TRUSTED COMPUTING:

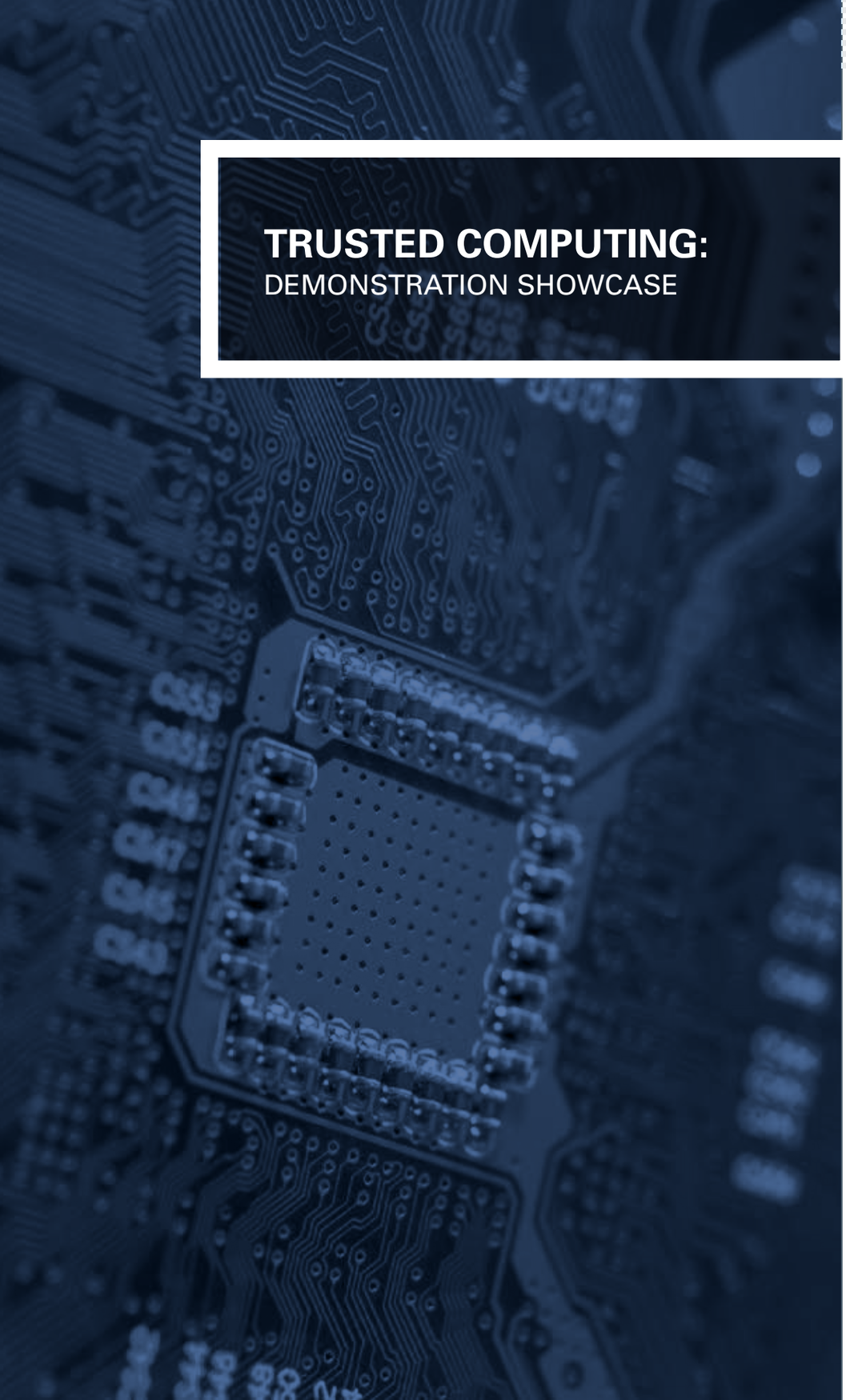
BILLIONS OF SECURE ENDPOINTS IN 10 YEARS

RSA® CONFERENCE 2013

TRUSTED COMPUTING GROUP™

SEMINAR AGENDA

10:00AM	Welcome and Opening Remarks
10:05AM	**Keynote Session:** Top 10 Priorities in IT Security for the County of Los Angeles and the Importance of Industry Standards
10:30AM	**Panel Session:** Advanced Persistent Threats and NIST SP 800-147 and NIST SP 800-155
11:15AM	Networking Break and Demonstration Showcase
11:30AM	**Panel Session:** Network Security, Critical Infrastructure and BYOD
12:15PM	Lunch and Demonstration Showcase
1:00PM	**Panel Session:** Protecting Content from Unauthorized Access
1:45PM	Closing Remarks and Raffle Drawing
1:55PM	Networking Break and Demonstration Showcase



TRUSTED COMPUTING:
DEMONSTRATION SHOWCASE

Absolute® Software

Securing Mobility

Absolute Software specializes in endpoint security, providing organizations with the ability to track, manage and secure devices regardless of user and location.

Absolute Secure Drive allows organizations to control all of the OPAL SEDs in their deployment. IT administrators can use a central administration console to remotely configure SEDs by device – administering users, authentication methods, policies, and system maintenance through to end-of-life.

Absolute Computrace provides a cloud-based console for IT administrators to remotely track and secure IT assets. Computrace persistence technology provides a consistent connection with each device so that IT can enforce compliance policies, identify computers that might be at risk, and take preemptive and reactive measures if a security incident occurs. Computrace includes Investigations and Recovery services for forensic intelligence relating to non-compliant or criminal activities.

Absolute Manage delivers authentic cross-platform IT asset management capabilities for PC, Mac, iOS, Android, and Windows Phone devices, all from a single console.

Absolute Software is recognized as a Visionary Vendor by Gartner in the Client Management Tools Magic Quadran

Practical Network Segmentation for Manageable Industrial Control Systems Security

Industrial Control Systems devices often make poor network citizens due to the lack of modern network security capabilities and poor integration with enterprise network configurations (lack of DHCP, non-standard protocols, etc.). There is a need to isolate the connectivity for these systems yet allow them to leverage common network infrastructure. Simplifying the full lifecycle management of multiple independent private isolated networks is a primary concern for enterprises with distributed ICS systems, including critical infrastructure. The SimpleConnect product line by Asguard Networks provides such a capability. SimpleConnect implements the IF-MAP Metadata for Industrial Control Systems Security specification, using IF-MAP 2.0 clients, to bring a new level of security automation to private connectivity. Juniper Networks MAG Series Junos Pulse Gateway running Junos Pulse Access Control Service acts as the Metadata Access Point (MAP) Server, which provides a centralized coordination service for the SimpleConnect MAP Clients.

Security for Dynamic and Ad-Hoc Networks

Mobile ad-hoc networks (MANETs) security faces various challenges different from other types of networks. Even in mobile networks the core infrastructure with all main nodes is static and only devices are mobile. In contrast, MANETs have no static core and all devices also take on the role of network nodes. Therefore, nodes can join the network without interaction with any central control entity and MANETs are subject to special attack vectors on several levels of the network infrastructure.

The presented approach uses TPM-based attestation for mutual checks between network nodes. The status and also the identity of a node can be verified via remote attestation whenever the node joins the network and then in regular intervals. Failure of attestation results in removing the link between the two nodes. Thus, links to a manipulated node will one by one be removed and similar to an immunological reaction the node will finally be removed from the network.

The approach has been implemented using a secure version of the B.A.T.M.A.N. routing protocol for MANETs. TPM-based attestation is integrated into the exchange of routing information in the B.A.T.M.A.N. protocol. The prototype shows that the integration of TPM-based attestation in MANET infrastructure can efficiently be done.

Further, in the running prototype the status of the network and the security associations are visualized as meta-data graph, using the IF-MAP TCG standard for meta-data access and the open-source IF-MAP server irond developed by University of Applied Science Hannover. The visualization nicely shows how infected nodes are excluded from the network link by link.

Plugging the Leaks: Security Automation

Enterprise and Government environments require a high degree of control over user access to critical applications and information resources. Integration of traditional network access control (NAC) with other security technologies, such as network leak discovery, can ensure protection of not only the network itself, but of the data the network contains and transports.

The problem of unauthorized, rogue, and insecure connections between the enterprise and the Internet continues to plague network and security managers. These "backdoors" provide a method by which the transport of critical data can circumvent security controls and "escape" the network. They also provide a method for outside entities to gain access to networks and their sensitive data.

This demonstration presents the automated enforcement of a network policy. Through the discovery of rogue or unauthorized network connections and the dynamic change of access privileges, attendees will see how TNC technologies can help protect the enterprise from these "backdoors".

TNC interfaces underlie this integration of network leak prevention and network access control:

- Lumeta IPsonar acts as a TNC Metadata Access Point (MAP) Client, detecting network leaks and publishing that information to the TNC MAP Server; other network devices can use that information to prevent unauthorized "backdoor" Internet connections that bypass network access controls.
- The Juniper Networks Junos Pulse Gateway, the policy management server at the heart of Juniper's Junos Pulse Access Control Service, acts as a TNC Policy Decision Point (PDP), providing user authentication and endpoint health checking, and provisioning policy to the network devices acting as Policy Enforcement Points (PEPs).
- The Infoblox Orchestration Server provides a highly secure and scalable Metadata Access Point (MAP) Server that acts as an active, real-time repository and distribution point for information to and from IF-MAP enabled devices and systems.

The TNC IF-MAP interface enables integration of network intelligence from additional security systems to add a behavioral consideration to the access decision.

Physical/Access Control Integration through IF-MAP

The Hirsch Identive Velocity™ physical security management system publishes physical access control events to an IF-MAP metadata server. IF-MAP compliant systems may subscribe to these events and use a person's physical presence in a building or area as a factor in that systems' operation. The initial use case is network access control, in which presence in a defined area becomes one factor the NAC system uses to grant or deny access to network resources. Since we publish these events in accordance with IF-MAP standards, any IF-MAP compliant device or system may subscribe to our events and transactions.

Data Protection in a BYOD World: 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 Registration Portal 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 Gateway, the policy management server at the heart of Juniper's Junos Pulse Access Control Service, acts as a TNC Policy Decision Point (PDP), consuming the user session information from the MAP Server, and provisioning policy to the network devices acting as Policy Enforcement Points (PEPs).

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

MITRE

Feasibility of High Security TPM Provisioning Processes in the Enterprise

Before TPMs can be used in an enterprise for machine identification, remote state verification (attestation), or authentication, we must establish trust in the hardware; and, in particular, in the TPM's Endorsement Key. (We call the establishing of initial trust, along with other necessary prerequisites for enterprise use of the TPM, "provisioning".) Although ideally these keys would be created and certified by the TPM manufacturer, this is not the case today; and in some enterprise environments, trust in the manufacturer's key handling is not necessarily a good assumption. In these cases, the enterprise must establish its own trust in each device it owns.

The best tools for provisioning TPMs today rely on software support, either local via the operating system, or remote via scripting. In either case, this means that we are establishing trust in our hardware by trusting the software; in both cases, a standard. While these approaches are highly time-efficient in deployed environments, they create a potentially significant security hole. In this demonstration, we show a prototype approach for high security TPM provisioning, discuss its advantages and disadvantages, and show its feasibility in enterprise settings when used in combination with existing enterprise processes.

Demonstration code will be available.

NCP
SECURE COMMUNICATIONS

Automated Security for Remote Systems

The increasing use of mobile devices or the integration of remote embedded systems introduces new threats to enterprise IT networks. While most of the well known security programs such as desktop firewalls, antivirus and harddrive encryption work pretty well for laptops, they are not available for mobile devices or remote VPN devices connecting to a central network. The only way to keep your network secure is by providing additional security on the central IT infrastructure and establishing trust in the devices used.

The problem is, most of today's security systems work isolated from each other and if they offer interoperability they do so only to a limited extent, which is insufficient to counter the new threats network security faces every day. TNC IF-MAP provides the possibility to interconnect different IT-security systems and provide an accurate representation of the health status of your IT network. The TPM Chip offers the perfect solution for establishing trust in a remote device by checking its health during bootup.

The demonstration shows the integration of different IT security systems like firewalls, intrusion detection and VPN working together in real time to counter threats emerging from a remote device or a smartphone. If the device should misbehave within the internal network this is detected and the device is limited in its access or shut off the network.

In the case of a remote embedded device the device additionally checks its health during bootup using the TPM and only establishes connection if the device image is correct.

NOKIA

Trusted Computing in Nokia Lumia

Nokia will showcase Trusted Computing technology, in the form of Windows Phone 8 secure boot on the Nokia Lumia 920. We look forward to sharing how the Nokia Lumia 920 delivers device integrity and provides a trustworthy foundation for supporting trusted applications and secure services.

We believe that Nokia Lumia smartphones built on Windows Phone 8 are on the leading edge of mobile security and are trustworthy for supporting the TCG published TPM Mobile Use Cases.

The TCG Seminar also provides a welcome opportunity to update any participants who are not familiar with the work of TCG 's Mobile Platform Working Group on the group's activities in developing specifications and certification processes.

SAMSUNG

Solid-State Self-Encrypting Drives: Where is your data tonight?

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.

wave®
The Trusted Computing Company

Leveraging the TPM to Provide Device-based Multifactor Authentication

Wave's EMBASSY Remote Administration Server manages the TPM to secure VPN and Microsoft DirectAccess and create a virtual smartcard for enterprise PC and tablet deployments alike. In this demo, a user logging into a secure website is prompted to enter a PIN for the TPM embedded in the laptop. Only a correct TPM PIN will allow access to the site. Global infrastructure has broadly supported smartcards as an authentication token—now the TPM is interoperable with that infrastructure. The device IS the smartcard.

World-leading Security Solutions by Wave, Delivered as Cloud Services

The Wave Cloud web application enables SMBs and large enterprises to quickly deploy self-encrypting drives (SEDs) and Trusted Platform Modules (TPMs). An innovative collection of web APIs enables organizations to extend Wave device security and authentication to enterprise apps and services.

Protect Your Organization against Endpoint Data Loss, Misuse or Theft

Safend Data Protection Suite protects organizations against the compromise or loss of data through its single-server, single-agent architecture. The Safend Data Protection Suite will discover, classify, protect, alert, log, block and encrypt your organization's most vital data whether devices are online or offline.

Using the TPM to Monitor the Security and Health of the PC Boot Environment

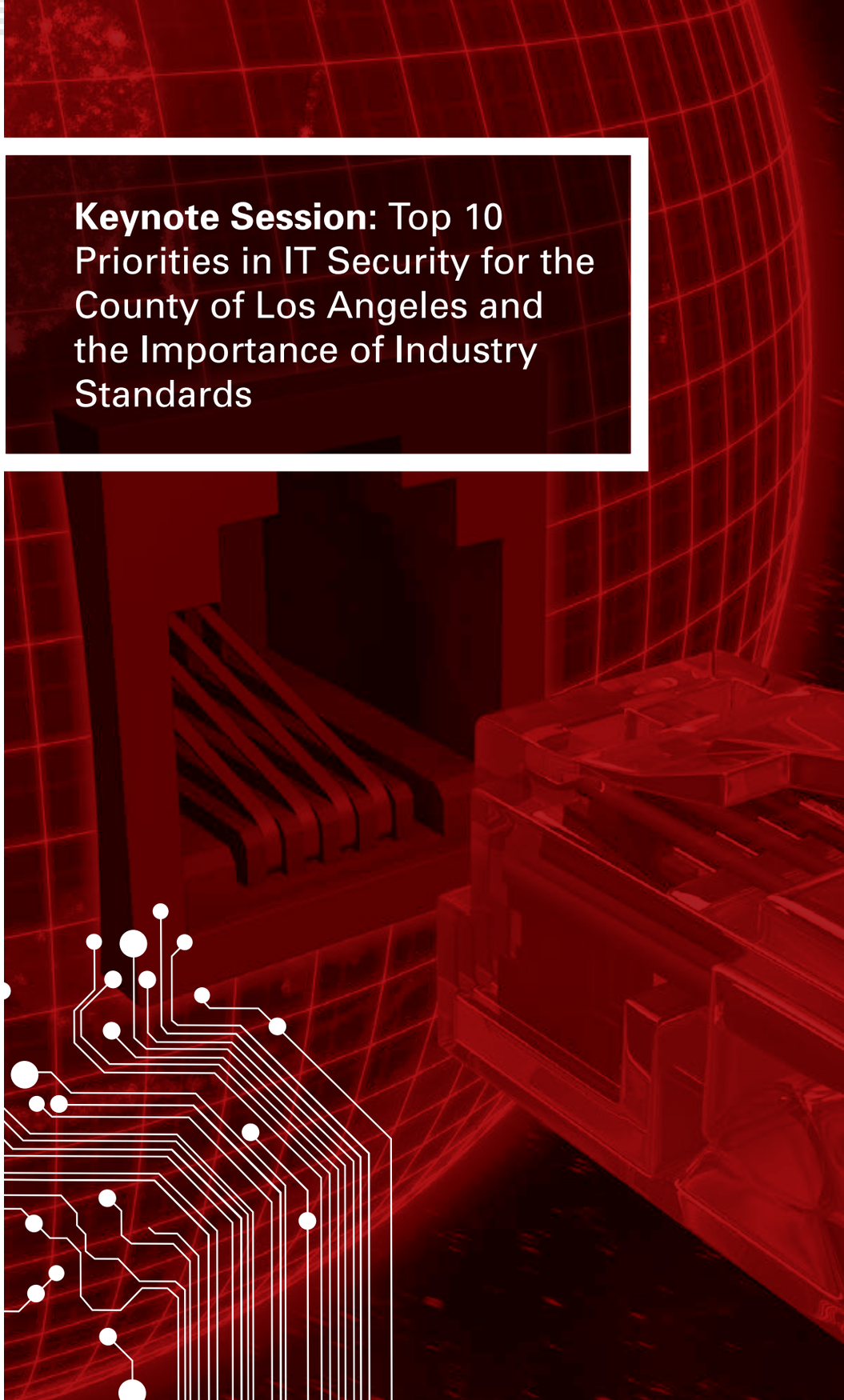
Wave Endpoint Monitor (WEM) determines the health of the endpoint based on TPM-secured Platform Configuration Register (PCR) measurements. In this demo, a "healthy" laptop is granted access to Wave Cloud. When WEM detects a suspicious change on the laptop – for example, by a firmware virus – the laptop is denied access to Wave Cloud.
Wave Endpoint Monitor (WEM) determines the health of the endpoint based on TPM-secured Platform Configuration Register (PCR) measurements. In this demo, a "healthy" laptop is granted access to Wave Cloud. When WEM detects a suspicious change on the laptop – for example, by a firmware virus – the laptop is denied access to Wave Cloud.

WINMAGIC®
DATA SECURITY

Managing OPAL-Compliant Drives in Windows 8 and UEFI with Secure Boot

With Windows 8 a new environment for security solution providers to utilize for PBA has arrived: UEFI. The Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. UEFI is meant as a replacement for the Basic Input/Output System (BIOS) firmware interface, present in all Windows-based personal computers.* When UEFI Secure Boot is turned on it means that the PBA software has to be 'signed' by Microsoft or the OEM so that it can be trusted to execute. With Secure Boot turned on computers are less susceptible to attacks on the booting process such as the Evil Maid attack.

Keynote Session: Top 10 Priorities in IT Security for the County of Los Angeles and the Importance of Industry Standards



Robert K. Pittman Jr., MPA, CISM

Chief Information Security Officer
County of Los Angeles

Mr. Pittman is the County of Los Angeles (County) Chief Information Security Officer (CISO), appointed by the Board of Supervisors' on September 16, 2008. Previously, he was second-in-command serving as the Assistant CISO and has over thirty years of Information Technology experience with the majority being in information security.

On February 29, 2012, he was awarded CSO of the Year by the Info Security Products Guide 2012 Global Excellence Awards presented in San Francisco, CA.

Mr. Pittman is currently completing his Doctoral degree in Public Policy at the University of Southern California (USC) targeting May 2013 graduation with his field of study being organizational behavior and culture. He is the recipient of Academic Honors' Society awards: Phi Kappa Phi (invitation only) and Pi Alpha Alpha.

Panel Session: Advanced Persistent Threats and NIST SP 800-147 and 800-155

Paul Roberts

Editor In Chief
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. Most recently, Paul edited Threatpost.com, the Kaspersky Lab news blog and was a Security Evangelist for Threatpost™ corporate parent. Prior to that, he spent three years covering the enterprise IT security space as a Senior Analyst in The 451 Group™ Enterprise Security Practice, where he wrote about trends and technology developments in the enterprise security market, with a concentration in endpoint security. Paul has held positions as an editor for Infoworld.com and a senior writer at Ziff Davis' eWeek.com.

Frank Molsberry

Technologist Office of the CTO
Dell

Frank Molsberry is a Technologist in Dell's Office of the CTO with a focus on Security Architecture and Technology. In that role he supports the current engineering efforts for incorporating security hardware and software into Dell products, works with the various security technology companies to evaluate and influence current and planned offerings, and participates with standards organizations such as the Trusted Computing Group (TCG) in the definition of future security standards.

Prior to his current position, Mr. Molsberry helped found Dell's Workstation Architecture and Development team and, more recently, the Enterprise Architecture and Technology Group. In all, he has over 25 years of management and engineering experience in advanced system software development and PC system architectures. Frank has a Bachelor's degree in Computer Science from the University of Texas at Austin and has a number of patents in the area of computer security. He does regular customer briefings on emerging technology trends.

Stacy Cannady

Distinguished Technologist
Digital Management, Inc

Stacy Cannady is a Distinguished Technologist with Digital Management, Inc (DMI), and a member of the Trusted Computing Group's Embedded Systems Work Group.

Stacy has worked in the field of trusted computing for ten years. As a Subject Matter Expert in trusted computing, his responsibilities require an in-depth understanding of the trusted computing market, including advances in hardware and software security as well as vendor and customer market dynamics.

Prior to his work with DMI, Stacy was responsible for marketing leadership for trusted computing at IBM and at Lenovo. At IBM, he played a principal role in making the TPM standard equipment in ThinkPad and ThinkCenter PCs. This created competitive pressure in the PC market and led to broad market acceptance of the TPM as standard equipment in enterprise-class PCs.

Stacy was also responsible for the security product strategy for IBM's PC Division and for Lenovo for eight years. This strategy required subject matter expertise in firmware security, biometrics, smart cards, identity management, encryption and access control. Additionally, at Lenovo, he was also responsible for incident response and served as Privacy Manager for the Software & Peripherals Business Unit.

Sunil Gottumukkala

Principal Lead Program Manager
Microsoft

Sunil Gottumukkala is a Principal Lead Program Manager in the Windows Security and Identity team at Microsoft. Sunil's current focus is on Isolation Platform and Platform Integrity for Windows. During his 12 years at Microsoft, Sunil worked on many different aspects of Security ranging from Access Control, Authentication Protocols to Hardware based security and shipped numerous Operating Systems and Frameworks. In his spare time, he loves spending time with his two daughters and playing basketball and volleyball.

Robert Thibadeau

Chief Scientist
Wave Systems Corporation

As Chief Scientist for Wave, Dr. Thibadeau serves as a principal advisor to the CEO on scientific matters, contributes to the long-term strategic vision of the company, and performs technical research. Dr. Thibadeau is responsible for identifying, recommending and developing new and innovative technologies that ultimately lead to competitive advantages in the marketplace through the company's products and services.

As Wave's primary interface to the scientific community, he is often called upon to share his expertise at conferences and industry events, speaking on advancements in security, encryption and storage. Dr. Thibadeau is an active member of the American Bar Association's eDiscovery and Digital Evidence Committee and co-authored the Data Breach and Encryption Handbook.

Prior to joining Wave in February 2010, he was Chief Technologist at Seagate Technology, LLC. There he pioneered a new form of hardware-based encryption, known commercially as self-encrypting drives. Dr. Thibadeau was also the Chair of the Storage Workgroup in the Trusted Computing Group, and a founding director of the Robotics Institute at Carnegie Mellon University. Dr. Thibadeau holds a number of patents. Dr. Thibadeau holds degrees from Emory University and the University of Virginia.

Panel Session: Network Security, Critical Infrastructure and BYOD

Phil Schacter - Moderator

Managing Vice President
Gartner

Philip S. Schacter is team manager for security and risk management strategies (part of the Burton Group acquisition). His focus of research is network security, security architecture, security governance, network identity and policy systems, remote work infrastructure, and security for tablets and other BYOD devices.

Steve Venema

Associate Technical Fellow
The Boeing Company

Dr. Steven Venema is an Associate Technical Fellow in the Networked Systems Technology organization of Boeing's Research and Technology (BR&T) business unit. He has extensive experience with robotics and control systems, network systems architecture, wireless security protocols and real-time embedded systems.

His current activities at Boeing include the development of new standards-based communications, network security, mobility and location protocols and services, with a focus on implementations for the Boeing enterprise and its customers. As part of his duties, he is actively participating in public standards development activities at the ISA (ISA100.15 WG), the Trusted Computing Group (TNC WG), and The Open Group (the Security Forum and the Real Time Embedded Systems Forum).

Dr. Venema holds both MS and PhD degrees in Electrical Engineering and also serves as an affiliate associate professor at the University of Washington.

Phyllis Lee

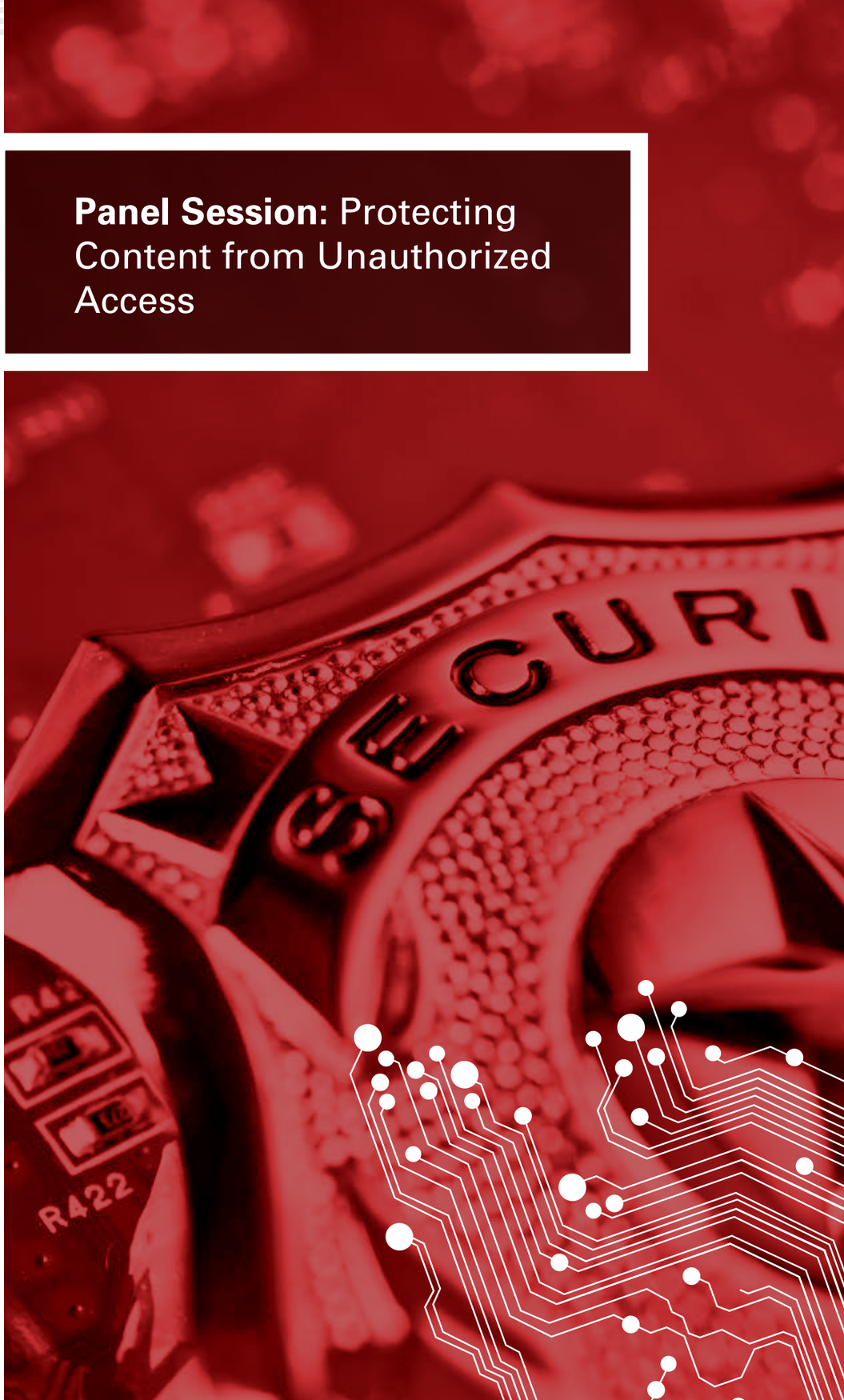
IAD Security Automation
Program Manager
National Security Agency

David Waltermire

Specification Architect, Security Automation Program
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.

Panel Session: Protecting Content from Unauthorized Access



Eric Ogren - Moderator

Founder
Ogren Group

Eric Ogren is the founder and principal analyst of the Ogren Group. Eric's background features over 25 years of software engineering, technology marketing, and industry analyst experiences, including more than 15 years in enterprise security. The lessons learned in executive roles at leading vendors such as OKENA and RSA Security, and in working with a variety of vendors while at the Yankee Group, contribute to pragmatic perspectives on market trends, vendor messaging and positioning, and customer decision criteria.

Hussein Syed

Director of IT Security
Barnabas Health

Hussein Syed has served in several different roles in IT organizations. His current position is the Director of IT Security for Barnabas Health in NJ. Hussein has over 15 years IT experience of which 10 years has been in IT Security. He has a thorough understanding of health care business enablement (both clinical and business-driven) focusing on secure practice and compliance. In his role he has to remain technical and understands its impact on risk, workflow, patient care/satisfaction and physician/clinician enablement. Hussein has also participated in Gartner, CISO Summit, and NJHIMMS roundtable sessions on HIPAA/ HITECH and IT Security.

Clain Anderson

Director of Software
Lenovo

Clain Anderson has thirty years' experience with four major PC companies and has played a pivotal role in bringing new products and technologies to the marketplace.

After completing an MBA at Utah State University, his experience base was established as a computer systems analyst for Deloitte and as an IT project leader for HP. While at Deloitte, Mr. Anderson passed the Certified Public Accountancy examination in a single attempt and was licensed as a CPA beginning in 1980.

Clain Anderson led marketing efforts at Hewlett-Packard for HP calculators, including the market launch of the world's first symbolic math calculators. He held increasing levels of responsibility at HP and was a wireless evangelist for handheld and notebook PCs. He spoke at numerous wireless forums, trade shows, and expert panels.

Mr. Anderson joined Digital Equipment in 1994 as Product Marketing Manager, and managed the launch of the Digital HiNote mobile line. He advanced to PC Channel Marketing Manager and later to Marketing Director for the Digital mobile PC line. He worked for Compaq briefly after the acquisition of Digital, at which time he joined IBM.

Over several years with IBM and then Lenovo, Clain Anderson led the product management of key new technologies for Thinkpad and ThinkCentre PCs, including new disk imaging tools, the industry's first preloaded system recovery tool, the first mobile personal computers with a security chip (Trusted Platform Module), and the world's first notebook computer to combine fingerprint biometric capability with a built-in security chip. He is

currently Director of Software for Lenovo responsible for a portfolio of unique software solutions including Landesk, Absolute Software, WinMagic, Adobe, and Sophos.

Mr. Anderson is a Certified Information Systems Security Professional (CISSP), a past member of the American Mathematical Society, and served on the boards of the Trusted Computing Platform Alliance and the Trusted Computing Group.

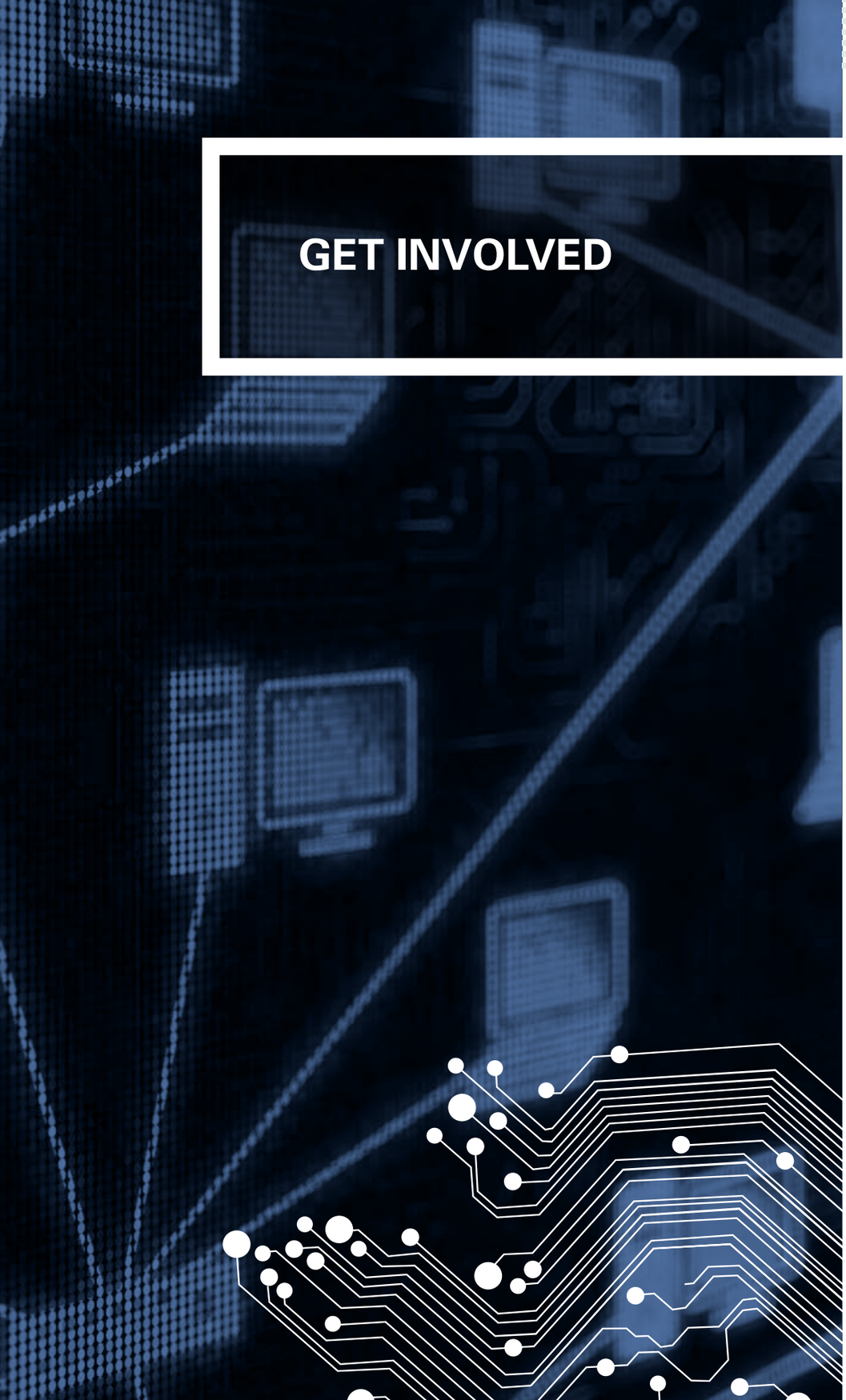
Jon Rolf

Technology Lead
National Security Agency

Michael Willett

Storage Security Strategist
Samsung

Dr. Michael Willett received a Bachelor of Science degree from the US Air Force Academy (Top Secret clearance) and a Masters and PhD in mathematics from NC State University. After a career as a university professor of mathematics and computer science, Dr. Willett joined IBM as a design architect, moving into IBM's Cryptography Competency Center. Later, Dr. Willett joined Fiderus, a security and privacy consulting practice, subsequently accepting a position with Wave Systems. Recently, Dr. Willett was a Senior Director at Seagate Research, focusing on security functionality on hard drives, including self-encryption, related standardization, product rollout, patent development, and partner liaison. Currently, Dr. Willett serves as a consultant on the marketing of storage-based security. Dr. Willett also chairs the Privacy Management Reference Model Project of the ISTPA, which has developed an operational reference model for implementing privacy requirements. Presently, Dr. Willett is working with Samsung as a storage security strategist, helping to define their self-encryption strategy across Samsung's portfolio of storage products.



GET INVOLVED

Trusted Computing Group Mission

The 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.

Why Join Trusted Computing Group?

Membership in the Trusted Computing Group (TCG) is your key to participating with fellow industry stakeholders in the quest to develop and promote trusted computing technologies. The organization's focus on research, standards writing, published studies and continuing education needs your input. By joining TCG, you will help influence both developers and enterprise end-users of trusted computing technology.

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


TRUSTED
COMPUTING GROUP™
Celebrating 10 Years