TRUSTED COMPUTING

An Already Deployed, Cost Effective, ISO Standard,

Highly Secure Solution for Improving Cybersecurity

Wave Systems Corp. response to

Department of Commerce
Internet Policy Task Force
Notice of Inquiry
Section 4. Authentication/Identity (ID) Management
Dated: July 28, 2010

480 Pleasant Street, Lee, MA 01238   Phone 877-228-WAVE
www.wave.com

Table of Contents

EXECUTIVE SUMMARY

The Internet has become an essential fabric in today's society. From home and school to government and industry we depend on an intertwined network of networks – the Internet. Today our use of the Internet is at risk and under daily attack by criminals and other countries representing an advanced persistent threat. Other technologies, such as cell phones, cable television and iPods have leveraged secure device identity to improve security and the user experience. The computer industry has addressed this need by implementing Trusted Computing.

> ***Imagine for a moment entering username and password every time you switched the channel on your cable box or when you cell phone connected to a new tower. Frankly, it's amazing we even use a PC.***

Trusted Computing represents an already deployed solution. Trusted Platform Modules (TPM) are available from multiple Integrated Circuit manufactures and included in virtually all business class personal computers. Over 350 million personal computers have built in Trusted Computing and millions more ship every month. It's in the box, on the motherboard and you didn't have to order it.

The TPM provides hardware based secure generation and storage of private keys using RSA 2048 cryptography. It is designed on an open standard that has been approved by ISO and is currently undergoing security certification according to Common Criteria.

Only your known computers should have access to your accounts

Critically important to any cybersecurity solution is privacy. The Trusted Platform Module enhances privacy by supporting the creation of multiple unique keys. A PC can have separate keys for each Internet trust relationship, such as a bank or online store. It is not a machine ID but a secure container for ID's.

Trusted Computing represents one of the most cost effective solutions to improve cybersecurity since there is no cost to deploy the solution and no single company gains from its use.

INTRODUCTION

The model of username and password for identification and authentication to web services has become ingrained in Internet users over the past twenty years . However, Industry and government alike have largely condemned this system. It carries a cost to the industry as all new websites must implement their own login authentication system, and it is dangerously insecure as passwords can be guessed or stolen.

However, username/password is familiar and ubiquitous. It is the only mainstream method for identification and authentication used since the web first began personalizing content with the introduction of forms in the mid-nineties. Consumers are largely content with this system and attempts to improve security, with a USB key for example, have rarely been successful unless mandated; an option available only to very high-value business services.

As members of the security industry we often overlook the fact that a majority of personalized web services are mostly about convenience. For every relationship with an online financial institution providing control over real assets, there are ten with services for movie delivery, frequent flyer programs, car rentals and hunting licenses, none of which offer a hacker any value beyond a little information snooping.

If we hope to improve this flawed, but stubbornly ingrained system, we need to focus on simplicity and ease of use. A better system must be at once easier, faster, more secure and within familiar paradigms.

Outside of the Internet, information services have long relied on device security for identity and authentication. Cable boxes and mobile handsets contain unique keys stored in the device hardware. You do not log in to HBO to watch a movie with your cable service or log in to Verizon to make a wireless phone call. The device remembers and secures the account relationship. It’s remarkably easy to use as it requires no interaction after initial setup.

The web is positioned to take advantage of a similar model now that over 350 million PC’s have shipped with Trusted Platform Modules (TPM). TPMs are security chips with the capacity to retain multiple unique keys. Virtually all business class PCs today ship with a TPM on the motherboard.

A unique and private key rooted in the TPM can be compared to a trusted browser cookie. It can be assigned and applied transparently, yet it cannot be compromised, copied or extracted and can only be accessed by the owner of the PC. From the perspective of user experience, authentication is distilled down to, “allow this PC to securely log me on.” From a security perspective it becomes a tight two-factor authentication: what I have, this PC; what I know, how to log on to this PC.

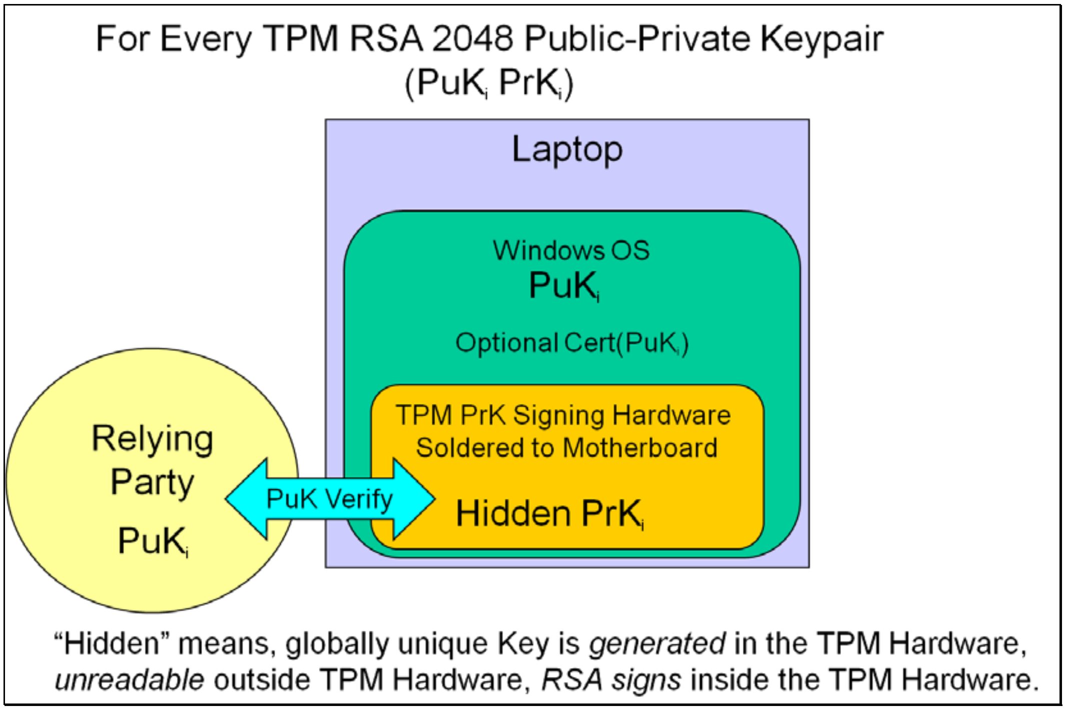
We propose that device identity is the best approach for augmenting cybersecurity. It at once improves user experience by paving the road for adoption and introduces a significantly higher level of trust and security. While username/password will persist for portable identification, hardware-based device identity can be leveraged to vastly improve web security and ease-of-use.

THE TRUSTED PLATFORM MODULE

Over the past decade major computer vendors including Dell, HP, and Lenovo have included a hardware-based authentication tool, the TPM, in their PCs. The TPM has a number of characteristics that make it a strong candidate for a government requirement for user and device identity in applications where security, ease of use, and privacy concerns are important.

The TPM is defined by an industry standards organization, the Trusted Computing Group (TCG), and has been accepted by ISO. To date there are over a half dozen international manufacturers of TPM, including STMicroelectronics, Intel, Atmel, Infineon and Broadcom. There is active work in TCG and by the manufacturers to complete FIPS and Common Criteria certifications.

From a user or device authentication point of view, the TPM provides the basic function of RSA 2048 bit public key cryptography protected by hardware. Most significantly, the TPM provides protected generation of the public and private keys (PuK, PrK) in the key pair, hiding of the PrK, and PrK signing. An external relying party can confirm the globally unique identity using PuK verification. This is illustrated below:


For Every TPM RSA 2048 Public-Private Keypair
(PuK$_i$ PrK$_i$)
Laptop
Windows OS
PuK$_i$
Optional Cert(PuK$_i$)
TPM PrK Signing Hardware
Soldered to Motherboard
Hidden PrK$_i$
Relying
Party
PuK$_i$
PuK Verify
"Hidden" means, globally unique Key is *generated* in the TPM Hardware,
unreadable outside TPM Hardware, *RSA signs* inside the TPM Hardware.

Since the TPM is soldered to the motherboard, and since every TPM can have many globally unique key pairs, the TPM can be employed for establishing identity with strong security claims, strong ease-of-use claims, and strong privacy claims. The strong security claims are that the identity cannot reasonably be spoofed or counterfeited. The ease of use claim is that once the user is logged into his laptop, the TPM signing is as least as reliable as his log in and no matter what (whether you believe the user is present at that moment, or not), can be known with high assurance to be coming from his laptop.

A great deal of attention in the details of the TCG TPM specifications has been paid to use cases where a TPM can be used to sign for a user or a device in ways that provide this high security and ease of use and yet can overcome many privacy concerns. The basic idea is that a laptop can have many globally unique identifiers, not just one. As the White House response paper describes (attached in Appendix), the TPM provides a unique identifier of sorts in its ability to do RSA 2048 signing with a hidden PrK, but it really provides an ecosystem of such unique identifiers that are designed to provide privacy.

To understand how the TPM does this, compare the TPM unique identifier to that on a SIM card in a mobile phone. The SIM card in the mobile phone has virtually eliminated phone service theft, since the unique identifier on the SIM is known by the Telephone provider and the Telephone provider has high assurance that the SIM card cannot be spoofed by a counterfeiter. The use of the TPM for public key cryptography can have the same property: a unique signing key can provide an unspoofable proof of unique identity.

But the problem with PCs is that they are not provisioned by one provider. There is not a Telco, or any other single company, that owns the services on your PC. The TPM solves this problem by allowing for multiple, independent Privacy Certification Authorities (Privacy CAs) that can each establish different user and device identities for the same PC. The term “privacy” here means that for the same PC, two companies can have different globally unique, unspoofable, device IDs, but each can prevent the other from knowing the device ID that each is using. The same is true for user IDs. However, each company can rely on the fact that their ID is globally unique and unspoofable.

This privacy property has many highly desirable consequences for the practical use of multipurpose computers. For example;

- A government employee may connect with a particular government network and with a particular government contractor’s network without the government contractor being able to correlate which PCs are allowed on the government network.
- For commercial use, two competitors can have different device and user IDs for the same PC without being able to correlate what the other competitor knows.
- For personal use, the person can know that if he allows one company, e.g. his power company, to know his unique PC identifier, this is not also allowing any other company to know it.

The TPM is not a conventional implementation of a Public Key Cryptosystem (PKI), in that the PuK may not actually be made public. In other words, a company or other agent acting as a Privacy CA and wishing to not share a particular laptop or user with other companies or agents, can choose to have the TPM protect the PuK from disclosure. In this sense, certificates, which are simply textual publications of PuKs, are not necessary. This is particularly the case when the PrK_i is used for a device identity. If the PrK_i is used for a user identity that can be shared, then a certificate may be manufactured to assert the PuK_i.

The ecosystem of consumer, commercial, and governmental participants is also free to improve authentication efficiencies with the TPMs by sharing "Privacy CAs." The work by the OpenID Foundation provides a means by which strong user and device identity can be shared where the user and the participating organizations trust one another. So, for example, in the government case, a user may trust any number of US Government websites, but wish to log in based on the same ID, provisioned by an OpenID Privacy CA, and the US Government websites can all use that same ID, which is still not necessarily revealed to non-US Government entities for other purposes.

A TPM also provides the opportunity to use a PC as a user authentication token. This is similar to the case with SIM cards and cell phones. This could virtually eliminate the need, as it does with cell phones, of having anything stronger than a four digit PIN to uniquely identify the person is present, sitting at the laptop, to all the providers regardless of which unique device IDs (PrK_is) the providers are using.

In summary, the TPM is an excellent candidate for meeting all the requirements for security, ease of use, and privacy desired by the Department of Commerce in the area of authentication.

MARKET APPLICATIONS OF DEVICE ID

The TPM is readily applicable as a means for enhancing both security and ease-of-use within a number of popular and widely deployed identity infrastructures.

OpenID

OpenID[1] is a second generation standard that enables websites to offload identity authentication to a third-party without compromising privacy or security. It is supported and implemented by such marquee brands as Google, Yahoo, AOL, Sears and many others. In a bid to unburden hundreds of thousands of government websites from individual identity management, the U.S. General Services Administration (GSA) on behalf of the Identity, Credential, and Access Management (ICAM) subcommittee of the U.S. CIO Council has supported OpenID for Level of Assurance 1 (LOA1) account verification[2].

While adoption has been widespread and the benefits of OpenID lauded throughout the community, consumer use has been tepid and wary. Consumers find the system unfamiliar and are suspect of using, for example, a Google account to log into Sears. There is a misassumption that this gives Google unintended insight into a relationship with another party.

OpenID used in conjunction with a TPM for identity and authentication has much to offer. Instead of entering a username/password a user can root their OpenID in a hardware certificate unique to a machine. In this model the consumer benefits from instant login, no username/password required, as well as a familiar and trusted paradigm of using a personal item (in this case the PC) as a means of identification.

Id.wave.com is a public identity provider that implements this model. The service is compliant with the US ICAM LOA1 Trust Framework and actively seeking certification from the Open Identity Exchange[3]. Certified ICAM compliance will enable id.wave.com to act as an identity provider to all participating government websites, such as the NIH[4].

There is a drawback in that most relying parties (account-based services) today only accept a single identity per account. If using a machine ID, a user is likely to want to register multiple machines, as well as a password login to use when travelling or for

[1] See The OpenID Foundation, http://www.openid.net.

[2] See the Open Identity Exchange, http://www.openidentityexchange.com.

[3] Ibid.

[4] See NIH/OIX Press Release, http://openidentityexchange.org/press-releases/nih-announces-oix-pilots-2010-03-03

backup. Until this becomes commonplace an identity service, such as id.wave.com, can enable this feature.

SAML

An older, more enterprise-focused identity standard is SAML[5]. Like OpenID, SAML seeks to concentrate identity authentication in a single entity. It is generally used to support enterprise single sign-on whereby an employee, once logged in to his or her corporate domain, has transparent access to partner sites and other external web services configured for federation.

Popular directory services such as Microsoft's Active Directory support SAML. By using standard certificate-based authentication, where the certificate is signed by the TPM, a machine can be securely authenticated into a corporate domain. The domain may then extend that authentication into the web through SAML.

From the perspective of an end-user, their corporate PC provides instant and transparent access to all services contracted by their company, both internal and external. From an administrative perspective, only machines which have been physically provisioned by the IT department can gain access to those services.

Wireless Access

Another ripe application of device identity with the Trusted Platform Module is securing wireless access. The predominant wireless security protocol, WPA, utilizes standard PKI. Simply by requiring the private key to be held in the hardware of the client (TPM), the network administrator can ensure that only known machines may gain access to the network. There is no key to be shared or stolen. Access requires the device itself. The subsequent securing of a physical device is far simpler and better understood than protecting secrets.

Again, widely used technologies, in combination with the standard security features now available on most PC motherboards, TPMs, can vastly enhance both security and ease-of-use.

[5] See OASIS, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

GOVERNMENT

Government Recognizes the Value of TPM

Since 2007, the Department of Defense has recognized the enhanced security of Trusted Computing by requiring the inclusion of TPMs in all PCs if possible.[6] The NSA will be promoting the security of TPM at their NSA Trusted Computing Conference and Exposition on September 14-16, in Orlando, Florida.[7]

Government Leadership

Both the cable and mobile phone industries solved their fraud and authentication challenges by implementing strong, hardware-based device identity. The diverse and fractured nature of the personal computer and Internet communities requires government leadership to implement improved cybersecurity.

The US government has a rich history of providing leadership to industry to improve the public good. Several examples of the change effected by this leadership can be seen in the Americans with Disabilities Act (ADA) and the Occupational Safety and Health Act (OSHA). For example, The Americans with Disabilities Act generally requires owners of buildings to provide equal access to wheel chair-bound people. Without ADA many building owners would not incur the additional expense to provide access but the legislation requires it and thus provides new freedom. The enactment of OSHA improved employee safety. While no employer would desire their employees to be injured, many would not implement the safety standards required by OSHA due to competitive pressures on

> "It's time for small business to wake up and understand the true risk of online banking," says Litan. "If the bank thinks you were negligent, they do not have any obligation to pay you back."
>
> The Western Beaver County School District in Pennsylvania, for one, is testing this stance. It is suing ESB Bank for executing 74 unauthorized cash transfers totaling $704,610 over four days during Christmas break a year ago. Court records show cash moved into 42 receiving accounts in several states and Puerto Rico. The bank retrieved $263,413 but did not recover $441,197.
>
> ESB's attorney, Joseph DiMenno, says the bank is confident it will be "fully exonerated" but declined to discuss the lawsuit in detail. In a court filing, the bank denied any liability and said the district's "failure to secure and protect" its computers and network were to blame for any damages.
>
> *USA TODAY*, "Cybercrooks stalk small businesses that bank online" 1/13/2010

[6] DoD Memorandum, John G. Grimes, Chief Information Officer, 3 July 2007

[7] http://www.ncsi.com/Home/Default.aspx

overall cost. OSHA provided an equal playing field in effect raising the cost on all businesses equally. Countless thousands of workers have been saved from death or disability by this act and society has benefitted.

Small business and consumers will rapidly implement the enhanced security and privacy of the Trusted Computing Module but this requires key industries to implement acceptance of hardware-based TPM certificates. The government should require certain industries such as banks, financial institutions, Internet commerce sites, insurance companies, physicians, and major corporations to accept hardware-based certificates to increase security and to reduce Internet fraud. Like ramps to buildings, consumers and small businesses would not be required to use device identity, but will have the option if they choose to reduce the risk of fraud.

BUSINESS CASE

Trusted Computing represents a compelling business case for consumers and small business. The TPM delivers simpler computing, higher security and improved privacy and the technology is already deployed on over 350 million personal computers. To best understand the value of Trusted Computing one should consider current alternatives.

Username and Password

Usernames and passwords have been used by most Internet sites which store personal information when creating a unique account. The security concerns with username / password are well documented including the use of: the same username and password for multiple Internet sites, easily guessed usernames and passwords, short password lengths, or written lists of usernames and passwords. All of these examples lead to significant exposure of consumers and small businesses to cybercrime and fraud. In 2009, the dollar loss from all cases of online crime referred to law enforcement in the United States reached $550 million, more than twice the 2008 level.[8] According to Internet World Stats there were approximately 227 million Internet users in the US in 2009[9], while on average the fraud cost is less than $3.00 per person, the cost if you are a victim is certainly much higher.

USB and Unique Key Tokens

A number of companies sell USB and Unique Key tokens which are used to generate a unique number when logging onto a specific site. While these solutions provide a high level of security they generally only work in a one-to-one relationship either internally for a company or between a business or consumer and a company.

An example of a Unique Key Token is the Bank of America (BOA) SafePass™ key card, the card generates a unique number each time it is used. The card only works with the BOA web site. If its use were expanded, it could identify the user as a BOA customer to other web sites, thus creating privacy concerns. consumers and businesses pay $20.00 for the BOA SafePass™ card and they must have a banking relationship with BOA.

[8] See Internet Crime Complaint Center, 2009 Internet Crime Report, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

[9] http://www.Internetworldstats.com/am/us.htm

Private Keys

Many companies store private keys on consumer and business computers. These private keys, among other things, allow an Internet site to know that the consumer has logged into the site in the past and will allow the user to log on without entering their username. Private keys can easily be copied from one computer to another by malware or viruses. The cost of private keys is nominal but the security is negligible since it is not bound to the device or stored securely.

Smart Cards

The US government is currently deploying individual smart cards to all federal employees in accordance with HSPD-12. While some agencies have developed their own PIV deployments, most agencies have elected to use the services of the GSA for purchasing their enrollment and issuing services. The current cost for cards issued by GSA is approximately $200 per card (Note this includes providing a background check (NACI)). It is important to note this does not include the significant cost to implement physical or logical access controls to facilities or systems.

Trusted Computing

The main points from the forgoing discussion of Trusted Computing and the Trusted Platform Module are:

Trusted Computing represents an already deployed identity and privacy solution. TPMs are currently included on virtually all business class personal computers shipped today. Over 350 million personal computers have built-in Trusted Computing and millions more ship every month.

TPMs are manufactured by multiple Integrated Circuit manufacturers and are available from all leading personal computer companies. TPMs are designed on an open standard that has been approved by ISO.

The highly secure TPM is currently undergoing security certification according to Common Criteria and there is active work in TCG and by the manufacturers to complete FIPS certification. The TPM provides hardware-based secure generation and storage of private keys using RSA 2048 cryptography.

Trusted Computing represents one of the most cost effective solutions to improve cybersecurity since there is virtually no cost to deploy the solution and no single company gains from its use.

APPENDIX

Trusted Computing White Paper

Submitted to the White House on June 24, 2010, by Wave Systems Corp.

Department of Defense Memorandum dated July 3, 2007

Issued by John G. Grimes, Chief Information Officer

NSA Trusted Computing Conference Announcement

http://www.ncsi.com/nsatc10/index.shtml

Trusted Computing White Paper

A proven security paradigm in use today and already deployed for improved Online Security

The internet has become an essential fabric in today's society. From home and school to government and industry we depend on an intertwined network of networks – the internet. Today our use of the internet is at risk and under daily attack by criminals and other countries representing an advanced persistent threat. Other technologies have leveraged device identity to improve security and the user experience. The computer industry has addressed this need by implementing Trusted Computing.

Cell phones, cable television and even iPods have solved their user authentication and security challenges by securely and uniquely identifying each device.

> In the early years of the cell phone industry, cell phone numbers were hijacked by criminals. Those numbers was sold permitting people to make bogus cell phone calls which were billed to the 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 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 when you start your computer and then just using the internet…. securely.

The computing industry has many times rallied around international standards either to reduce cost or to improve usability. Prior to Windows 95 a number of competing network protocols was available with various digital formats and physical cable connectors. With the release of Windows 95 computers were required to support Ethernet and to have RJ-45 jacks. This ended the debate on networks; Ethernet is available today worldwide. Consumers and business can be confident regardless of where they are in the world that everyone uses Ethernet and has cables and jacks based on this standard. Likewise, people are confident that purchasing a computer or laptop today will have an Ethernet jack and an OS that supports the protocol.

Trusted Computing represents the Ethernet for cyber security. Trusted Computing is a user–friendly, powerful tool to increase computer and internet security; just like device identity has increased the usability and security for cell phones, cable systems and the entertainment industry. Simply put, the heart of Trusted Computing consists of a Trusted Platform Module (TPM) which is a highly secure chip with a unique serial number on the motherboard of personal computers (PC).

Over the past few years over 350 million Trusted Platform Modules have been shipped on virtually every business class PC. TPMs are based on an open, international industry standard shared by leading manufacturers through an industry association, the Trusted Computing Group. TPMs are manufactured by a number of leading chip companies including; AMD, Infineon and Intel. All the leading PC manufacturers incorporate TPMs in business class machines including; Dell, HP, Toshiba, Acer, Lenovo, Samsung, Sony, Gateway, Panasonic.

TPMs have now reached a tipping point. Due in large part to refresh rates of less than five years for PCs, estimates suggest that nearly every business, doctor's office and most government PCs have TPMs inside. The Department of Defense has required all PCs purchased since 2007 to include a TPM, if possible. The National Security Agency (NSA) is supporting the use of TPMs by the DoD to secure their network. Civil agencies and NIST recognize that device identity is a high priority in network security.

The President and the government are in a unique position and have a responsibility to provide leadership for issues too large for any one company to address. Several examples of the President stepping forward and leading change can be seen in the Americans with Disabilities Act (ADA) and the Occupational Safety and Health Act (OSHA).

> For example, The Americans with Disabilities Act generally requires owners of buildings to provide equal access to wheel chair bound people. Without ADA many building owners would not incur the additional expense to provide access but the legislation requires it and provides new freedom. Additionally, others have benefited as an unintended consequence of the ADA, such as the delivery driver who now uses a ramp to a building or a cut in a sidewalk.
>
> Another example of a President providing leadership was the enactment of OSHA improving employee safety. While no employer would desire their employees to be injured many would not enact the safety standards required by OSHA due to competitive pressures on overall cost. OSHA provided an equal playing field raising in effect the cost on all businesses equally. Countless thousands of workers have been saved death or disability by this act and society has benefitted.

While industries like Cellular phones and cable TV networks have a compelling business case to implement device authentication the computer industry has evolved differently creating the cyber security challenge we face today. While some, especially hackers, believe that we should support any computer, any time, on any network, we probably could all agree that running a nuclear power plant on our daughter's laptop is not a good idea. Only a known machine should be able to connect to the network operating that nuclear power plant or to networks which contain sensitive data.

As the internet and computing have become elements of the essential fabric in today's government, business and personal lives, the security of cyber space becomes more and more crucial. The President and Congress can help government, business and consumers by incorporating two tenets into future legislation which will encourage the migration to Trusted Computing. We would suggest two key positions be adopted in Cyber Security and other legislation.

Sensitive Data: Only "Known Computers" should be connected to "Sensitive Networks." Known Computers are computers that have tamper resistant identities that are held in a Trusted Platform Module or similar hardware device that is designed as part of the computer. A Sensitive Network is any network that transmits Personally Identifiable Information (PII) or confidential data where there is a duty to protect that information. Examples of Sensitive Data include;

- Health records
- Financial Records
- Critical infrastructure information e.g. utilities

Critical Institutions Should Support Known Devices: Critical institutions which transmit PII or confidential data should be required to accept credentials from Known Computers. For example, as a consumer you may wish to limit access to your bank accounts to only your two computers with TPMs, but you are not in a position to compel the bank to accept your credentials. Likewise, as a doctor you may wish to register your computers with your insurance providers, but you are not in a position to compel them to support the standard. Examples of Critical Institutions include;

- Insurance Companies
- Doctors
- Banks and Financial Institutions
- Government Services with sensitive information (e.g. VA, IRS, HHS)

Society Benefits: Trusted Computing, using highly secure TPMs, provides significant benefits to society as we seek a simple, affordable solution to improve cyber security and maintain confidence in the ability to conduct Online Transactions Securely.

- TPMs are based on a **free and open** industry standard supported by the leaders in the PC industry
- TPMs are **already deployed** and currently available on 350 million computers
- TPMs are **inexpensive** - costing only about one dollar
- Known devices on networks is a **proven security solution** for the Cellular phone and Cable TV networks
- Known devices can **solve the consumer and business nightmare** of user name password authentication

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

JUL 0 3 2007

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF DOD FIELD ACTIVITIES
EXECUTIVE DIRECTOR, DOD CYBER CRIME CENTER

SUBJECT: Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media

References: (a) DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(b) DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004, as supplemented by ASD NII/DoD CIO memorandum, same subject, June 2, 2006
(c) DoD Policy Memorandum, "Department of Defense Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
(d) DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices," April 18, 2006

References (a) through (c) require encryption of various categories of sensitive DoD data at rest under certain circumstances. Reference (d) provides recommendations on means to protect sensitive unclassified information on portable computing devices used within DoD and advises that the suggestions are expected to become policy requirements in the near future. This memorandum establishes additional DoD policy for the protection of sensitive unclassified information on mobile computing devices and removable storage media. It applies to all DoD Components and their supporting commercial contactors that process sensitive DoD information.

It is DoD policy that:

(1) All unclassified DoD data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants (PDAs), or removable storage media such as thumb drives and compact discs, shall be treated as sensitive data and encrypted using commercially available encryption technology. Minimally, the cryptography shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant and a mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails or to support other mission or regulatory requirements. DoD information that has been approved for public release does not require encryption.

(2) Priority shall be given to satisfying the requirements of reference (c) and to encrypting DoD information on mobile computing devices used by senior officials (e.g., flag officers and senior executives) and other individuals who travel frequently, particularly to areas outside of the continental United States where loss, theft, or exploitation of the devices is more likely or the consequence of the loss would be more severe.

(3) The requirement to encrypt sensitive unclassified data at rest on mobile computing devices and removable storage media is in addition to the management and access controls for all computing devices specified in references (a) through (c).

(4) In anticipation of emerging encryption product capabilities, as well as requirements for device authentication, DoD Components shall ensure all new computer assets (e.g., server, desktop, laptop, and PDA) procured to support the DoD enterprise include a Trusted Platform Module (TPM) version 1.2 or higher where such technology is available. Written justification must be provided to the responsible Designated Approving Authority if assets are procured without TPM technology in cases where it is available.

DoD Components shall purchase data at rest encryption products through the DoD Enterprise Software Initiative (ESI). The ESI establishes DoD-wide Enterprise Software Agreements / Blanket Purchase Agreements that substantially reduce the cost of common-use, commercial off-the-shelf software. Information on encryption products that meet the requirements of this policy may be found in Attachment 2. Other implementation details may be found at http://www.esi.mil and at http://iase.disa.mil

This policy is effective immediately. DoD Components will report the status of their implementation efforts to this office no later than December 31, 2007. The DoD CIO points of contact are David Hollis (703) 602-9982, david.hollis@osd.mil and David Tuteral (703) 604-0503, david.tuteral.ctr@osd.mil of the Defense-wide Information Assurance Program Office.

John G. Grimes

Attachments:
1. Definitions
2. Press Release

cc:
Chief Information Officers of the DoD Components

DEFINITIONS

JUL 0 3 2007

Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices
and Removable Storage Media Memorandum

Data at Rest: Refers to all data in computer storage (e.g., on hard disk drives, CDs/DVDs, floppy disks, thumb drives, PDAs, cellphones, other removable storage media, etc.) while excluding data that is traversing a network (data in transit) or temporarily residing in computer memory to be read or updated (data in use).

Laptop Computers: Also known as notebook computers, are small mobile personal computers light enough to carry comfortably. Laptops can be battery-operated and often have a thin liquid crystal display (LCD) screen. Some models can mate with a docking station to perform as a full-sized desktop system.

Personal Digital Assistants (PDAs): Also known as palmtops, hand-held computers, and pocket computers, are any small hand-held device that provides computing and data storage abilities. Examples of PDAs include, but are not limited to, BlackBerrys, Treos, Palm Pilots, and Smartphones.

Removable Storage Media: Refers to cartridge and disc-based removable and portable storage media devices that can be used to easily move data between computers. Examples of removable storage media include, but are not limited to, floppy disks, compact discs, USB flash drives, external hard drives and other flash memory cards/drives that contain non-volatile memory.

Trusted Platform Module (TPM): The TPM is a microcontroller that stores keys, passwords and digital certificates. It typically is affixed to the motherboard of computers. It potentially can be used in any computing device that requires these functions. The nature of this hardware chip ensures that the information stored there is made more secure from external software attack and physical theft. The TPM standard is a product of the Trusted Computing Group consortium. For more information on the TPM specification and architecture, refer to www.trustedcomputinggroup.org/groups/tpm.

Sensitive Unclassified Information: Information that is not classified but restricted from public disclosure. For full definition, refer to DoDD 8500.1, "Information Assurance," October 24, 2002.

Attachment 1

HIGH ASSURANCE PLATFORM®

NSA
TRUSTED COMPUTING
CONFERENCE AND EXPOSITION
September 14 - 16, 2010 Orlando, Florida

USING THE HIGH ASSURANCE PLATFORM® TO CREATE SECURITY IN A CONNECTED WORLD

NSA Trusted Computing Conference and Exposition

The National Security Agency invites you to attend the first NSA Trusted Computing Conference and Exposition hosted by the Trusted Computing Division of the NSA/CSS Commercial Solutions Center (NCSC), in partnership with the High Assurance Platform® (HAP) Program Office.

September 14-16, 2010
Doubletree Orlando Hotel at the entrance to Universal Orlando
in Orlando, Florida

The theme for the year's event is
"Using the High Assurance Platform® to Create Security in a Connected World."

Cybersecurity vulnerabilities increasingly threaten national security, our economy, and our way of life. Most existing solutions fail to address the heart of the problem: **Is your computer safe?** In partnership with industry and academia, the NSA is pioneering breakthrough Trusted Computing technologies that stop cyber threats dead in their tracks. If you are concerned about the security of vital data, networks and critical enterprise applications, you will want to attend the **NSA Trusted Computing Conference and Exposition**.

Government and Commercial IT Decision Makers - take advantage of this opportunity to learn how to start building *Security in a Connected World:*

- See live demonstrations of trusted computing solutions that stop malicious intruders
- Learn about practical solutions you can deploy now
- Hear how revolutionary new technologies are being used by leading organizations to protect their data and networks
- Get a glimpse of upcoming technologies from cybersecurity experts in government and industry

Industry Technology Vendors - learn how you can develop cutting-edge solutions that leverage trusted computing technologies:

- Experience the latest HAP computing security technologies
- Understand the HAP technology roadmap, and opportunities to extend or incorporate trusted computing technologies into your products
- Hear from IT security leaders and decision makers about tomorrow's top trusted computing priorities

Academic Institutions (especially those with technology incubators, tech parks and IT security start-up ventures) - network with industry and government to help launch and grow sponsored ventures.

Top Government and Industry Thought Leaders Deliver Keynote Presentations on Cybersecurity and Trusted Computing's Critical Role!

This premier event is acutely focused on addressing the mounting cybersecurity threat. Join us in September and begin your journey to *Security in a Connected World.* Registration is open:

Conference Fee

Government Attendees:
$449.00 early registration fee
(valid up to six weeks before event begins)
$499.00 regular registration fee

Contractor/Industry Attendees:
$529.00 early registration fee
(valid up to six weeks before event begins)
$579.00 regular registration fee

Register at www.ncsi.com