEPLOY SEDs:

Wave Cloud

You know you should be encrypting data on every device in your organization, especially your laptops. Self-encrypting drives (SEDs) are the fastest, easiest and most secure way to do that – but setting up to support and manage SEDs can seem daunting. The world's first cloud-based service for managing SEDs, Microsoft Bitlocker and OSX FileVault, Wave Cloud lets users take advantage of the benefits of SEDs without jumping through the hoops traditionally associated with SED management, such as infrastructure development and training. Whether you're doing a small proof-of-concept or full-blown production deployment, Wave Cloud is the fastest way to get there.

- Active monitoring, logging, and reporting of all user and device events associated with SEDs
- Compatible with Windows 8.1, 8, 7 and Vista operating systems; and OSX 10.8 and 10.9 (for OSX FileVault)
- No infrastructure to buy or set up — fast, easy compliance
- The only cloud-based management solution that gives you drive initialization, user management, drive locking, and user recovery for all Opal-based, proprietary, and solid-state SEDs

#11 VISIT OUR DEMO

SOLID-STATE DRIVES WITH SELF-ENCRYPTION:

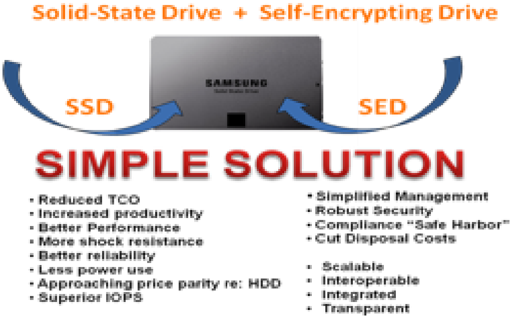
Solidly Secure

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 Cloud* and others.



SIMPLE SOLUTION

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

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

- Scalable
- Interoperable
- Integrated
- Transparent

VISIT OUR DEMO #11

WINMAGIC® DATA SECURITY

Micron

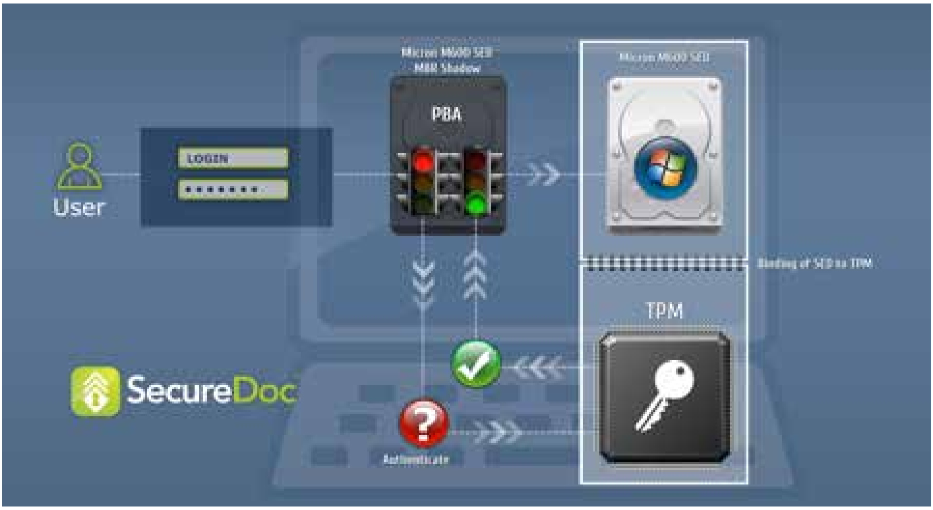
SED MANAGEMENT WITH TPM PROTECTION

Trusted Computing Technologies Supported: Opal Self-Encrypting Drive 2.0 and TPM

Self-Encrypting Drives (SEDs) are fast becoming the standard for enterprise customers who want a level of security built right into their devices since SEDs have their own on-board technology to encrypt data written to the drive. Organizations worldwide are increasingly securing confidential information on SEDs, recognizing that this approach simplifies the deployment of security for data at rest and provides significant cost savings.

With TPM embedded and enabled on a laptop, SecureDoc binds a SED with the TPM chip on device thus making it unusable if ever separated from the laptop. This demonstration will showcase how SecureDoc manages a SED such as a Micron M600 and encryption while integrating pre-boot authentication and the TPM embedded on a laptop; thus providing an ultimate and robust encryption security solution that is extremely easy to use.

WinMagic's SecureDoc Enterprise Server (SES) offers organizations total control over their data security environment by managing everything encryption across multiple platforms within the enterprise under one centralized enterprise server. This includes manageability of policies, password rules, Microsoft Bitlocker, Mac OSX FileVault 2, iOS, Android, SecureDoc Cloud and integration with industry-standard technologies such as Opal-compliant SEDs along with TPM.



#19 VISIT OUR DEMO

Get Involved

Trusted Computing Group Mission

Trusted Computing Group (TCG) 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.

Since its formation in 2003, TCG has been leading the industry with open standards that drive the creation of customizable security solutions for cloud, IoT, mobile, PC client, server, storage and network applications.

Why Join Trusted Computing Group?

Membership in the 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 the technical specifications, implementation guides, reference implementation 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.

Contact Us to Learn More

Trusted Computing Group Administration

Phone: +1.503.619.0562

Email: admin@trustedcomputinggroup.org

Web: www.trustedcomputinggroup.org/resources/rsa_conference_2015_tcg_association_seminar

TRUSTED
COMPUTING GROUP®

www.trustedcomputinggroup.org