National Institute of Standards and Technology
U.S. Department of Commerce

Request for Information

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Docket Number: 130208119-3119-01

March 15, 2013

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
Phone 413-243-1600

wave®
The Trusted Computing Company

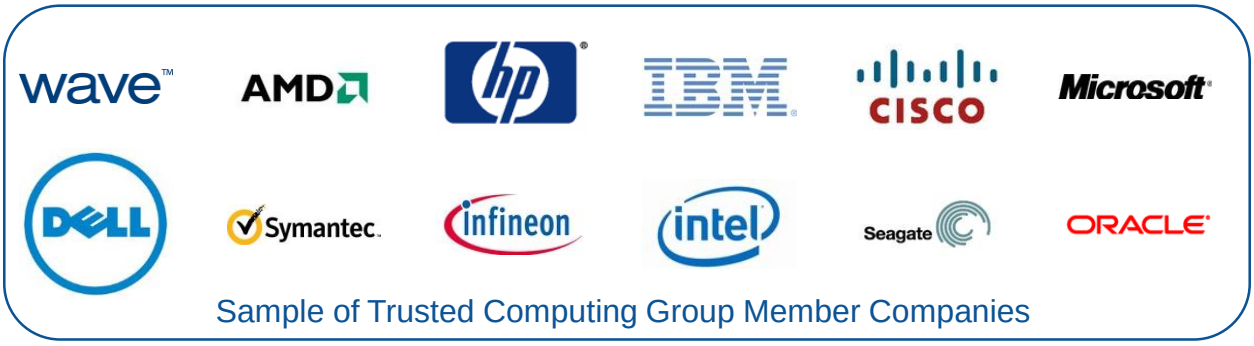
Abstract

As NIST looks ahead to solve the current and ever-growing threat of malicious cyber activity by recommending a resilient cyber framework Wave Systems Corp. believes a large part of the answer has already been proven on billions of devices. Robust and stable standards have been developed by the computer industry and others including NIST. The foundation for this new security is already deployed in about a billion computers globally and the numbers are accelerating with Microsoft compliance requirements for much of Windows 8 including tablets and smartphones.

The fundamental cyber framework solution should be based on three key components:

1. An access model built on secure, hardware-rooted device identity solves the majority of cybersecurity challenges. Clearly the computer/user access paradigm today is not working well; so step one is to use a proven model with a successful track record on over 4 billion devices.
2. The integrity of the computer itself to execute is core programs has to be trusted in the cyber framework. Only hardware, chips on the motherboard, can be trusted to provide the foundation for trusted execution of the BIOS, MBR and device drivers where the most sinister and secret cyber-attacks occur.
3. Bi-lateral trust of the connection between an endpoint and the network needs to be based on the inherent security of hardware.

The computer industry recognized the looming cyber threat in 2003 and has delivered a solution; an industry-led, open standards-based solution: Trusted Computing. The Trusted Computing Group was formed and today involves nearly all the major computer and component manufacturers.



Sample of Trusted Computing Group Member Companies

wave®
The Trusted Computing Company

History

Computer security breaches and attacks have been around since before the dawn of the personal computer. The cyber security concern today is different because of our dependence on computers as a core element of our infrastructure and systems are no longer isolated enclaves, but interlinked through the web.

A good starting point is to look at other massive networks that have successfully evaded cyber-attacks. The cellular and cable TV operators have always had a compelling business case to prevent fraudulent use of their networks. Cellular and cable companies quickly discovered that hardware-based device identity built into the mobile phone or cable box virtually eliminated fraud. Computers on the other hand evolved very differently. Computers historically were manufactured by a wide range of companies with a primary focus on price and functionality – security was not a primary concern. As attacks grew and trust eroded, security concerns escalated.

In the early years of the cell phone industry, cell phone numbers were hijacked by criminals. Those numbers were sold, thus permitting people to make bogus cell phone calls which were billed to the rightful cell phone owner. Today, with over 4.6 billion users worldwide, cell phone hijacking is unheard of. The cell phone industry recognized the problem and created an international standard to securely and uniquely identify each cell phone. Built into every phone (or its SIM card) is an Electronic Serial Number which is securely part of each call. Imagine if you had to enter your user name and password every time you placed a call. Or worse yet, every time you changed cell phone towers.

The cable TV industry faced a similar challenge in its early days. Bootleg cable boxes could be purchased and people could pirate service without paying for it. Fast forward to today where cable boxes have a unique serial number and pirated service has virtually evaporated. Device identity permits subscriber-based cable services, which, like cell phones, eliminates the requirement to enter user name and password every time you change channels.

Imagine only entering your user name and password only once, when you start your computer, and then just using the Internet …. Securely.

Recognizing these security concerns were eroding confidence, Microsoft chairman Bill Gates announced in early 2002 a company-wide "Trustworthy Computing initiative," which aimed to incorporate security into every aspect of software development at the company. Then in 2003, the Trusted Computing Group was formed by the computer industry to address growing concern and know vulnerabilities. The industry experts knew that a foundational security element based in hardware was required. The result was the industry standard for the Trusted Platform Module (TPM). Microsoft accelerated deployment by requiring TPMs in all computers shipped with Enterprise or Ultimate versions of Visa and later Windows 7. With Windows 8, deployment accelerates as a broad range of platforms, including computers, tablets and smartphones require TPMs. TPMs provide a number of critical components to security which provide a foundation for the three key components listed above: unique device identity; storage for keys, certificates and critical measurements about the pre-boot environment (BIOS Integrity); and cryptographic functions.

Another massive network with virtually no fraud is iTunes. Apple has effectively demonstrated the effective use of hardware-based device identity. For a moment let's consider iTunes. Only your devices get to use your iTunes store of songs, movies and apps. Virtually no fraud in iTunes and it likely cost Apple less than $5 per device to manage a network of over 100 million devices. Your iDevice logs into iTunes and you get your updates and that new hit song. Simple, cost-effective, resilient, private and secure – yes it checks all the boxes. iTunes works incredibly well because the foundational element is a hardware-based device identity in the endpoint.

wave®
The Trusted Computing Company

Trusted Computing Group

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. TCG is an international industry standards group with over 150 members representing leading chip, computer, software companies as well as governments and others. TCG represents over ten years of collaborative development of open, published standards related to computer security. Some of the TCG standards are also available in ISO.

The TCG develops specifications amongst its members. Upon completion, the TCG publishes the specifications for use and implementation by the industry.

The TCG publicizes the specifications and uses members' implementations as examples of the use of TCG Technology. The TCG is organized into a work group model whereby experts from each technology category can work together to develop the specifications. This fosters a neutral environment where competitors and collaborators can develop industry best capabilities that are vendor neutral and interoperable.

Today the Trusted Computing Group (http://www.trustedcomputinggroup.org/) has issued and continues to work on standards addressing a broad range of computer security issues, including;

- Authentication
- Data Protection
- Network Access & Identity
- Cloud Security
- Mobile Security

The open standards approach taken by TCG means that multiple manufacturers create chips, disk drives, software and other components according to openly published specifications creating a low cost solution.

As NIST seeks public-private partnerships in developing the Cyber Framework it should keep in mind the computer industry has already invested over a billion dollars in developing and deploying the hardware, firmware and related software to support the Trusted Computing paradigm. At the same time, industry, government and consumers have already invested another billion dollars when purchasing computers and now tablets and smart phones with Trusted Computing built in.

wave®
The Trusted Computing Company

Government Requirements for Trusted Computing

Like industry, the US Government has recognized the value of hardware-based security as embodied in the Trusted Computing model. The following provides a few examples of Trusted Computing being included in government memoranda or specifications:

1. July 3, 2007, DoD CIO John Grimes memorandum required all computers, where possible, include a TPM for future device authentication.[1]

2. April 8, 2008, US Army LandWarNet NetOps Architecture (LNA) for Trusted Platform Module provides extensive details on the use of TPMs[2] summarizing the information contained in the Army LNA. This document advises that most system administration functions of the TPM are required for LandWarNet operations. This document also spells out device authentication requirements under sections for Identity Management and TPMs.

   > **Identity Management**: …***Permits only users, components/devices and applications with the proper/verified credentials*** (as defined by the information provider) to access information or services on the LandWarNet or Global Information Grid. Interacts with Defense Information Systems Agency and approved Commercial certificate registries to obtain validated certificates.
   >
   > ***Trusted Platform Management: Enables remote/local configuration and management of Trusted Platform Management modules on computing platforms. Allows authorized administrators to take ownership/control of the Trusted Platform Management chip, enabling activation, ownership, and decommissioning of the module, as well as archival of recovery keys.***

3. The May, 2009, White House "Cyberspace Policy Review" points out;

   > **Resiliency Requirements**
   >
   > The infrastructure must be resilient against physical damage, unauthorized manipulation, and electronic assault. In addition to protection of the information itself***, a risk mitigation strategy for cyberspace must focus on the devices used to access the infrastructure***, the services provided by the infrastructure, supporting elements of the networks, and all means of moving, storing, and processing information. The strategy also must include prevention, mitigation, and response against threats to or subversion of the people who operate and benefit from the infrastructure, the processes that run or take advantage of the infrastructure, and the supply chains used to build and maintain the infrastructure.[3]

4. NIST SP 800-155 (December 2011) - BIOS Integrity Measurement Guidelines (Draft)[4] outlines the security components and security guidelines needed to establish a secure Basic Input/Output System (BIOS) integrity measurement and reporting chain. BIOS is a critical security component in systems due to its unique and privileged position within the personal computer (PC) architecture.

---

[1] July 3, 2007 John G. Grimes, DoD CIO Memorandum – DoD Policy (4)
[2] April 8, 2008 US Army US Army LandWarNet NetOps Architecture for Trusted Platform Module
[3] Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure, Executive Office of the President, May 29, 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[4] [NIST-SP800-155] Regenscheid, A., and Scarfone, k., "NIST Special Publication 800-155: BIOS Integrity Measurement Guidelines (Draft)", NIST, December 2011, http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf

Outdated or malicious BIOS could allow or be part of a sophisticated, targeted attack on an organization - either a permanent denial of service (if the BIOS is corrupted) or a persistent malware presence (if the BIOS is implanted with malware).

> Client computers such as desktops and laptops rely on the Basic Input/Output System (BIOS) to initialize their hardware during boot. The BIOS is firmware, and it can be configured. If the BIOS code or configuration is altered from the intended state, either maliciously or accidentally, the desktop or laptop may experience losses of confidentiality, integrity, and availability, including system instability, system failure, and information leakage. Also, the desktop or laptop could be vulnerable to more elaborate attacks such as covert monitoring, and it could be used as a stepping stone for attacking other systems***. These consequences underscore why it is so important to detect changes to the BIOS code and configuration— and this can be accomplished by measuring and monitoring the integrity of the BIOS.***
>
> - Provide the hardware support necessary to implement credible Roots of Trust for BIOS integrity measurements.
> - Enable endpoints to measure the integrity of all BIOS executable components and configuration data components at boot time.
> - Securely transmit measurements of BIOS integrity from endpoints to the Measurement Assessment Authority (MAA).
>
> A Hardware Roots of Trust (RoT) is preferred over a Software RoT since it can be demonstrated to behave in an expected manner in a significantly higher percentage of attack scenarios.

5. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0, December 2, 2011, addresses the importance of verifying the identity of devices;

> In addition to complex cyber and physical security threats, the Federal Government faces significant challenges in being able to carry out its mission activities in a manner that fulfills the needs of its business partners and the American public and appropriately leverages current information technology capabilities to enable electronic service delivery. ***These challenges lie in being able to verify the identity of an individual or non-person entity (NPE) in the digital realm and to establish trust in the use of that identity in conducting business.*** As a result, strong and reliable ICAM capabilities across the entire Federal Government are a critical factor in the success of all government mission work. A common, standardized***, trusted basis for digital identity and access management within the federal sector is needed to provide a consistent approach to deploying and managing appropriate identity assurance,*** credentialing, and access control services. The approach must also promulgate implementation guidance and best practices, build consensus through government-wide collaboration, and modernize business processes to reduce costs for agency administration.[5]
>
> The FICAM goes on to point out:
>
> ICAM comprises the programs, processes, technologies, and personnel used to create trusted ***digital identity representations of individuals and NPEs, bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources***.
>
> and,
>
> Identity management includes the processes for maintaining and protecting the identity data of an individual over its life cycle. Additionally, many of the processes and technologies used to

[5] http://www.idmanagement.gov/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202.pdf page 1

manage a person's identity may also be applied to NPEs to further security goals within the enterprise.

6. US Army - NETCOM Technical Authority (TA) Implementation Memorandum for Army End-User Computing Environment, Version 2.0, 19 June 2012 (NETC-G-0412-002-E-STD) FOUO.[6] Additional information about this NETCOM requirement can be found at https://chess.army.mil/content/files/Authority_(TA)_Implementation_Memorandum_For_Army_End-User_Computing_Environment.pdf

The recently issued US Army NETCOM TA provides very specific requirements for the use of TPMs to increase security of the Army network. The following section paraphrases some of the important information in the TA. To request a copy of the TA please contact US Army Netcom.

This TA identifies specifications for hardware, operating systems, software and configurations that the Army needs in order to create a secure, standardized computing environment for end-users.

All common end-user computing environments operated by the Army, including both the Nonsecure Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet), are required to follow this TA.

The TA defines the common end-user computing environments as those including a range of devices, from zero/thin client to workstation, laptop, tablet, slate and virtual desktop infrastructure solutions.

Microsoft Windows recommended Hardware Configuration for Workstation, Desktop, Laptop, Lightweight/Tablet/Slate all require TCG TPM V1.2 with Core Root of Trust Measurements. When procured, the TPM will be activated and Army ownership established. This will enable TPM functionality like Microsoft BitLocker or machine identity without necessitating any touch from IT.

Currently, Windows-based end-user environments require the use of vendor-provided software to manage TPM and self-encrypting drive (SED) passwords.

Embedded into the motherboard of the computer, the TPM is a crypto-processor security chip that roots storage of platform authentication credentials in the hardware of the machine itself. This TPM functionality allows the platform to authenticate with a high degree of assurance. The TPM also can store measurements on the state of the platform that allow a high degree of trust in the platform's integrity. Furthermore, Microsoft makes use of the TPM as a management tool for their full disk encryption solution, BitLocker Drive Encryption (BDE). The TA cites a requirement that all new machines purchased must include an activated TPM. It further states that this will eliminate the need for touch labor when the TPM is being used in the ways set forward by the TA.

The Trusted Computing Group describes what a Trusted Boot process looks like in TPM-enabled system based on behavior of the TPM in the boot process. Using the TPM in this way ensures the BIOS and operating system have not been tampered with. The TPM can be used in this way to measure the BIOS and critical operating system files in pre-boot before allowing them to load. If an anomaly in the measurements is identified, the trusted boot process prevents the file from executing and alerts the administrator. These alerts can be used as IA events when coupled with the correct management systems.

Authenticating a platform to the network can be accomplished by the open-standards 802.1x solution. This solution is supported by the major networking OEMs and has been incorporated into all Army-approved operating systems. Machine identity must be verified in order to use 802.1x, as this is a piece of the network connection process. ***To ensure that this function supports all of DoD as well as Army travelers, the credential used to identify the platform needs to be independent of*** the Active Directory forest the machine belongs to. To satisfy this requirement, DoD PKI non-person entity (NPE) certificates will be used within the Extensible

[6] US Army - NETCOM Technical Authority (TA) Implementation Memorandum For Army End-User Computing Environment, Version 2.0, 19 June 2012 (NETC-G-0412-002-E-STD) FOUO

Authentication Protocol Transport Level Security (EAP-TLS) standard. ***Protection of these NPE certificates will be based on TPM functionality***. The Trusted Computing Group's Trusted Network Connect specification outlines the foundation for the standards used in this process.

The TA also provides requirements for Trusted Computing Opal (SED) standard drives.

SSDs are designed in such a way that renders all software wipe processes ineffective. ***SSDs purchased by the DoD will perform hardware encryption in accordance with the OPAL standard.*** Passwords, both user and recovery, will be set and escrowed for all SEDs. SEDs will be required on all new mobile devices purchased.

7. The National Security Agency has sponsored two Trusted Computing Conferences and plans for another conference again in 2013.

Threats and Recommendations

As NIST develops the Cyber Framework concrete use cases may serve to bring solutions into focus from theory to reality. Here we highlight three scenarios of clear and present cyber security threats and we will show how Trusted Computing is solving these vulnerabilities.

Cyber Threat 1: Attacks from Outside Computers

Today networks are attacked primarily from outside agents many times each minute. They seek to gain access by stealing user login information. A common example is phishing but many other techniques are used. By limiting network access to only known computers we substantially eliminate a major vector and vulnerability. Being able to impersonate a user by providing their username, password, city of birth, mother's maiden name, or any other phishable information, is of no use when the network recognizes hardware, by the hardware's immutable identity. Imagine for a moment that a nuclear reactor installation has deployed 500 computers and only those specific computers are allowed on the network. How much safer would we be?

When we consider DHS US CERT's list of Threat Sources, 90% of the cyber threats are from the outside.

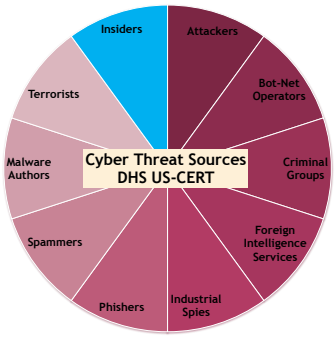


Figure 1: DHS US CERT - Threat Sources

Most computer networks have failed to recognize the first line of defense is to allow only known, healthy and trusted devices on the network. Most computer networks are primarily concerned with who is on the network, but they should first be concerned with what is on the network. By implementing the paradigm of "only known devices," the Cyber Framework will create a new outer perimeter of security which is augmented by all the other existing security, but now focused on only its own devices. "Only known devices" should be the foundation for the security architecture. Systems architects will need training or advise to understand and incorporate this new paradigm of trusted devices.

The TPM provides a hardware-rooted device identity which can be used to ensure "only known devices" are allowed access to a network, server, Cloud service or any other restricted resource.

Wave has enterprise management software today to turn on, enable and manage TPMs delivering device identity for corporations and government agencies. It has been tested and deployed in scale.

Wave is also deploying a device attribute service, in conjunction with the NIST NSTIC program, which leverages the unique device identity to protect consumers and business transactions while increasing privacy. This service works with virtually all devices even those that lack a TPM. Wave's device attribute service, Nodes, provides information to the relying party about the level of security of the device identity since not all devices today have trusted hardware components.

Recommendation:

NIST should make "Only Known Devices" a core principle of the Cyber Framework. This simple yet powerful paradigm is proven on billions of mobile devices and is already deployed on about a billion computers based on open industry standards.

Cyber Threat 2: Rootkit Attacks

The really scary cyber-attacks are the ones where you don't even know it happened or they render the machine unusable. Three recent published attacks rise to that level of concern: Stuxnet, Aramco and South Korea. All three have one thing in common these were root kit attacks.

Today more than ever before agencies and industry are faced with an insidious Advanced Persistent Threat (APT). Attacks by hackers and even foreign governments are migrating to a system level much closer to foundational hardware. These attacks, such as those planted by rootkits, occur before the operating system loads often targeting the system BIOS and Master Boot Record. Rootkits are often invisible to current anti-virus and anti-malware solutions because they have the highest levels of privileges (see Figure 2). Designed to steal information to achieve economic, political and strategic advantage or to disrupt or render personal computers unusable these APT attacks may also cause government and critical infrastructure to be offline for extended periods of time. APTs can establish and maintain a concealed occupying force in their target's environment, a force attackers can call on at any time.

For many years, anti-virus products protected computers from most network threats but APTs' sophisticated hacking attacks are more serious and harder to solve as they target the PC boot environment. Another reason the computer industry developed TPMs is that they foresaw the evolution of such threats and designed an industry standard hardware solution to fight them.

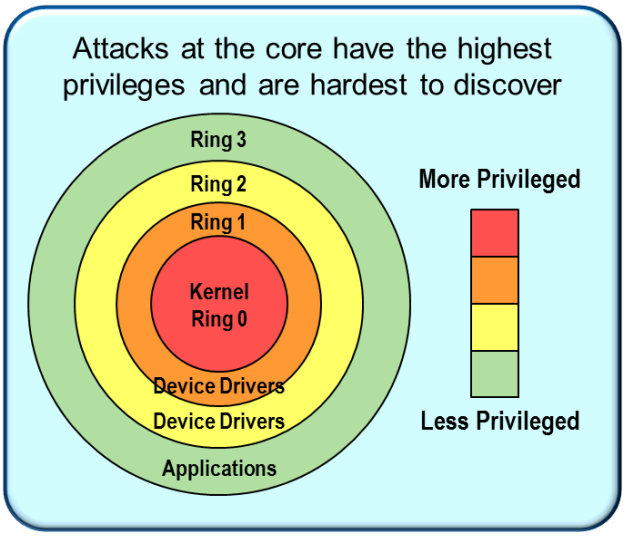


Figure 2: Privilege rings for the x86 (protected mode)

"APTs facing enterprises today are more complex, nefarious and sophisticated than ever before," said Richard Stiennon, Chief Research Analyst at IT-Harvest and author of Surviving Cyberwar. "Malware hiding in a device's BIOS will go undetected by traditional anti-virus programs operating at the OS level, creating a strong need for a solution that can identify an attack as it happens."

NIST has recognized the value and importance of protecting the BIOS by spelling this out in detail in two recent publications: SP 800-147 and SP 800-155 (draft). The DoD has recognized this threat by issuing a CIO directive to comply with 800-147 and left open for revision when 800-155 is completed.

NIST SP 800-147 (April 2011) - BIOS Protection Guidelines[7] provides security guidelines for preventing the unauthorized modification of BIOS firmware on PC client systems.

Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS's unique and privileged position within the PC architecture.

It is crucial that the organization institute a mechanism for identifying, inventorying, and tracking the different computer systems across the enterprise throughout their life cycle.

Computers with TPMs have a built-in ability to securely store measurements taken of the pre-boot environment. These measurements can be reported and centrally compared to previous "known-good" or "Golden" measurements. The storage areas in the TPM are called Platform Configuration Registers (PCRs) and they store the hash of critical start up values. Reporting of PCR measurements uses public key cryptography guarded by the TPM, called "quoting," to guarantee that the measurements are not spoofed. The PCR data and other TPM log information can then be used to make access decisions or analyzed in bulk to search for anomalous platform behavior.

Wave's approach is rooted in hardware-based technologies, the effects of rootkits and other malware can be spotted before the OS even starts. Wave Endpoint Monitor (WEM) allows IT to utilize the hardware security already invested in by industry and government to ensure PC health from the start of the boot process while creating a higher level of trust in the endpoints. WEM has been tested and deployed within the federal government.

In addition to the Trusted Computing Group's (TCG) TPM specifications, the TCG has also published the Opal Self-Encrypting Drive (SED) standard. Wave is the first to demonstrate how SEDs, when combined with Wave's EMBASSY® software, can detect a malware pre-boot attack and neutralize it before it has a chance to do any damage. This is made possible since during the SED initialization process Wave software securely installs a pre-boot environment that runs on the main processor during pre-boot. Also, because this low-level code is remotely managed by Wave's enterprise server software, security policies can be enforced in pre-boot. After the TPM completes its measurements, but before the OS loads, the Wave pre-boot code can detect anomalies and repair them under centralized IT policy control.

Recommendation:

NIST should complete SP 800-155 and issue this standard.

NIST can reduce a major vulnerability to devastating attacks by recommending as part of the Cybersecurity Framework that industry and government implement BIOS integrity and machine health based on hardware that they already own.

Cyber Threat 3: Unsecure Networks

The reality of today's go-everywhere do-everything world is that computers must gain access to information anywhere, anytime. Currently two popular methods are commonly used to facilitate access to network resources: Virtual Private Networks (VPN) and wireless network access (802.1x). These methods are well understood and generally considered safe. The reality is the opposite: security of VPN and wireless is substantially at risk because certificates with software-based keys are used to authenticate the endpoint.

[7] [NIST-SP800-147] Cooper, D., Polk, W., Regenscheid, A., and Souppaya, M., "NIST Special Publication 800-147: BIOS Protection Guidelines", NIST, April 2011, http://csrc.nist.gov/publications/PubsSPs.html#800-147.

In 2010, NSA demonstrated how simple and inexpensive it is to hack into a VPN or wireless network using tools from the Internet. As a result, NSA now recommends that VPN and wireless access be hardened using certificates whose private keys are bound to hardware, not files on a disk drive. We all know people who have used jail-break software to move the soft VPN/wireless key from one machine to the next.

Deployment and migration to hardware-based network access certificates is fast and users will be unaware of, but thankful for, the improved security. This provides hardware-based authentication to VPNs and wireless networks while removing the potential of users sharing or thieves acquiring software-based keys.

PwC – Real world experience deploying TPM for VPN and wireless security

PricewaterhouseCoopers (PwC) is a leading global tax and advisory service firm with over 160,000 employees. PwC leveraged the power of TPMs to improve their network security globally. PwC shared the following key points about their global deployment in a presentation at the RSA conference in 2011.

- The solution needed to be end-user hassle-free and low cost
- After checking PC inventory, virtually all PwC PCs had TPM 1.2 – no incremental hardware cost
- No external shipping costs with TPM versus other hardware-based authentication methodology
- No "lost" TPMs as you have with other external devices – external device loss rate can be as high as 15%
- Not including logistical, lost, damaged and stolen device costs: Smartcards were twice as expensive as TPM; USB token three times as expensive as TPM
- TPM protected against theft of private keys on PCs using "Jailbreak" software
- Four people in eight months deployed TPM-secured access to approximately 85,000 end users

Wave EMBASSY® Remote Administration Server (ERAS) has tools which system administrators can use to remotely turn on, enable, activate and take ownership of the TPM in today's computers. IT administrators can then simply configure their certificate authorities (CA) to create certificates with TPM-based (hardware) private keys. Instead of enabling the TPM machine-by-machine, Wave tools can help enterprises enhance network and data security across the entire enterprise.

Recommendation:

NIST should embody in the Cybersecurity Framework the value and importance of binding network access certificates to hardware in the computer rather than relying on software based-certificates.

wave®
The Trusted Computing Company

Conclusions

Wave believes that Trusting Computing addresses the goals and objectives outlined by NIST for developing the Cybersecurity Framework.

1. Trusted Computing represents an open, industry, cross-sector, consensus-based, set of security standards and concepts.
2. Trusted Computing standards have been developed over the past ten years by the TCG.
3. Trusted Computing core components have been deployed on approximately one billion computers world-wide.
4. The standards are tested, repeatable, performance-based, and cost-effective. Since Trusted Computing standards are open its components represent a competitive marketplace, delivering both multiple sources and low cost.
5. The computer industry has invested over one billion dollars in developing and deploying the hardware, firmware and related software to support the Trusted Computing paradigm.
6. Critical infrastructure, industry in general, government and many consumers have already purchased computers containing core components of Trusted Computing like the TPM. That investment is accelerating as Trusted Computing expands to tablets and smart phones.
7. The Trusted Computing paradigm represents proven best practices of hardware based security already the successful foundation of security and network access for over four billion mobile phones.
8. Looking beyond industry and government cybersecurity concerns Trusted Computing represents a larger solution to consumers who also benefit daily from the internet.

General Keith Alexander is without question a leader in the fight against today's cyber threats to the United States. General Alexander is the current Director, National Security Agency (DIRNSA), Chief, Central Security Service (CHCSS) and Commander, United States Cyber Command.

In a Winter 2012 interview with CGI Initiative For Collaborative Government's Leadership magazine General Alexander was asked, "How can we best secure mobile device hardware in an extremely heterogeneous environment?"

General Alexander replied, **"First, there is great value in leveraging the lessons learned from the work done to improve the security of PCs over the last decade. The private sector began incorporating roots of trust in devices (e.g., Trusted Platform Modules [TPMs]) over the last decade, providing a "root" for further security to build upon in the device."**

http://www.collaborativegov.org/publications/Leadership%20Winter%202012.pdf (page 11)

Wave recommends three core principals provide the fundamental foundation for the Cybersecurity Framework. They are;

1. NIST should make "Only Known Devices" a core principle of the Cyber Framework. This simple yet powerful paradigm is proven on over four billion mobile devices and the hardware is already deployed on about a billion computers based on open industry standards. This access model is built on secure, hardware-rooted device identity solving the majority of cybersecurity challenges promulgated by today's user centric access.

2. NIST should complete SP 800-155 and issue this standard. NIST can reduce a major vulnerability to devastating attacks by recommending as part of the Cybersecurity Framework that industry and government implement BIOS integrity and machine health leveraging hardware that they already own.
3. NIST should embody in the Cybersecurity Framework the value and importance of binding network access certificates to hardware in the computer rather than relying on software-based certificates. This will strengthen bi-lateral trust of the connection between an endpoint and the network.

Appendix

Modernize the Network: Device Identity Networks Meet Enterprise Needs

wave®
The Trusted Computing Company

Modernize the Network:

Device Identity Networks Meet Enterprise Needs

Introduction – Meeting Stakeholder's Needs

The enterprise network is being modernized because users expect better services and because the old models are too expensive.

This transition is already underway, but not enough has been done to determine the best network architecture to achieve the goals of users and enterprises: Users need consistent service on all their devices regardless of how those devices are connected to the network; the enterprise needs security and manageability; the network owner needs to minimize costs. Outlined here is our strong and simple case for how the network should be constructed to achieve the goals of users, enterprise management, and network owners. This architecture is built on simple, fundamental principles that will scale to support the largest networks in the world.

The Big Picture – The Essence of Mobility is Device Identity

Network modernization is being driven by the fundamental transition to a "mobile architecture." Mobile can be complicated – it's not the size or weight of the device[1], nor is it the operating system that makes it a "mobile device" – it's the device's usability, functionality and connectivity that make it mobile.

Users expect services that are the same regardless of how the device is connected. The mail should arrive the same way on 3G, 4G, Wi-Fi, LAN, satellite, directly connected or remoted though another device.

What is really happening is that network membership, previously based on how the device is physically connected, plus User ID and password, is changing to membership based on the device's own tamper-resistant ID and the PIN of the current user of the device. This transformation to a device ID-based network is what defines mobile. This is not new for service delivery networks: Cable is device-based, satellite TV is device-based, Xbox™ is device-based, iPad is device-based, cellular is device-based; it is only enterprise IT that is still user- and network connection-based.

The mobile model needs to be extended to the entire enterprise: desktop, laptop, tablet, phone, etc. To do this, it is crucial to pay attention to the lessons of the past. You can't build a cellular network without a SIM module. The hardware security of the SIM assures that the integrity of the network remains strong. Today standards-based security from the Trusted Computing Group (TCG) provides a similar foundation for the end user device. The fact that only "known devices" can be connected to the network lays a very solid foundation of trust and security, and provides substantial cost reduction. With this common root-of-trust foundation it is possible for many parallel efforts to build on it – from supply chain integrity to dynamic content protection and labeling. Security needs to be fully integrated from the foundation of the solution, yet automated and hidden from the user. The best security is the security that the user never sees - it just works.

[1] 'Device' is the generic and common term we are using in this paper for any computer or other appliance that can serve the needs of a user in accessing cyberspace. The broader, industry standard term is 'endpoint', as defined by the Internet Engineering Task Force (IETF) and the Trusted Computing Group (TGC), and adopted by the National Institute of Standards and Technology (NIST). In most contexts, Wave uses and fully supports this standard.

However, not all devices are created equal – the identity and capabilities of the device define the network. In many cases, enterprises treat the device as an afterthought, but in reality it's the device that defines the network. A services-based, mobile network is dramatically more efficient and trustworthy. The cost for Apple to manage iPads is very low and so is the cost for cellular networks, who deploy millions of devices and change dynamically every day. Achieving the economics of a modern network demands disruptive technology: Device ID first, User ID second and an authentication model at the service level – not at the network level. This assures that only devices with the right capabilities and the right user are receiving a specific service.

The User Experience – Bind Users to Devices; Devices to Services

The consumerization of information technology is all about the user experience. Users need a network where once their device is registered, all of their services are automatic – no more hoops to jump through.

It is no longer acceptable to require a user to log into a VPN to check their mail. Blackberry broke that model years ago. Blackberry is a true mobile service – always there for you, always secure, but the user has none of the keys that could propagate the service to other devices. While mail is expected to be available outside of the firewall, we are still struggling with all other services: As we move to web-based services, each service has (or should have) a different password. This is not easy for users, who are failing to secure their access to services. It is too easy to click on the wrong thing and have a Trojan steal all of your passwords without you ever knowing it.

We need a digital assistant to keep track of all the services we belong to and a device that can connect to them without our interaction. Consider the Blackberry – it has delivered a consistent expectation of always-on service as one of the key principles of the modern network. The user needs this process to always work and always be automated. The reference model is "voice" on cellphones. I get off the plane and connect to a new network and my phone just works, regardless of geographic location. It rings and makes calls right away. Just as with a cell phone, if I pick up my desktop PC and take it to another building due to a flood, it should continue to work. This is what it means for service to be delivered all the time, and the device to be always on.

The model to copy is the set-top box. All the channels are open but Pay-per-view requires a PIN for each purchase. We assumed that the user prevented other users from connecting to the device because they locked the house and as a result the box does not generally require an access code to turn it on. There are always exceptions but the exceptions should dictate the extra step and not encumber the general usage model.

Identifying the user is still critical, as is user-to-device binding to make the whole system work. In the device-centric network, the device has means to assure the correct user is the only one who can use it, or in a shared system, that each user controls isolated portions of the machine. Device encryption forces a strong binding of the correct user to a machine: if the device is lost or stolen, access to all data is prevented. When a user is logged into a device it is critical that access credentials are properly isolated as well. Personal keys, corporate keys and service keys must all be isolated so access can only be controlled by authorized systems.

Finally, all of this has to be transparent for the user. The user logs into their device with a PIN or a biometric and their device provides access to all of the services that the user is authorized for. Secure networking and content protection should function seamlessly and simply in the background.

Device Identity – The Network of Known Devices, Not Physical Connections

At the heart of this new network architecture is the identity of the device. Making device identity the core of the network is happening all around us, yet is not fully appreciated within an enterprise IT environment. Most architects think “mobile” is different from enterprise; this is the first indication that the picture is not clear to them. Device identity enables a new control model on the network, based on endpoint devices, not connection to a network. The first step is to register the device. This registration provides the foundation for specific, granular controls. A device can be denied service, granted additional services, be bound to one or many users and interrogated for capabilities. Capabilities are critical in the modern network where all devices will not be created equal: My phone might not be able to protect HIPAA data and my tablet might be able to, so don’t let me download HIPAA data to the phone, only to the tablet.

So, a 'network' is no longer a physical communications medium, but rather a network of devices that know about one another in order to engage in transactions together. A device can belong to multiple identity networks. Apps provide isolation between these identity networks, so that participation in each such network is private with respect to other networks. One simple means of providing isolation is that browser plug-ins don't share a common identity, but a browser independent trusted isolation process is stronger and simpler.

Device Identity and device attributes are the foundation for asserting device capabilities. Both identity and these other device attributes can be asserted with varying degrees of assurance, ranging from very low assurance, as is provided by most security technologies today, to almost mathematically certain assurance, as is demonstrable for self-encrypting drives or Device Identity. The Trusted Platform Module (TPM) provides the foundation for a tamper-resistant identity in over 600 million devices. It also provides standard methods to prove that capabilities of the machine are measured and can be assured to be part of a specific device. Communication and availability of device capabilities are critical to supporting a mixed environment of devices with the appropriate service. This can all be done transparently to the user.

Supply chain integrity goes hand-in-hand with Device Identity and capability assertions. As devices become more complex it becomes critical that all device element suppliers provide digital signatures for their components. Every element of each device can be traced back to its origin and every device can be verified to be in a known state. This will take years to achieve, so it's critical to start with a strong standard and build the procurement requirements to assure every device is measured and reported on. Trusted computing represents the 3+ billion dollar down payment by industry to adopt this common model. Industry now needs to continue to invest and leverage the down payment to achieve a measured supply chain for cyber devices. Trusted computing secures PCs today – but will secure everything tomorrow.

Device Identity is one of the best investments any enterprise can make. The TPM standard is easy to buy as it is built-into the computing platform. The critical factor is beginning to use the technology and participate in its future – the return on this investment has been clearly demonstrated by the global growth of cellular, cable, satellite and Apple – all of whom have chosen device Identity as their security foundation. Yet enterprise information technology has been stuck investing in user credentials, with minimal returns so far. The modern network will no longer be based on which twisted pair is used, but on the identity of the device and sometimes the user. This is the money-saver that has been proven by Voice-over-IP phones.

Control – By the Owner of the Device, not a Vendor; Permissions by Assertions

One of the key stresses in the enterprise today is the shifting of control to carriers and the major mobile players like Apple. While it is great for them to be service providers they should not be in control of the enterprise users' devices (or a consumer's devices, for that matter).

Today there is only a single point of control for each device. In time, multiple control entities for each device may be possible – for example, "give me the HIPAA data; my device has a self-encrypting drive; just ask my employer." In other words, BYOD should be thought of as one company's machine being joined to another company's domain of control, where the second domain of control uses assurances from the first domain to make decisions. Much of the current thinking on virtualization and isolation does not adequately address assured capabilities and will result in massive failure. Proof of this can be found in the cable industry in the 80s and cellular industry in the 90s where assurance of attributes was not based on solid foundations and was easily hacked.

Control of devices needs to be in the hands of enterprises (and consumers), not in the hands of service providers, like AT&T and Apple. The enterprise is the only one that can assure the level of attention to detail is correct and needs to assure the control model is correct for their business. "Managing" a device, without controlling it, as the Mobile Device Management vendors advocate, is awkward, complex, expensive, and prone to failure. For example, when Apple updated to iOS 6.1, it effectively disabled all MDM security, as the lock screen was easy to bypass. No enterprise was able to test this prior to the release of iOS 6.1, and it is not possible to prevent iOS from upgrading the device because Apple is in control – not the enterprise.

The Trusted Computing Group provides a model for enterprise control. The primary objective is clear – control by the owner of the platform and strong isolation of the keys that are provided so a user cannot steal the corporate keys and the corporation can't use or migrate the user's credentials. The assertion of device capabilities can be made to any service provider and validation can be verified through the device or the network, supporting both a federation and a claims-based model.

User Binding – Known Users on Known Devices through Hardware

While the modern network will be based on device ID, the user is still the ultimate consumer of the services via the device. What user binding does is enable the device to be sure who its user is, so the device can take it from there deep into cyberspace, without having to bother the user who is riding the device anymore for the same information again and again, at each place they visit together. User Binding assures that only known users are on known devices.

If the binding is done entirely in software, even biometric identification will not be very secure. A trustworthy binding between users and devices depends on the security of the data about the users and their connections, so it depends on securely embedding the data in the device hardware: the authentication data for the user is held and matched in hardware on the device itself. There are two ways to do this, based on the Trusted Computing Group specifications and the hardware provided by vendors that conform to the specification. One is the TCG's Opal specification for self-encrypting drives (SEDs), and the other is the Trusted Platform Module (TPM).

Of course the most commonly understood value of strong data encryption, especially the hardware encryption found in SEDs, is that it makes the device safe to lose. But equally important, SEDs provide a highly effective way to bind users to their devices. The TCGs Opal specification is primarily a user-to-device binding specification for SEDs. The specification covers multiple users, recovery, suspension of service, and unlocking for shared services without user presence.

TPMs also support user authentication, by binding users to specific keys. Using such a key, the device can then log into services without involving the user again. Of course, for certain higher security transactions a real-time authentication would be required to release the use of the secret key for that service. It could also be used for timed sessions where a time out requires re-entering the PIN.

The silent use of dual, independent user device binding systems can dramatically increase the level of assurance for a specific transaction: "This is a known user verified by the SED on a known device verified by a TPM key, who has just entered a second PIN (or fingerprint or smartcard read or voice recognition,) to an independent key in the TPM." The degree

of assurance of this binding can be provided as a metric, and matched appropriately to the kind of transaction for which the binding is used. This is notably lacking in most mobile devices today. For example, iPads only support a single user and offer weak recovery methods that can be replayed and recovery passwords that can be sniffed.

Services – Each using its own Independent Identity Network

The purpose of a network is the delivery of services when and where you need them, on the device you are using. It is not possible to deliver service to an unknown device with any assurance that the service is not tampered with on the device. All sensitive services require a strong identification of the user bound to the device, and so of course a strong identification of the device itself. Only known devices should be attached to sensitive networks and services. The service can then be assured that the user is authorized to receive the service's data and that the device has the capabilities to protect the data.

The identity-based network can deliver further attributes to create yet higher levels of assurance, such as a certification that the device is physically inspected once a week, or that the device is currently connected to an internal network. The connection data could be reported, for example, by a network switch or could be a claim from the network switch asserted by the device.

A Web app environment shares a single browser identity and application identity. This apps model enables strong isolation and can support multiple independent identity networks, each associated with a different service. The challenge is to create isolation within the device. While Virtual Machines (VMs) are intended to do this, isolation is not assured unless the VMs themselves can be isolated. The solution lies with Trusted Execution of code running in an isolation kernel.

Content Control: Content Identity Tied to Services, Devices, and Users

The purpose of services is to provide, to the right users, the ability to access and change content. The needs of the modern enterprise will be completely supported by matching network capabilities when Content Identity is added to device, user, and service identity. Content identity enables the delivery of dynamic content, at your fingertips, when you need it, where you need it; and any of your devices, with the owner of the content still able to control its use.

With devices at the core, the service that controls access to content can control the presentation and reuse of content on the device that is rendering it. This requires knowledge of the device and its capabilities, knowledge of the users, and the ability to track the content, and the application of that knowledge to determine and apply allowed usage policies. Content identity comes in many gradations from simple classification and encryption to full-on Digital Rights Management and reporting. In general, the network of today uses old fashioned connections -based security. "I have a key and you have a key and so we can talk." When each piece of content has a unique identity and classifications, the service will deliver content only to known users on appropriate devices.

One of the greatest challenges is that the rendering of the content must happen on the device, so the decryption engine and rendering policy execution for the content must also be in the device if content is to remain secure. It is not possible to securely deliver sensitive content to an unknown device. The unknown device could always be able to make the perfect digital copy in real-time.

Every user is both publisher and consumer. The modern enterprise-controlled, device-based network can assure the integrity and nonrepudiation of content as it is created on a device and assure it is not tampered with once it leaves the originating device. This is critical not only for user-generated content but also sensor data and machine-generated audit data. As the device design continues to mature, and procurement understands how to buy modern devices, this assurance will become very strong. As the quality of data increases, the effort expended on inspection and monitoring can be reduced.

Economics – Lower Costs through a Consistent Network Endpoint Model

Device-centric networks are easier to use, enable mobility, and are more secure, but for the network owner, the most powerful reason to adopt a modern networks is to save a great deal of money. Simple, elegant solutions are much less expensive, while working better.

The modern network is based on the global service networks that have billions of devices deployed. Over the last 20 years the economics of these networks has been very well researched. The existing networks are like the TSA at the airport. Every person has to be scanned every time as though they have never been scanned before. However, when a

pilot enters the line, based on their identification, they get priority service and a reduced scanning level. Now, TSA has introduced PRE for Frequent Flyers. After registration the traveler is subjected to a reduced security protocol. The traveler saves time and money, and the TSA can pass more travelers per unit of time due to reduced transaction time (saving money and increasing capacity). It's a win, win.

Known devices mean enhanced service at lower costs – no need to lock down devices when they are attached to a physical network, no need to install and update – heavy client software, just control the services provided. Known devices mean easier identification of attackers. No need for the enterprise to support different client management software for different device operating systems. No need to treat mobile and enterprise devices as different categories. The network can be configured dynamically and include endpoints whether they are around the world or five cubicles down the hall.

Standards – Leverage and Protect their already Massive Deployment

The standards to enable the modern device-centric network are well established and broadly available. Trusted computing now has over three billion dollars invested in the technology and deployment of the device centric network. Leveraging this investment provides the instant returns that most enterprises seek.

Unfortunately most enterprises still have a user-based model for their PCs, and are attempting to find some way of including mobile devices in this awkward model, where the will never fit. Turn this upside down, mentally add the 600 million PCs with TPMs to the modern mobile network, treating the TPM as the SIM module and the enterprise network becomes the carrier or the service network, like iTunes. Standards ensure that control is put into the owner's hands and not taken over by a single vendor, whether he vendor be Microsoft, Apple, Google, or Verizon. Constant diligence is required to prevent corrupting standards for a single company's benefit.

Conclusion – Make Enterprise Networks 'Mobile', not vice-versa.

The modern, device-identity based enterprise network architecture provides a clear path for the convergence of the enterprise network and the mobile network. It can deliver a great experience for the user and the enterprise controls every institution requires, while enabling a modern model of service, anytime, anywhere, on any registered device. It supports the new reality of many devices that will have differing capabilities that change frequently. It provides the operational cost savings without sacrificing the delivery of service or security so desperately needed. It lays the foundation for a content-sharing future where all users and devices can produce assured data. Finally, it leverages already-deployed industry standards to reduce the capital cost of switching implementations. Experience with this new model is limited in the enterprise computing world, but very well understood by the global service companies.

Erase the white board, step back and start with the device - the modern network architecture will come to light. Every device is mobile.

wave
The Trusted Computing Company

About Wave
Wave Systems Corp. (NASDAQ: WAVX) reduces the complexity, cost and uncertainty of data protection by starting with the device. Wave leverages the hardware security capabilities built directly into endpoint computing platforms themselves. Wave has been among the foremost experts on this growing trend, leading the way with first-to-market solutions and helping shape standards through its work as a board member of the Trusted Computing Group.

When it comes to SEDs, Wave has been among the earliest pioneers, promoting, managing and supporting SEDs from major storage vendors for more than six years.

Wave offers a complete suite of products to support the transition and migration to an embedded security model, starting with existing devices, including Wave EMBASSY® Remote Administration Server for managing self-encrypting drives, and Wave Cloud for the cloud-based management of SEDs. For more information, visit www.wave.com.

03-000362/ version1.00 Release Date: 03-06-2013

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com