Securing the IoT with Trusted Computing

Guide to TCG Seminar and Demonstration Showcase

RSA® CONFERENCE 2016

TRUSTED COMPUTING GROUP®

Seminar Schedule

8:30 WELCOME / INTRODUCTION TO SESSION

	MARK SCHILLER	*TCG Executive Director*

8:40 – 9:15 KEYNOTE:
Trust-Based Security for Multidimensional Clouds

	DOUG CAHILL	*Senior Analyst for Cybersecurity, Enterprise Strategy Group (ESG)*

9:15 – 10:00 PANEL 1:
IoT, Trust, and Security

MODERATOR:	**DARIN ANDERSEN**	*CEO and President, CyberTECH*
PANELISTS:	**MAX SENGES**	*Product Manager, Google Research*
	LEE WILSON	*Product Development Engineer, Security Innovation*

10:00 – 10:10 UPDATE FROM TCG AND DEMO HIGHLIGHTS

	MARK SCHILLER	*TCG Executive Director*

10:10 – 10:55 PANEL 2:
Things to Do with the TPM

MODERATOR:	**PAUL ROBERTS**	*Editor and Chief, Security Ledger*
PANELISTS:	**MATTHEW GARRETT**	*Principle Security Software Engineer, CoreOS*
	PAUL ENGLAND	*Software Architect, Microsoft*

10:55 – 11:05 BREAK

11:05 – 11:50 PANEL 3:
Network Security in the IoT

MODERATOR:	**DEREK HARP**	*Director for ICS Global Programs, SANS Institute*
PANELISTS:	**TONY SAGER**	*Senior VP and Chief Evangelist Center for Internet Security*
	STEVE VENEMA	*Senior Security Analyst, Polyverse*

11:50 – 12:00 END OF SEMINAR—LIVE RAFFLE DRAWING FOR PRIZES

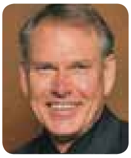
RAFFLE DRAWING PRODUCTS DONATED BY

- *Drive Trust Alliance*
- *Infineon*
- *Intel*
- *Micron*

12:00 – 12:30 DEMONSTRATION SHOWCASE

MOSCONE WEST ROOM 2006/2008

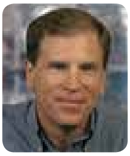
BRIEF WELCOME / INTRODUCTION TO SESSION



MARK SCHILLER
Executive Director
Trusted Computing Group

KEYNOTE

Trust-Based Security for Multidimensional Clouds



DOUG CAHILL
Senior Analyst for Cybersecurity
Enterprise Strategy Group (ESG)

PANEL 1:

IoT, Trust, and Security

DARIN ANDERSEN, Moderator
CEO and President
CyberTECH

MAX SENGES, Panelist
Product Manager
Google Research

LEE WILSON, Panelist
Product Development Engineer
Security Innovation

PANEL 2:
Things to Do with the TPM

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

MATTHEW GARRETT, Panelist
Principal Security Software Engineer
CoreOS

PAUL ENGLAND, Panelist
Software Architect
Microsoft

PANEL 3:
Network Security in the IoT

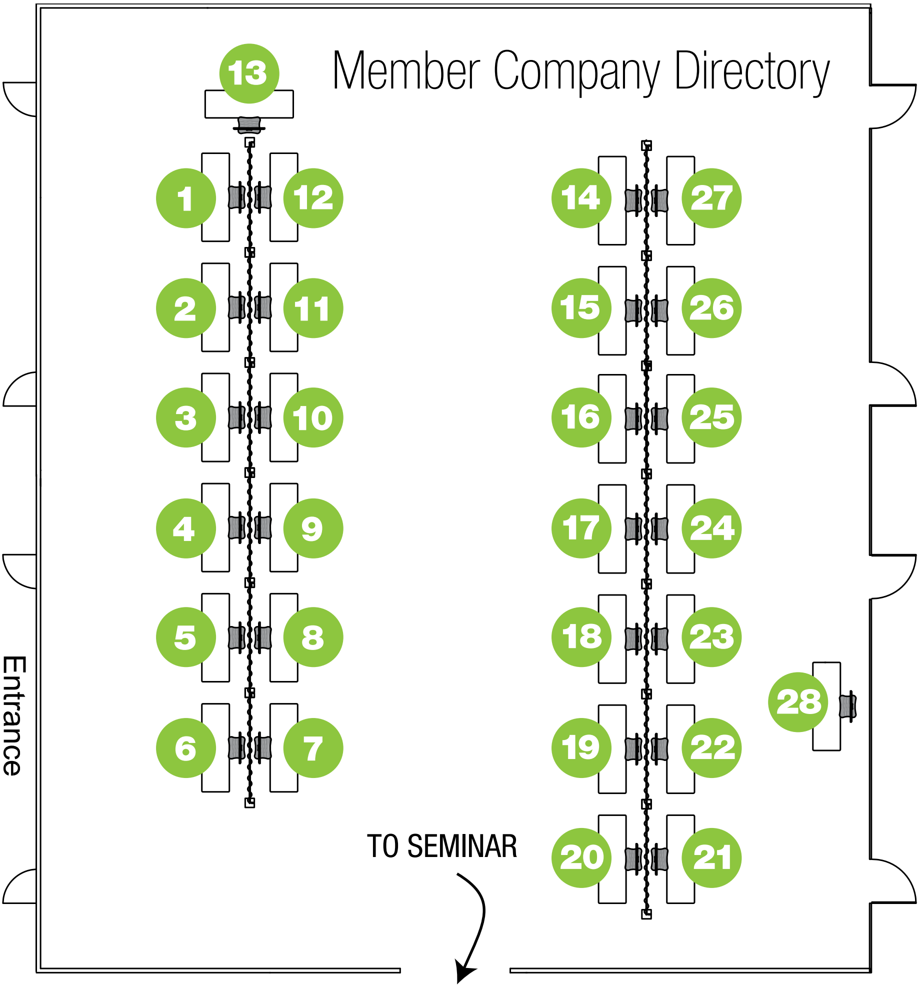
DEREK HARP, Moderator
Director for ICS Global Programs
SANS Institute

TONY SAGER, Panelist
Senior VP and Chief Evangelist
Center for Internet Security

STEVE VENEMA, Panelist
Senior Security Analyst
Polyverse

Demonstration Showcase

Member Company Directory



1. Tempered Networks
2. Fujitsu
3. JW Secure
4. Microsoft
5. Microsoft
6. CoSoSys
7. Aruba
8. Micron
9. Dell
10. PulseSecure
11. PulseSecure
12. WinMagic
13. Industrial Internet Consortium
14. Drive Trust Alliance
15. Fraunhofer
16. Infineon | GlobalSign
17. Infineon | WIBU Systems
18. Cisco | HSR | Infineon
19. Intel
20. Intel | Book Signing
21. Intel
22. Intel
23. Intel | Landesk
24. Huawei | Infineon
25. Anvaya Solutions
26. Embedded Computing Design
27. Security Ledger
28. TCG “Ask #TPM Expert”

ANVAYA Solutions

THINK OUTSIDE THE BOX — SECURE YOUR TLS!

The TLS (Transport Layer Security) protocol is the underpinning of secure transfer of information on the Internet today. TLS v1.2 is the current standard with TLS v1.3 on the horizon.

The TLS protocol uses cryptographic operations which have been traditionally implemented in software. The non-crypto operations in TLS include the functionality satisfying the SSL/TLS protocol requirements, and also the functionality interfacing to the TCP/IP network layers.

The TLS protocols are innately robust from the security point of view. However, their implementations using software library modules are beset with vulnerabilities which have been exploited for the last several years.

In our demo we present the hardening of the native security offered in the definition of TLS v1.2 and v1.3 protocols by embedding the crypto operations and TLS function calls inside dedicated fixed function hardware.

VISIT OUR DEMO #25

SECURING IoT WITH TRUSTED COMPUTING

Trusted Computing Technologies Supported: TPM and TNC

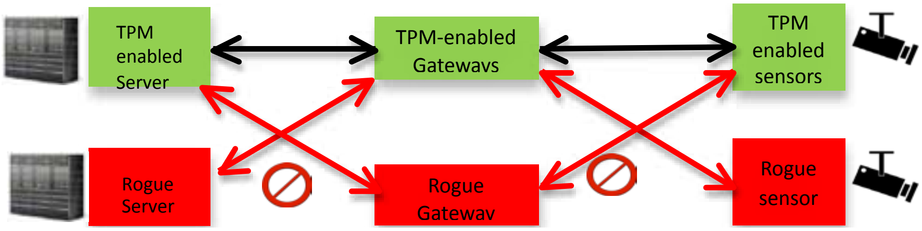
The Use Case for this demonstration is a deployment of IoT sensors and actuators (perhaps those found in a Smart Building) managed by a Cloud-based application that is remote to the sensors (such as the Building Management application). The server and the IoT devices are connected over the public Internet, 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.

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.

- OpenSSL mutual authentication requires a certificate AND a validated integrity report to start a session.
- Enterprise devices (green) use a TPM to protect an enterprise certificate and a device integrity report.
- Rogue devices (red) either do not have a valid certificate, a recognized integrity report or neither.



#18 VISIT OUR DEMO

ENDPOINT PROTECTOR | by CoSoSys

DATA LOSS PREVENTION IN MIXED ENVIRONMENTS — WINDOWS, MAC AND LINUX

Mac OS X and Linux saw a notable increase in market share in 2015, with industry experts predicting continued growth in the coming years. Windows is still dominating the enterprise networks, but Mac OS X and Linux have become increasingly common in companies' workstations, requiring solutions that ensure they are just as secure as the rest. Ignoring any of the 3 platforms creates a hole in the data security strategy, making the implementation on just two of them or one of them obsolete.

Endpoint Protector 4 Data Loss Prevention integrates in mixed environments and offers complete protection against data leakages and data thefts. The demo will highlight the content filtering capabilities on all 3 operating systems, helping organizations to secure data and prevent leakages that could easily happen through online applications, the cloud and through portable storage devices. Documents with highly sensitive data like Credit Card Numbers, Social Security Numbers, PII, financial information, etc. will remain within the corporate networks with Endpoint Protector DLP implemented. They will only be uploaded/copied on the trusted websites/portals/devices and sent to trusted individuals if DLP will be properly setup on all employees' workstation, regardless if they have Windows, Mac OS X or Linux.

Additionally, the demonstration will show the detailed reports and graphics that serve for audit and detect potential data security incidents. IT Administrators can visualize who is transferring what data at what time and the destination, having the possibility to also download a copy of the transferred files or the blocked files to check their content.

Due to the current threat landscape and the increased number of breaches caused by insiders, demand for Data Loss Prevention is constantly rising. Business should take into consideration all operating systems to make sure data protection is consistent and doesn't have gaps that make the whole system vulnerable.

VISIT OUR DEMO #6

ENABLING MISSION-CRITICAL IoT APPLICATIONS WITH A DELL EDGE GATEWAY

Automotive is one of the most exciting applications of the IoT with recent advancements in fleet management, easier parking, a better way to find a ride home, and a path to autonomous cars. However, with this innovation, it is critical to adopt effective security technology and practices to ensure that these connected systems are not compromised. This demo shows how separation in data planes can deliver higher security across a wide range of applications, including automotive. See how intelligent gateways from Dell and LynxSecure virtualization software work together to effectively manage both an in-vehicle infotainment system and an Engine Control Module, while keeping the operating systems separate and more secure.

#9 VISIT OUR DEMO

OPEN SOURCE MANAGEMENT SOFTWARE FOR SEDs

Bright Plaza forms the Drive Trust Alliance, jointly with (Tom) Coughlin Associates

- Mission: promote (TCG/OPAL) SED adoption; Alliance of company/organization/individual Sponsors that will benefit from cost efficiencies in: marketing, on-going education, compliance, creation/support open source software for managing SEDs

Open Source Software:
DEMO—Open Source for TCG(OPAL)/Enterprise; Windows/MAC/Linux; Easy to Use by Anyone

- Client software: initialize and provision a TCG/OPAL Self-Encrypting Drive (SED), unlock one or more TCG ranges on that drive for reading and/or writing (Demo on Apple Machine)
- Network agent application for remote management of these functions using: OASIS KMIP protocols or OMA protocols (in the case of mobile OSes)
- Roadmap: pre-OS boot (PBA) software and allow TCG OPAL ranges re: non-PBA use cases

Technical Marketing, Educational, and Compliance Services:

- Marketing/Educational Services: Technology Tutorials, Technology Tutorials—OnSite, Internal Sponsor Education—Onsite, Webinar-based Education, Conference Talks, Conference Booths, Conference Sponsorship (Less Conference Fee), Tailored SED Collateral, White Papers, Public Relations Partnerships
- Compliance Services: Information Security Architecture, Comprehensive Information Security Program, Risk-based Assessment, Cyber Response Plans, Incident Response and Business Continuity/Disaster Recovery, Business Continuity Management

WWW.DRIVETRUST.COM

VISIT OUR DEMO #14

Fraunhofer
SIT

ADVANCED FIRMWARE UPGRADE SCHEMES USING TPM 2.0 ENHANCED AUTHORIZATION POLICIES

Most embedded devices come with the need to store persistent data about their configuration, state, or application data, which are not part of the base firmware image. Furthermore, most devices require means to perform firmware upgrade of the base executables without alteration of the persistent data.

Using a TPM 2.0 it is possible to encrypt the persistent data for a given device. The TPM also has the capability to bind this encryption to known trustworthy firmware images, such that only the original firmware, but no bogus alternative firmware, can decrypt the persistent data. In order to upgrade the firmware image, without accessing to the encrypted persistent data, requires schemes that are more advanced.

This demonstrator realizes a concept for advanced firmware update schemes, where the persistent data is encrypted using the TPM and bound to the current firmware image. In this scheme, updates are performed by adding the new firmware image to the list of trusted firmware images without the need to re-encrypt or even access the persistent data. Furthermore, the formerly trusted firmware is being removed from the list of allowed firmware images to prevent downgrade attacks, making use of TPM 2.0's Enhanced Authorization Policies and monotonic counters.

This concept was implemented for a Connected Car IoT application scenario using a Linux-Based Automotive Head Unit where the whole persistent application storage data is secured against unwanted access. This application storage includes not only configuration, but also personal data – e.g., the address book – and vendor Intellectual Properties – e.g., navigation data. The whole process works in an "offline" manner based on a TPM 2.0 and the SIT-TSS 2.0 implementation, requiring no direct connection of the device to the original manufacturer.

#15 VISIT OUR DEMO

FUJITSU

SECURE REMOTE MAINTENANCE FOR ECUs IN A CAR USING TPM

APPLICATIONS OF TCG TECHNOLOGY FOR AUTOMOTIVE AREA

1) Remote firmware update for ECUs in a car with integrity checking by TPM

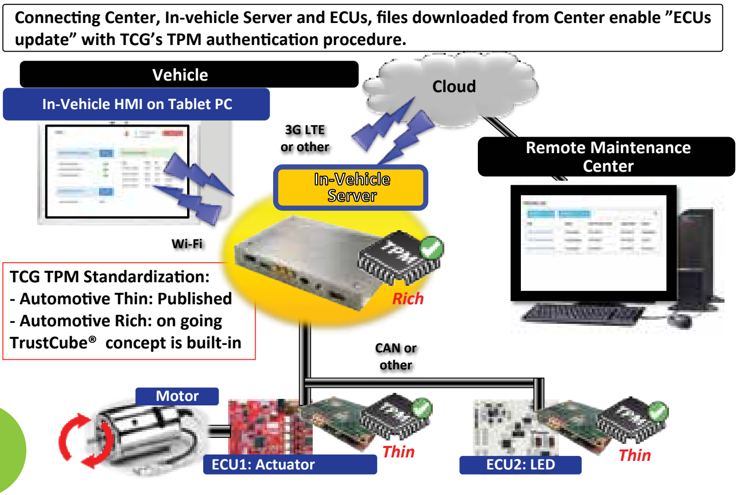
2) Prevent any mistakes or wrong ECU populating at all Third Party detail shops

Details:

1) The secure update is implemented using the following three steps:
   - Accurate remote determination of in-vehicle software and hardware configuration and integrity
   - Verification of successful completion of intended software updates
   - Secure long-term storage of audit logs of the related updated operations and TPM measurement operations

These are based on TPM 2.0 Automotive-Thin Profile v1.0 published by TCG.
http://www.trustedcomputinggroup.org/resources/tcg_tpm_20_library_profile_for_automotivethin

2) Based on TCG/TPM mutual authentication, typically, third party detail shops must handle cars from multiple auto makers. The shop would order replacement parts (ECUs) suitable for different vehicles. The shop might populate wrong ECU and in order to prevent this mistake, they should check based on the statement of direction. Unfortunately, the check has to be done by a person and therefore cannot be 100% guaranteed. Based on TCG/TPM mutual authentication, populating of wrong ECU can be found and rejected.



Connecting Center, In-vehicle Server and ECUs, files downloaded from Center enable ”ECUs update” with TCG’s TPM authentication procedure.

TCG TPM Standardization:
- Automotive Thin: Published
- Automotive Rich: on going

TrustCube® concept is built-in

VISIT OUR DEMO #2

aruba
a Hewlett Packard
Enterprise company

NAC AND ENDPOINT DEFENSE FOR A MOBILE WORKFORCE

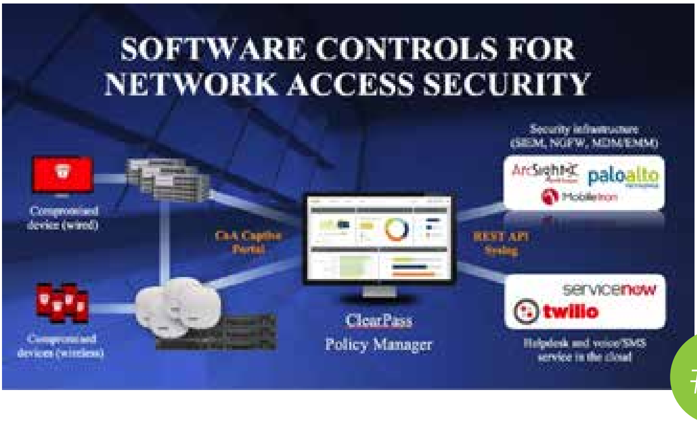
Wireless Demo:

1. Connect mobile device (Android/IOS) to WLAN
2. Show that device is able to access the internet without an issue
3. Launch malware application
    - Behind the scenes the FW (PANW) detects the malware and sends a Syslog to ArcSight
    - ArcSight receives the warning and initiates an API call to ClearPass to bounce and redirect the user to a captive portal page
4. Show that device cannot access the internet and now gets a captive portal page indicating an issue and a helpdesk ticket has been opened upon the user's behalf
5. Wait for phone call and sms/push notification to wireless device which demonstrates the helpdesk automation

Wired Demo 2:

1. Connect an HP laptop to a HP 2920 switch
2. Show that device is able to access the internet without an issue
3. Launch malware application
    - Behind the scenes the FW (PANW)) detects the malware and sends a Syslog to ArcSight
    - ArcSight receives the warning and initiates an API call to ClearPass to bounce and redirect the user to a captive portal page
4. Show that device cannot access the internet and now gets a captive portal page indicating an issue and a helpdesk ticket has been opened upon the user's behalf

Wait for phone call and sms/push notification to user's phone which demonstrates the helpdesk automation



SOFTWARE CONTROLS FOR NETWORK ACCESS SECURITY

Security infrastructure (SIEM, NGFW, MDM/EMM)

Helpdesk and voice/SMS service in the cloud

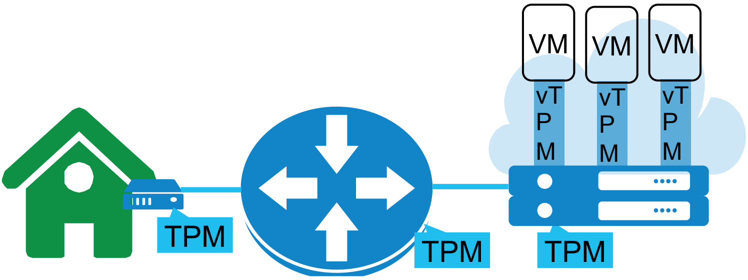
#7 VISIT OUR DEMO

HUAWEI AND INFINEON SECURE THE IoT WITH TPM

Many industry surveys have shown that security is the number one concern for the Internet of Things (IoT). Huawei's IoT platform addresses this concern head-on by building in support for security, including Trusted Computing. In this demo, Huawei's IoT dashboard leverages Infineon's Trusted Platform Module (TPM) chips to monitor and manage key components of the IoT system – the IoT gateway, the router, and the cloud server.

Huawei's IoT platform validates the software integrity on each IoT component by verifying the integrity information and device identity using the Remote Attestation feature of the TPM and an Attestation Identity Key (AIK) protected by the TPM. The IoT platform also supports virtual TPMs that provide security to the applications in Virtual Machines (VMs), leveraging a hardware TPM.

In this manner, the security of IoT systems can be easily verified from the cloud. Any problems can be quickly identified. This demo illustrates Huawei's solid commitment to ease of use and to providing strong security to all of its customers.



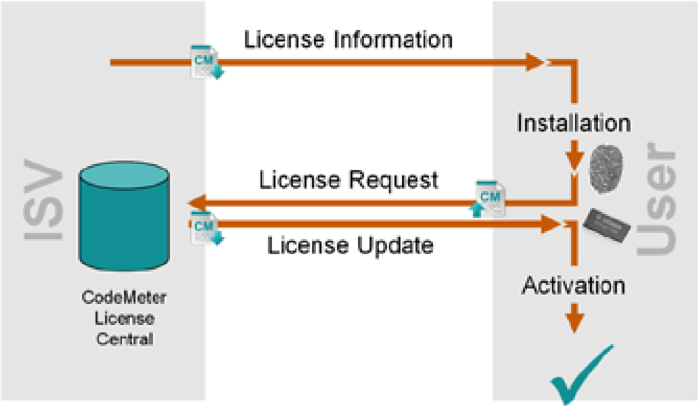
VISIT OUR DEMO #24

IP PROTECTION AND FLEXIBLE LICENSING APPLIED TO TPM CONNECTED DEVICES

Attackers often use reverse engineering to find software vulnerabilities that they can exploit to create counterfeit products, steal sensitive data, or tamper with for sabotage and espionage purposes. With embedded systems, this can lead to serious and dangerous hacks, as recent attacks on safety-critical automotive components have shown.

This demonstration shows how to protect software integrity against cyber violations and safeguard the intellectual property your business growth relies on.

Wibu-Systems CodeMeter® creates secured code and licenses. These licenses can be bound to a secure element, a hardware dongle or an Infineon OPTIGA™ TPM, in the target system, creating confidence that the code and the licensed features are only used on that system. License creation and deployment can be seamlessly integrated into existing business processes, such as ERP systems or e-commerce platforms. This mechanism opens up completely new business models, such as feature upselling and time-based or pay-per-use licenses, for the IoT and other intelligent devices.



#17 VISIT OUR DEMO

intel

LANDESK

REMOTE SECURE ERASE

LANDESK Management Suite and Intel® Remote Secure Erase
Repurposing a PC made easy

Executive Summary

When a PC is retired or repurposed, information security policies often require data to be “wiped” from the drive. Wiping can be difficult and time consuming. LANDESK Management Suite with Intel® Remote Secure Erase is a better solution.

An Intel® Remote Secure Erase-based solution provides the IT administrator a way to wipe out all data; allowing for immediate reuse while saving significant administrative time and costs. Unique to this solution is the capability to complete the secure erase independent of a functioning OS while being fully managed using LANDESK Management Suite.

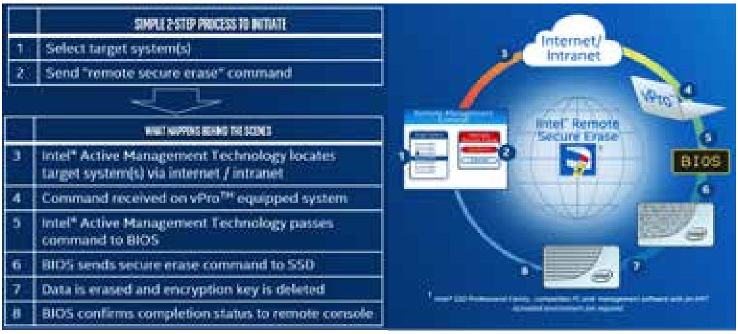
Reduce administrative costs, reinvest your IT time in higher priorities through the use of LANDESK Management Suite with Intel® Remote Secure Erase as your solution of choice.

Use Case

The main usage of this technology is within a corporate environment which has the requirement to wipe data when repurposing a system. Intel® Remote Secure Erase can be used to save time and money for IT administrators, while meeting information security policies.

With this solution, if an employee leaves a job, is terminated, or is moving to a new PC, IT is able to issue the secure erase command remotely to ensure the SSD is securely wiped; eliminating the need to remove or shred the SSD. This solution also allows a drive to be erased prior to shipping to another location, thus eliminating the risk of data being lost or stolen during transit.

How it works



	SIMPLE 2-STEP PROCESS TO INITIATE
1	Select target system(s)
2	Send "remote secure erase" command

	WHAT HAPPENS BEHIND THE SCENES
3	Intel® Active Management Technology locates target system(s) via internet / intranet
4	Command received on vPro™ equipped system
5	Intel® Active Management Technology passes command to BIOS
6	BIOS sends secure erase command to SSD
7	Data is erased and encryption key is deleted
8	BIOS confirms completion status to remote console

[1] Intel® SSD Professional Family, compatible PC and management software with an AMT activated environment are required

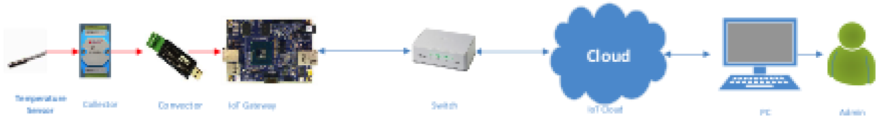
VISIT OUR DEMO #23

TRUSTWORTHY IOT GATEWAY

In many IoT scenarios, scientists or government officials rely on data received from remote deployed monitor devices and sensors to create models and make decisions. While these remotely deployed gateways provide valuable and real-time data for scientists, engineers and policy makers, they are often prevalent to attacks due to simplicity and accessibility to attackers. Finding a way to secure these IoT gateways becomes a challenge for IoT security experts.

Security companies and expert has been tried to solve the IoT gateway challenges for years, traditional Anti-Virus vendors mitigate their while-listing software to embedded systems, there are other vendors try to use open source tools like IMA security to monitor applications' unintended changes. These solutions' shortcoming are costly or too complex to use, besides that, above solution consumes too much compute resource in a constraint environment and couldn't provide enough security level as hardware security technology provides.

To solve the shortcoming of current solutions in the market, this demo using Trusted Platform Module (TPM) as hardware root-of-trust to maintain and verify the integrity value of gateway OS, and remote attest gateway with servers in the cloud. This approach enable IoT Gateway vendors to build a trustworthy gateway with affordable effort, it is low cost, ease of use, and extensible to all IA based platform and more robust hardware security technology.



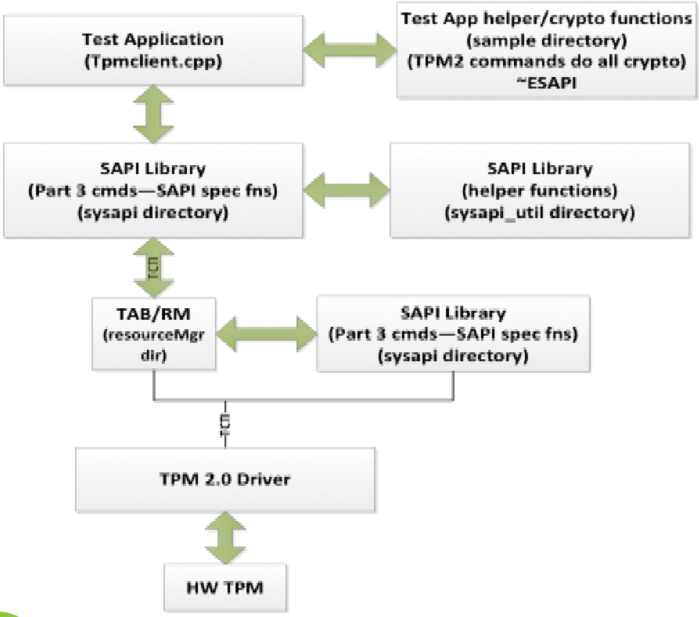
#22 VISIT OUR DEMO

TPM 2.0 FAMILY ENABLING FOR LINUX

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. Also provides the system resources as was done for TPM 1.2



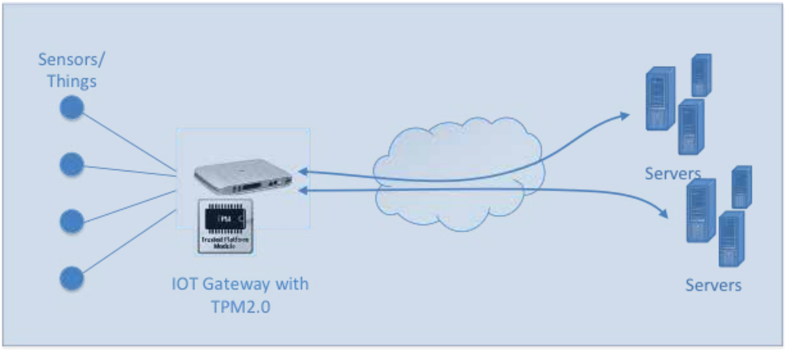
VISIT OUR DEMO #20

EFFECTIVE TPM 2.0 VIA ANDROID AND REPRESENTATIONAL STATE TRANSFER (RESTful) ARCHITECTURE

The emergence of "thingsbot" and many other security threats in IoT are fast become attractive targets to hackers on aiming the smart appliances, as the "things" often have less security focus. Often, embedded hardware root-of-trust implementations are not well presented at the user space too. As a result, the real potential and its intended design expectation falls short. One such example is the Trusted Computing Group's Trusted Platform Module 2.0 (TPM2.0) implementation, of which lack of application level usage implementation. The aim of this presentation is to share one seamless method to expose such embedded APIs of TPM2.0 into the application user space; whereby larger developer community could benefit from. One promising end-to-end IoT device security solution usage, is by strengthening platform security and HWRoT with TPM2.0 usage via Android platform.

In this demo we will present TPM2.0 Use Cases via Smart Home concept. Sensors from smart fridge will generate events base on the low inventory, and the events are being communicated to a smart and secured gateway system. The gateway will exercise TPM2.0 Keys store, Provisions and Authentication mechanism, and the home gateway will sent event messages to home user's Android tablet. Home user via the tablet Android apps being notified of the event, verified, and make payment order to refill inventory.

The demo will comprise of HWRoT security usages in RESTful architecture and framework. In this demo, the idea of ease-of-use IoT security implementation via TPM2.0, together with the harmonious practices of TPM2.0 via Android platform will be presented.



#19 VISIT OUR DEMO

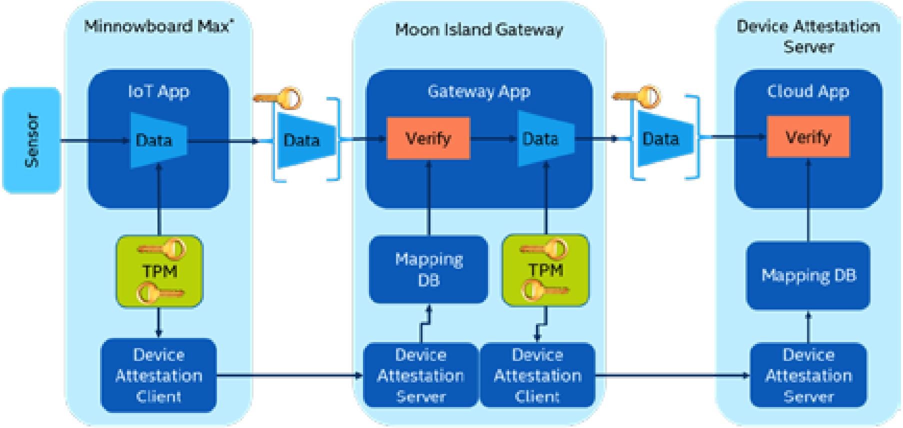
TRUSTING IoT DEVICES USING REMOTE DEVICE ATTESTATION

Unlike what we normally view as computing clients, IoT sensors, actuators, gateways and other infrastructure components do not have “human users” logging into them providing identity and authentication of that identity. Instead, IoT components act autonomously. This doesn’t reduce, in fact, it increases, the need to identify these devices. As these devices are a composite of hardware and firmware, identification includes not just the identity of the hardware but also the firmware running on that hardware. This is called Remote Attestation and the TPM was architected to solve this problem by providing the hardware and firmware’s identity along with a proof of those identities to an external service.

Using an Intel MinnowBoard Max with TPM 2.0 and the Linux TPM 2 driver and TCG compliant System API software stack we will demonstrate the use of TPM 2 protocols to authenticate the platform’s identity and software stack to an IoT gateway and Cloud-based server. The attestation infrastructure will use Intel’s Device Attestation 2.0.

The MinnowBoard Max will act as the IoT edge device communicating to an Intel Moon Island-based IoT Gateway. The Gateway will authenticate the MinnowBoard Max before authorizing data to flow back to the Cloud component. The Cloud component, will in turn authenticate the Intel Moon Island Gateway before accepting data from the Gateway or the MinnowBoard Max

Visit our RSA Booth #N3705.


Minnowboard Max*
Moon Island Gateway
Device Attestation Server
Sensor
IoT App
Data
Data
Gateway App
Verify
Data
Data
Cloud App
Verify
TPM
Mapping DB
TPM
Mapping DB
Device Attestation Client
Device Attestation Server
Device Attestation Client
Device Attestation Server

Intel® Expansion Kit with MinnowBoard MAX*

VISIT OUR DEMO #21

Micron®

SELF-ENCRYPTING SOLID STATE DRIVES

— SEDs from the Notebook to the Server

As Data Security has increased in importance, Full Drive Encryption (FDE) has moved from a recommended solution, to highly desired, to legally-required in many data storage applications. The Self-Encrypting Drive (SED) is a specific type of FDE which deploys hardware-based encryption performed by the storage device itself. State-of-the-art AES 256-bit encryption engines are always on, running without the performance loss seen in many software encryption solutions. Encryption keys are generated and kept secure by the drive itself, inaccessible through the storage interface. Key management for SED is simple, as no additional hardware or software is necessary to manage encryption keys. The host system need only manage authentication through password, passcode or other authentication device.

Amazingly, stored data in mobile computing and data center computing face analogous security risks. Mobile computers (notebooks, tablets, smart phones, even IoT) maximize worker productivity, but also cast valuable data out into a risk-filled world. Likewise, even with strong physical security, thousands of drives daily leave data centers throughout the world, through failure, retirement or even theft. SED can close these security gaps. When a mobile computer is lost, or a drive must be removed from the data center, data-at-rest on an SED will remain encrypted and secure. Also, data sanitization is fast and easy for SED, as a simple command can make all the bits on the drive unreadable, by any known means, almost instantly.

Micron Technology, Inc. (www.micron.com), a global leader in advanced semiconductor systems, is demonstrating both our M600 TCG Opal SSC[1] SED in a notebook, and our M510DC TCG Enterprise SSC SED, running in a RAID system as a Hyper-V™ host in Microsoft® Windows 10 Professional. Our encrypted notebook computer can also run as a client in this Hyper-V system, showing encryption at the endpoint, and encryption at the virtual machine level.

[1] SSC = Security Subsystem Class.

#8 VISIT OUR DEMO

JW SECURE STRONGNET™ SECURE ADMIN

Privileged account management done right from the start.

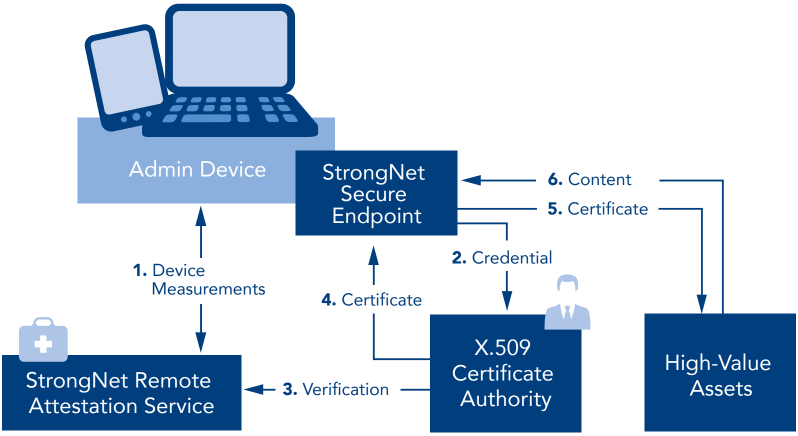
As a result of the growing Bring Your Own Device and cloud computing trends, enterprise connectedness has exponentially increased. At the same time, the DevOps movement has expanded the number of accounts with system administrator access to servers and data. With all of these entry points, the increasing sophistication of Internet attackers and the potential for insider threats seriously threaten enterprise data security.

Protect your business with hardware-enforced endpoint 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. This enforces your security policies in a way that is both meaningful in the face of determined adversaries as well as transparent to your users. This combination of hardened workstations and secure network enables low-risk computing for high-privilege users.

Make security choiceless.

StrongNet™ Secure Admin uses the Trusted Platform Module to deliver high-integrity user and computer credentials. Our proprietary Measurement Bound Keys ensure that credentials will not be accepted unless the mobile device complies with security policy. And by making endpoint security policy enforcement transparent, automatic, and hardware-based, you get a best-in-class solution for blocking the bad guys.



VISIT OUR DEMO #3

Microsoft

ENTERPRISE READY IOT DEVICES

Security features that Enterprises and Government customers depend on, now on the smallest of devices with Windows 10 Core IoT!

Windows 10 IoT Core is a version of Windows 10 that is optimized for smaller devices with or without a display, and that runs on the Raspberry Pi 2, Arrow DragonBoard 410c & MinnowBoard MAX. Windows 10 IoT Core utilizes the rich, extensible Universal Windows Platform (UWP) API for building great solutions. Windows 10 IoT Core brings the power of Windows to your device and makes it easy to integrate richer experiences with your devices such as natural user interfaces, searching, online storage and cloud based services

UEFI SECURE BOOT Secure Boot is a security standard developed by members of the PC industry to help make sure that your device boots using only software that is trusted by the device manufacturer. When the device starts, the firmware checks the signature of each piece of boot software, including firmware drivers (Option ROMs) and the operating system. If the signatures are good, the device boots, and the firmware gives control to the operating system.

BITLOCKER Windows BitLocker Drive Encryption is a security feature that provides better data protection for your device, by encrypting all data stored on the Windows operating system and data volumes against offline access. IoT devices are usually deployed in potentially hostile environments without supervision. Unauthorized individuals could attempt to access data, OS files and configuration information by simply pulling the SD Card out of the device. BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys cannot be accessed until the TPM has verified the state of the device. Encrypting the entire volume protects all of the data, including the operating system itself, the Windows registry and temporary files.

SECURE CERTIFICATE STORAGE WITH THE CNG PLATFORM CRYPTO PROVIDER Cryptography API: Next Generation (CNG) is designed to be extensible at many levels and cryptography agnostic in behavior. The Platform Crypto Provider provides a generic way applications and services to make use of the TPMs secure key storage capabilities without the need of special code. PCPKSP provides full support for certificate enrollment or import of hardware bound keys that cannot be exported or duplicated. This provides security against device cloning or leakage of device stored credentials.

STRONG AND RELIABLE ENTROPY GENERATOR IoT devices usually do not have the rich set of peripherals to their disposal as PCs, Notebooks and Servers, so if an identical OS image is deployed on identical IoT devices, the amount of entropy that these devices possess is very limited. The TPMs strong RNG helps Windows to maintain high level entropy and keep the devices unique.

http://ms-iot.github.io/content/en-US/IoTCore.htm
https://technet.microsoft.com/en-us/library/hh824987.aspx
http://windows.microsoft.com/en-US/windows-vista/BitLocker-Drive-Encryption-Overview

#5 VISIT OUR DEMO

Microsoft

HEALTH ATTESTATION FOR WINDOWS SYSTEMS

OVERVIEW

Windows 10 includes support for Mobile Device Management solutions to evaluate the health of Windows 10 devices by using boot measurements recorded in the Trusted Platform Module (TPM). The measurements reflect configuration information about boot, the starting state of the Windows 10 operating system and how some operating system security features are configured. For devices enrolled with a Mobile Device Management solution, boot log information and signed TPM Platform Configuration Registers values are sent to Microsoft's Health Attestation Service and processed into easy to consume information for Mobile Device Management solutions. Mobile Device Management solutions can receive the information and apply policy actions based on evaluation of the results. For example, policy might only grant access to a file share for clients that had BitLocker Drive Encryption enabled during boot.

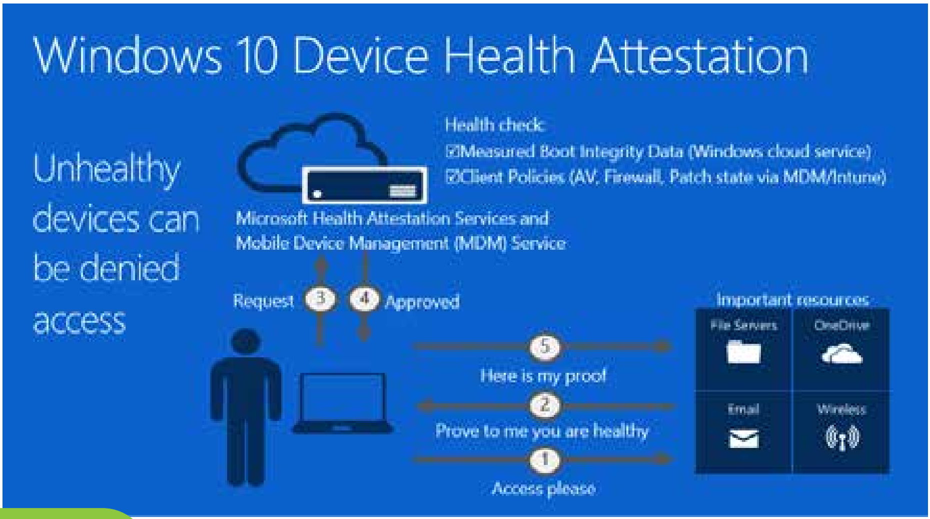
EXAMPLE SECURITY PROPERTIES

- UEFI Secure Boot on/off
- Virtual Secure Mode on/off
- BitLocker on/off
- Windows Boot Manager version
- Code Integrity Policy Hash

MORE INFORMATION

https://msdn.microsoft.com/en-us/library/windows/hardware/dn934876(v=vs.85).aspx

ARCHITECTURE



Windows 10 Device Health Attestation

Unhealthy devices can be denied access

Health check:
☑Measured Boot Integrity Data (Windows cloud service)
☑Client Policies (AV, Firewall, Patch state via MDM/Intune)
Microsoft Health Attestation Services and
Mobile Device Management (MDM) Service
Request
3
4
Approved
Important resources
File Servers
OneDrive
Email
Wireless
5
Here is my proof
2
Prove to me you are healthy
1
Access please

VISIT OUR DEMO #4

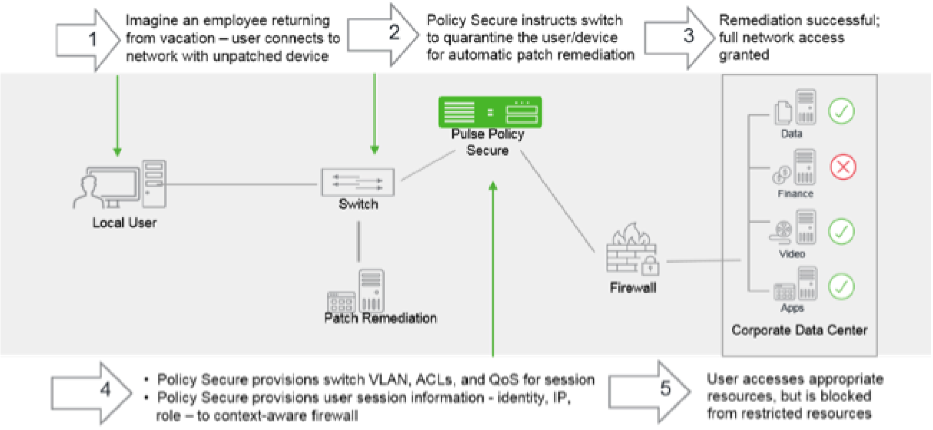
Pulse Secure

INTELLIGENT ENDPOINT COMPLIANCE

Pulse Policy Secure NAC utilizes Trusted Network Communication (TNC) end-point compliance standards to enable endpoint posture evaluation and secure access for BYOD, guest, and corporate devices.

BYOD security is a hot topic for the enterprise - end users want to work from their preferred personal devices, and corporations desire the productivity gains and cost reductions associated with permitting them. But with greater flexibility comes increasing threat - personal and guest devices are at a higher risk of compromise than corporate devices. How do we ensure that we can trust these devices enough to allow them on our networks?

Pulse Secure's Policy Secure NAC solution offers the ability to evaluate compliance and provide context-based secure access to personal, corporate, and guest endpoints. TNC's endpoint compliance standards enable Pulse Secure to collect endpoint posture pre- and post-admission across corporate, personal, and guest devices.



1 Imagine an employee returning from vacation – user connects to network with unpatched device

2 Policy Secure instructs switch to quarantine the user/device for automatic patch remediation

3 Remediation successful; full network access granted

4
- Policy Secure provisions switch VLAN, ACLs, and QoS for session
- Policy Secure provisions user session information - identity, IP, role – to context-aware firewall

5 User accesses appropriate resources, but is blocked from restricted resources

#10 VISIT OUR DEMO

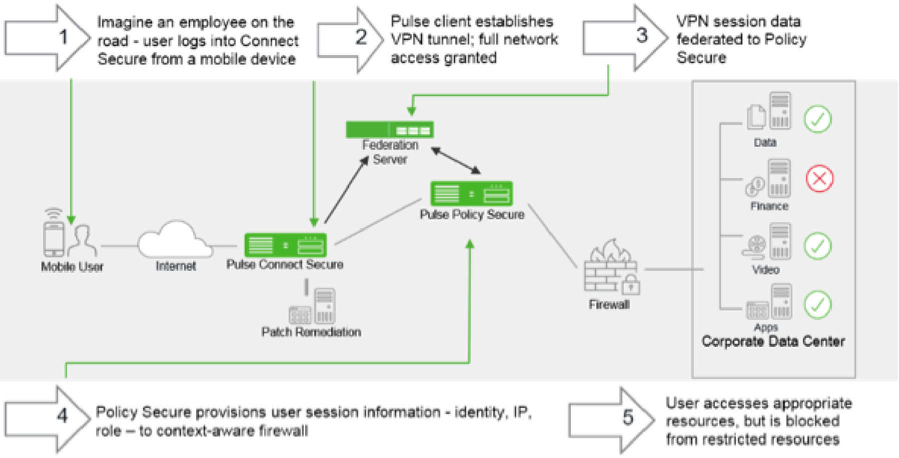
Pulse Secure

SIMPLIFY SECURE ACCESS

Pulse Connect Secure SSL VPN and Policy Secure NAC leverage Trusted Network Communications (TNC) security automation standards to enable context-based, seamless remote & local secure access.

Organizations are increasingly seeing staff using their laptops, smartphones, and tablets in the office, at home, and on the road. The traditional on-premise desktop is no longer at the center of the end-user's universe. With the trend toward users accessing corporate resources from anywhere at any time, secure access in a BYOD world means organizations must enable access to corporate networks in ways that minimize risk to the organization while maximizing the productivity of their employees.

Pulse Secure's Connect Secure SSL VPN gateway and Policy Secure NAC solution offer single sign-on for remote users accessing protected internal resources, and a seamless transition from remote to local access. TNC's security automation standard, IF-MAP, enables Pulse Secure to coordinate user information and provide transparent secure access.



1 Imagine an employee on the road - user logs into Connect Secure from a mobile device

2 Pulse client establishes VPN tunnel; full network access granted

3 VPN session data federated to Policy Secure

4 Policy Secure provisions user session information - identity, IP, role – to context-aware firewall

5 User accesses appropriate resources, but is blocked from restricted resources

VISIT OUR DEMO #11

TEMPERED NETWORKS®

"CLOAKING" IS THE NEW PERIMETER

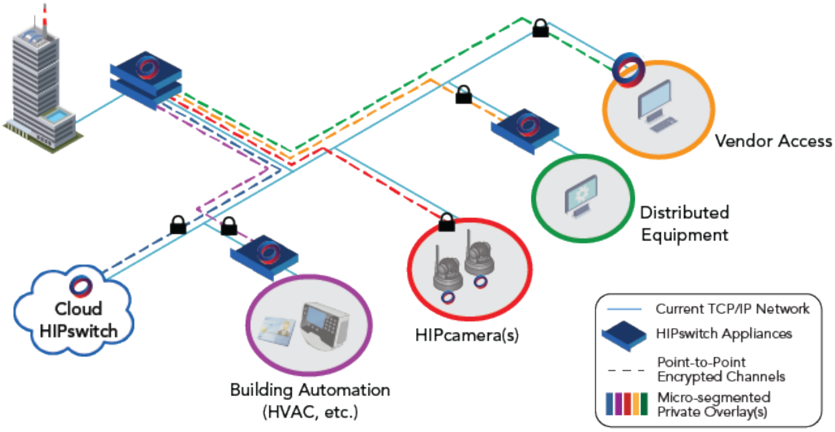
With the combination of cloud computing, mobile and IoT, securing the assets of any organization with existing solutions has become exponentially more difficult. Perimeter security, as we know it today, is limited in its ability to address this new computing model.

How do you create the appropriate trust and opaqueness in this new digital world to replace the old perimeter security that is so vulnerable? When devices can't protect themselves (IoT), they are in the wild and out of your control (Mobile), or distributed outside your facilities (Public Cloud); it's a tall order.

Solution specifications:

- First, ensure that only trusted entities can talk to other trusted entities. This requires a unique, cryptographic identity (CID) that is only known to the other trusted players and replaces the IP address as the identifier (HIP Protocol).
- Second, invoke policies that specify which CIDs can talk to another CID (whitelisting).
- Third, employ strong encryption to conceal any communication (AES-256).
- Lastly, automated orchestration (IF-MAP) is required to ensure error free configuration.

Bringing it all together:

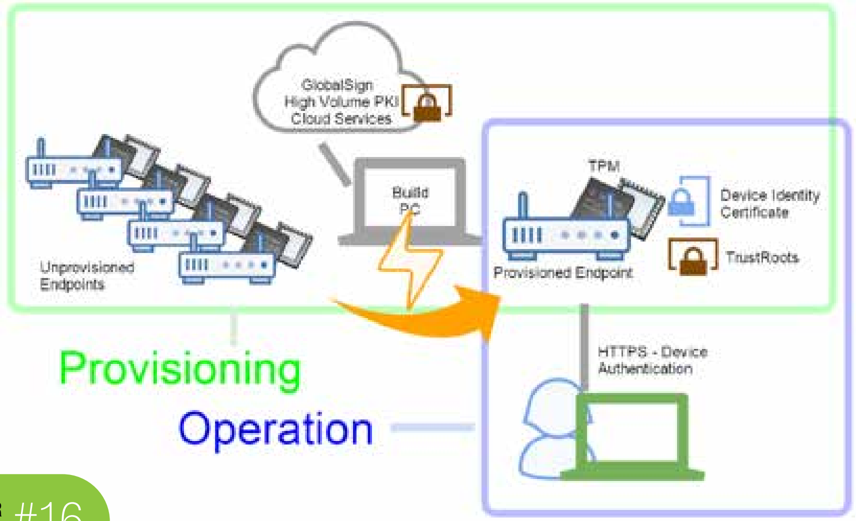


#1 VISIT OUR DEMO

SCALABLE STRONG DEVICE IDENTITY THROUGH PROVISIONING AND OPERATION

Some critical security concerns that an IoT provider needs to address include authentication, privacy and integrity. Mitigating risks in securing trust credentials, as well as building proven solutions at an IoT scale, are addressed in this Strong Device Identity demonstration combining GlobalSign's high-scale cloud-based PKI service and Infineon's OPTIGA™ TPM.

This joint demo shows how the Provisioning and Operation of IoT endpoints can leverage PKI and secure hardware in a scalable method while also building robust device identity. Combining both of these technologies illustrates how to mitigate against risks, like key compromise and identity spoofing, while also being able to extend trust and deployment models at a massive scale. In the Provisioning phase of the demonstration, we introduce a build PC, which helps automate the steps for certificate enrollment through to GlobalSign's high-scale cloud-based PKI service. The build PC helps coordinate secure cryptographic operations on Infineon's OPTIGA™ TPM and interface a CSR into the cloud services for certificate issuance. The concepts included with the build PC can be adopted into a wide range of potential use cases as the capabilities of devices will vary. In the Operation stage of the use case, we demonstrate the device using the credential to authenticate via an embedded web server and client browser. This Operational example is easily extensible into more prevalent architectural device models to cloud authentication.



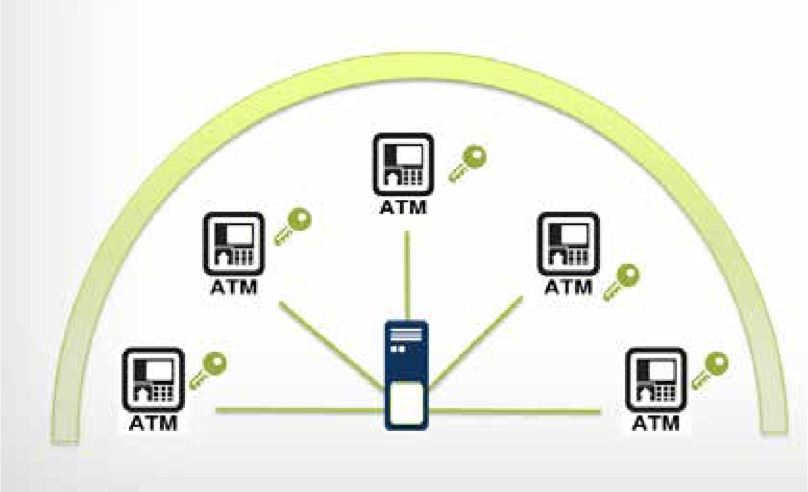
VISIT OUR DEMO #16

WINMAGIC
DATA SECURITY

SEDS IN THE IoT

As with desktops and laptops Self-Encrypting Drives can have a key role to play when protecting data at rest in the IoT. However, IoT devices often operate in very different environments than laptops. ATM's *(Automated Teller Machines)* are one example of an IoT device that often sit in a potentially hostile environment open to physical attack and at the same time an attractive target. ATM's are usually network connected, expected to boot automatically and, unlike a laptop, there is no trusted user present to perform pre-boot authentication.

Through this demonstration, WinMagic will show how ATMs with SEDs can be authenticated and managed with SecureDoc's pre-boot networking technology, PBConnex.



#12 VISIT OUR DEMO

TRUSTED
COMPUTING GROUP®

STRATEGIC PARTNERS —

Trusted Computing Group & Industrial Internet Consortium (IIC)

industrial internet
CONSORTIUM

MEDIA PARTNERS —

Embedded Computing Design & The Security Ledger

Embedded COMPUTING DESIGN
Connecting Silicon, Software, and Strategies for Intelligent Systems

the security ledger
Cyber Security News & Analysis

NOTES:

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/RSAC

TRUSTED COMPUTING GROUP®

www.trustedcomputinggroup.org