The Trusted PC: Current Status of Trusted Computing

Trusted computing incorporates security at the core of a computing platform (PC, PDA, cell phone, etc.) by providing a unique identity, cryptographic capabilities and secure storage. The trusted platform can help ensure the validity of a system by creating a "foundation of trust for software processes".1 This paper, focusing on the Trusted Computing Group's standards, will provide an overview of trusted computing as it stands today: its methods, applications, possible pitfalls and current implementations.

The Trusted PC: Current Status of Trusted Computing

Chris Hageman
GSEC Practical Assignment Version 1.4b
June 23, 2003

Abstract

Trusted computing incorporates security at the core of a computing platform (PC, PDA, cell phone, etc.) by providing a unique identity, cryptographic capabilities and secure storage. The trusted platform can help ensure the validity of a system by creating a "foundation of trust for software processes".[1] This paper, focusing on the Trusted Computing Group's standards, will provide an overview of trusted computing as it stands today: its methods, applications, possible pitfalls and current implementations.

Trust in Platforms

An argument for establishing trust at the core of a system is that while you can continue to add layers of software-based security, the trust you place in any given layer of software is only as good as the trust you have in the software or hardware on which it is running. For example, a virus in the MBR that is loaded into memory before the operating system loads may stealthily continue its damage while the OS runs – all the while presenting the user with a normally functioning computer. You need to have confidence that the hardware, software and firmware have not been maliciously modified since the last system boot, and ensure that no malware has been introduced.

The Trusted Computing Group (TCG) defines trust as the "ability to feel confident that the software environment in a platform is operating as expected".[2] In other words, the combination of hardware and software that comprise the platform is operating as per some specification. In order to compare the state of the platform to a specification, you need to reliably measure and report information about the platform. This information is then validated by some mutually trusted third party (e.g. a Certificate Authority) to declare that the platform is exactly what it says it is and can be trusted for a given purpose.[3]

The goal of trusted computing is to provide confidence in the state of the machine from power up to shutdown. One method to provide this is via a separate, secure piece of hardware, such as TCG's Trusted Platform Module (TPM).

[1] Pearson, "How can…", sec. 2
[2] TCG, "Frequently Asked Questions", p. 1
[3] TCPA, "Building A Foundation of Trust…", p. 3

This hardware provides three basic services:

1. **Platform Identity** – the ability to uniquely identify a platform and verify that the platform uses trusted computing methods.

2. **Cryptographic Services** – functions such as key generation and encryption/decryption are performed in a secure manner.

3. **Protected Storage** – an area that can only be accessed by certain secure functions.

Sundeep Bajikar provides a threat matrix comparing current software solutions to hardware-based solutions (via a TPM) in his whitepaper on trusted computing and notebook PCs.[4]

Threats	Current Solutions	Weaknesses	TPM Solutions
Data theft	Data encryption (EFS, VPN, encrypted email, etc.)	Encryption keys are stored on the hard disk and are susceptible to tampering	Protected storage of keys through hardware
Unauthorized access to platform	1. Username/Password 2. Biometrics and external tokens for user authentication	1. Subject to dictionary attacks 2. Biometrics can be spoofed 3. Authentication credentials not bound to platform	Protection of authentication credentials by binding them to platform
Unauthorized access to network	Windows network logon, IEEE 802.1x	1. Can be bypassed 2. Certificate can be spoofed 3. Authentication data is stored on the hard disk and is susceptible to tampering	1. PKI based method for platform authentication 2. Hardware protection of authentication data

TCPA and TCG

In October 1999, Compaq, HP, IBM, Intel and Microsoft formed the Trusted Computing Platform Alliance (TCPA), which eventually grew to over 190 members, to focus on "improving trust and security on computing platforms".[5] One of the major products of this working group was a specification for a trusted subsystem. This subsystem contains the Trusted Platform Module (TPM) that provides core security services to the rest of the platform.

[4] Bajikar, p. 6
[5] TCPA, "Frequently Asked Questions", num. 1

However, the TCPA is being replaced by the Trusted Computing Group (TCG). On April 8, 2003 the TCG announced its formation, consisting of new founding member, AMD, along with the original founding members of the TCPA. In addition to supporting and continuing work on the TCPA specifications, the TCG will also license and market the security technology.

The older TCPA web site[6] still has good information that is not necessarily replicated on the new TCG website[7]. Also, since the TCG is so new, most publications still refer to the TCPA.

The TCG supports implementation standards so that "the security and cryptographic community can assess the mechanisms involved, and so that customers can understand and trust the effectiveness of new features".[8] These standards are intended to supplement current security methods and standards (such as smartcards, IPSEC, IKE, PKI), not replace them.

The TCG's three main reference documents are:

Main Specification (Version 1.1b; Aug. 23, 2002)
The Main Specification is a 332-page document defining a Trusted Subsystem along with a set of definitions, structures and protocols to interact with it.[9] The subsystem by itself does not create a secure platform, but does provide a secure means to measure and report on the state of a system.

PC Specific Implementation Specification (Version 1.00, Sept 9, 2001)
The PC Specific Implementation Specification is a 70-page implementation reference for a 32-bit PC architecture. The PC specification defines:

- Measurements to be made.
- How the BIOS interfaces with the TCPA subsystem.
- Subsystem behavior during initialization state changes (e.g. power-up, hard and soft resets).

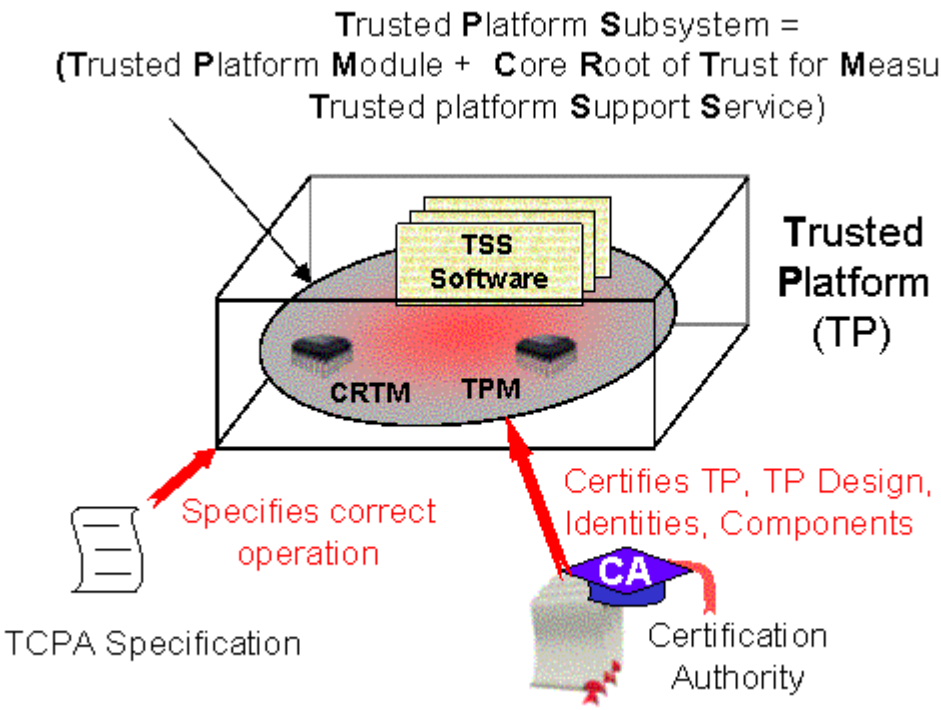
TPM Protection Profile (Version 1.9.7, July 1, 2002)
This 64-page document defines security requirements in order to implement a TPM. The document relies on portions of the ISO/IEC Common Criteria evaluation methods and can be used by an evaluation

[6] www.trustedcomputing.org
[7] www.trustedcomputinggroup.org
[8] TCG, "TCG Main Specification", p. 1
[9] Powell, p. 4

lab to evaluate the security of a component.[10] Note: this document doesn't seem to appear on the TCG site, but you can find it at the TCPA site.[11]

TCG Architecture

The Trusted Platform Subsystem consists of the Core Root of Trust for Measurement (CRTM), the Trusted Platform Module (TPM) and the Trusted Platform Support Services (TSS). These three entities provide trusted services to the rest of the platform. However, third-party certifications are also needed to validate the platform.



A view of the Trusted Platform Subsystem[12]

Core Root of Trust for Measurement (CRTM) – provides secure measurement functions.

Trusted Platform Module (TPM) – provides secure storage and measurement reporting along with other cryptographic services. The TPM may also contain the code that makes up the CRTM, but does not need to. The TCG designed

[10] Powell, p.4
[11] http://www.trustedcomputing.org/docs/TCPA_PCSpecificSpecification_v100.pdf
[12] Pearson, "Trusted Computing…", sec. 5

it this way because while the TPM can be specified as platform independent, the measurements the CRTM makes are based on the platform's architecture, therefore the CRTM remains platform dependent.

Trusted Support Services (TSS) – provides services such as I/O operations for communications between the trusted subsystem and the rest of the platform. The services also include some cryptographic functions, such as 3DES symmetric encryption/decryption, that are not included in the TPM due to reasons of cost

Note: while the CRTM, TPM, and TSS are technically three different components according to the specifications, you will often find them grouped together and referred t as simply "the TPM".

TCG Definitions and Operation

A *root of trust* is a "set of unconditionally trusted functions"[13] that serve as the foundation on which all other trust is built. The execution of the platform (either from a power-up or a reset) begins with execution of the CRTM, which in the case of a PC may be either the BIOS boot block, or the entire BIOS. The trust in the rest of the system (e.g. any measurement made and reported) is based on the integrity of the CRTM.[14] Therefore, both the CRTM and TPM must be protected against hardware and software attacks. The level of protection is specified in the particular platform's protection profile and is certified at manufacture. Upgrades and modifications are allowed only according to the manufacturer's (or whoever certifies the platform) instructions and authorization.

The CRTM measures integrity metrics during system initialization and during runtime. *Integrity metrics* are "data reflecting the integrity of the software state".[15] In the case of a PC, metrics include the BIOS, MBR, and any other firmware bound to the board. The *measurement* is a hash of the software or firmware code. These measurements only reflect the current state of the software (version, patch level, etc.) and don't make any distinction as to whether it is "good" or "bad", "secure" or "insecure". That decision is left to the entity that is looking at the information. The CRTM's only job is to reliably measure and report the results to the TPM.

For example, if the CRTM measurement of the BIOS code does not match a known value, the system may cease booting, or may boot and simply report the state as "not trusted" after the boot sequence is finalized. This depends on the rules enforced by the platform. The rules regarding how to react to integrity metrics are not defined by TCG specifications.

[13] Proudler, sec. 4
[14] TCG, "TCG PC Specific…", p. 13
[15] TCG, "TCG Main Specification", p. 2

The CRTM provides security throughout the boot and run process by extending its root of trust into a *chain of trust*, providing evidence that the system boot was carried out by trusted firmware.[16] The CRTM first measures and reports on itself. Then it reports on the BIOS. The BIOS measures (via CRTM/TPM services) and loads the boot loader. The boot loader, in turn, measures the OS and the OS, can use the TPM at anytime to measure other applications. "As long as software is measured and the result stored before execution, any unauthorized software cannot hide itself".[17] If unauthorized software is present, it will be reflected in a measurement that is stored in the TPM.

The mechanics of measurement and storage provide methods to ensure that the reported values are reliable. The TPM contains (in protected storage) both a measurement log and Platform Configuration Registers (PCRs). The log contains a full history of all measurements and the PCRs contain values representing a sequence of measurements (but not the actual integrity metric). The log and PCR value can be used to validate one another. The process is as follows:

1. **Measurement.** The CRTM creates a hash of the software, firmware or other values it is measuring.

2. **Report to TPM.** The CRTM reports a description of the measured entity and the measurement itself to the Trusted Platform Module.

3. **Storage.** The TPM stores the description and measurement in a log, then:

    a. *Appends* the measurement to the value already store in the appropriate PCR. (Note that measurements are assigned to PCRs according to the platform specification.)

    b. *Hashes* this new value.

    c. *Replaces* the existing value in the PCR with the new hashed value.

When a an inquirer requests the measurements, the TPM can be relied upon to securely report values stored in a PCR, along with the log of measurements for that particular PCR value. The TPM will sign the data with the private key of a key pair. The inquirer, upon receiving this data can compare the PCR value to a known quantity (supplied by a trusted third party) in order to validate the state of the platform. The inquirer knows that the reported metric is reliable, because it can use the same append-hash-replace method on the log to calculate the PCR

[16] American Megatrends Inc., p. 7
[17] Proudler, sec. 6

value. If the reported PCR value and the value calculated from the log don't match, then either the log or the PCR is corrupt. This prevents someone from simply replacing the PCR register.

The TPM provides facilities for securely and reliably storing and reporting integrity metrics. Its secure storage is accessed only by specific trusted functions and it holds the PCRs, some keys, and flags used internally by the TPM. The secure storage, located in the TPM's NVRAM, is not meant to hold a large quantity of data, but rather to protect certain keys that can be used to encrypt data. One such key, the Storage Root Key (SRK), is used to encrypt other keys which then can be stored in unprotected areas. Controlled access to the keys is achieved by the fact that you can enforce one or more requirements (password, platform status, software state, platform identification) in order to have the TPM use the SRK to decrypt any of these keys. The rest of the platform never has direct access to the SRK. It is used only by the TPM to decrypt other keys at the request of the platform.

The TPM provides the following cryptographic services:

- Hashing (SHA-1)
  - Hashes small pieces of data (e.g. metrics)
- RSA asymmetric key generation, and encryption/decryption
  - 2048 bit
  - digital signing
  - key wrapping
- Random Number Generation
  - key generation

The whole Trusted Subsystem, as a separate component of a computing platform, is meant to be optional. Disabling or deactivating it only turns off access to its services. For example, American Megatrends, in its whitepaper on AMIBIOS8 and TCPA explains that the trusted services can be disabled by the "BIOS, TCPA applications or TCPA OS utilities".[18] However, there are those who fear that not running trusted systems might cause them to miss out on future applications or data tied to trusted systems.[19]

[18] American Megatrends Inc., p. 5
[19] Vaughan-Nichols, p. 20

Platform Identity and Certification

In addition to the hardware and software services themselves, there are certificates that are involved with validating a trusted platform:

> *Endorsement Certificate* – contains the public key of the Endorsement Key (described below). It verifies the platform is a genuine TPM. The Endorsement Key and Endorsement Certificate must be supplied by separate entities.
>
> *Platform Certificate* – provided by vendor to indicate that the TPM and other security components are genuine.
>
> *Conformance Certificate* – certifies the conformance level of the TPM. It is provided by an evaluation lab.

During manufacture, each platform is given an identity, a 2048-bit public/private key pair, called the Endorsement Key (EK). This key is unique to the particular TPM, which in turn makes it unique to the platform. This key lasts the life of the machine. However, there does seem to be a TPM command to generate a new key if needed.[20] Presumably, if the key pair was somehow compromised, an authorized party could generate a new EK instead of just junking the machine.

The EK can be used for signing integrity metrics as well as other keys known to the TPM (for example, the Storage Root Key mentioned above). The value of the key is never divulged directly to an enquirer and "… much of the value (or trust) associated with the TPM comes from the fact that the EK is unique and that it is protected within the TPM at all times".[21]

Of course, having a unique identity raises flags with privacy advocates. Remember the Pentium III identification number? Also, guaranteeing that keys are not compromised during the manufacturing process would seem to be a huge burden to the manufacturer, and may not be a process that is going to be readily accepted or trusted by the consumer.

The EK need never be used in communication with an inquirer. Instead, there can be an arbitrary number of uncorrelated Attestation Identities Keys (AIKs), each of which is sufficient to prove that it identifies a trusted platform.[22] The platform's owner can ask the TPM to generate a new AIK and submit a certification request to a Certificate Authority (CA). The request would contain the public AIK value, the Endorsement Certificate, Platform Certificate and Conformance Certificate. The CA will verify, sign, and return the new AIK to the

[20] Bajikar, p. 8
[21] Ibid.
[22] Proudler, sec. 8

platform. Then the platform can use the new AIK to give to anyone who wishes to identify it as a trusted platform. At any time, the platform can have as many AIKs in use as it wants.

Trusted Computing Applications

Controlled Access to Software or Other Licensed Information

A digital content distribution site (say for movies or music) could require that its subscribers use trusted PCs with a certain software set. When a subscriber wants to download music from a legitimate distribution site, the site will check that the user is running in a trusted mode. If the user's platform is approved, he/she can download the music. In addition, parts or all of the content are sealed to the platform – preventing further distribution of the music.

This application to Digital Rights Management (DRM) by helping online content providers enforce their distribution policies seems to be one of the largest concerns for many. There is a fear that the real impetus behind trusted computing is not really to keep intruders out, but to block users from access to certain types of data and to give vendors more control over the user's computer.

Ross Anderson, of the University of Cambridge, is a vocal opponent of trusted computing, stating "[It] benefits big companies at the expense of consumers and lets technology take too much control of systems away from users".[23] He keeps a web page devoted to trusted computing critique.[24]

Enhanced Data Protection

A trusted platform can take advantage of the hardware-protected storage in order to protect keys. It also adds a multi-layer approach to protecting the keys, because not only can you authenticate the user (via smartcard, biometric, etc.), but also the platform itself. If a key can be bound to a specific platform and user, then the only way a key can be used is for a user to logon to that specific piece of hardware. This fact can also help protect data in transit, since once another party is convinced of the trusted state of your platform and has also authenticated you, then they can use these two facts to increase the confidence that anything digitally signed on the platform did indeed come from you.[25]

Another benefit of this protection is that if a user runs a Trojan horse it may access some unprotected data, but could not access anything that is protected because it would not have access to the keys that protect that data. This use of trusted computing would require that the platform maintain a list of approved applications. However, labeling and restricting applications makes open source advocates nervous because a platform may view open source applications as

[23] Vaughan-Nichols, qtd. p. 20
[24] http://www.cl.cam.ac.uk/%7Erja14/tcpa-faq.html
[25] Pearson, "How Can…", sec. 4

untrusted and not allow them to run.[26] This is more of a critique of how the system in applied rather than one of trusted computing methods, since it depends on who creates and maintains the list. If it is the individual user, then there should be no problem. However, in the case of something like Microsoft's Next Generation Secure Computing Base (another implementation of trusted computing, reviewed below), the fear seems to be more well-founded since Microsoft's methods are more vendor specific.

Identity Attestation

This ability can be useful for a corporation that only allows access to its VPN or corporate database via trusted platforms, or even specific machines. Likewise a supplier could require trusted PCs in order to connect to their extranet.

The infrastructure to build and manage these trust relationships, however, could prove costly and politically complicated according to Andrew Huang, whose experience with Microsoft's Xbox (examined below) gave him important insights into trusted computing. These complications come from the fact that application vendors would need to "inspect all interoperability candidates for Trojan horses and back doors prior to trusting them".[27]

Products on the Market

Microsoft NGSCB[28]

The Next Generation Secure Computing Base (NGSCB), though not an implementation of the TCG specification, will incorporate future versions of the TCG TPM. NGSCB was showcased in MAY 2003 at the Windows Hardware Engineering Conference (WINHEC), and may be included in the 2004/5 release of "Longhorn", however many speculate we probably won't see it until 2006.[29] Originally, research started in 1997 under the name "Palladium", but in January 2003, Microsoft changed the name to Next Generation Secure Computing Base, reportedly because another company had trademarked "Palladium".[30]

NGSCB will actually load from Windows, creating an NGSCB secured partition relying on a "nexus" component (also known as the "nub" or Trusted Operating Root) that functions like an OS microkernel to provide protected memory, identity attestation, sealed storage, and secure I/O.[31] The CPU needs to be NGSCB-aware and requires chipsets, I/O devices, graphics co-processor to all handle encrypted I/O. Because of these requirements, there is a fear that this type of implementation will slow the trusted computing market due to costly redesign.[32]

---

[26] Vaughan-Nichols, p. 20
[27] Huang, "The Trusted PC…", p. 104
[28] http://www.microsoft.com/resources/ngscb/default.mspx
[29] Foley, Evers
[30] Evers, Dudley
[31] Vaughan-Nichols, p. 19
[32] Ibid.

NGSCB also requires a Notarized Computing Agent (also known as "my man" or "identity service authority") to authenticate trusted applications and data. For example a movie company that wants to sell secure content will create an NCA, such as a movie player, and distribute it.[33] Users would then run that player to gain access to the movies distributed by the company.

NGSCB is drawing fire from numerous sources, including the Electronic Privacy Information Center (EPIC), which has a section of its site devoted to NGSCB/Palladium and states:

> Palladium could place Microsoft as the gatekeeper of identification and authentication. Additionally, systems embedded in both software and hardware would control access to content, thereby creating ubiquitous Digital Rights Management schemes that can track users and control use of media.[34]

Microsoft Xbox

The Xbox gaming console, though again not an actual TCPA implementation, employs some trusted computing methods and is an interesting case showing potential weakness in the hardware-based security concept. Andrew Huang, of Xenatera Partners, successfully infiltrated the Xbox security and maintains a portion of his site devoted to the Xbox and consoles in general. [35]

According to Huang the XBOX is basically a PC with hardware enhancements, such as secret boot block camouflaged by a decoy boot block in an external ROM. However, the code from the secret boot block is transferred in the clear over the HyperTransport bus. Huang was able to build the equipment for $50 in order to read the bus, and he estimates you could rent the same equipment for $500 per month.[36]

Huang asserts that assuming hardware attacks are too costly and not providing adequate protection from them is a mistake. He laid out some other methods for physically attacking a box:

- SPAM (schizophrenic access memory) – a method of presenting unmodified memory during any inspection process, while actually running patched memory.

- SPIOS (schizophrenic basic input/output system) – a method to switch BIOS images in order to break security.

---

[33] Lettice
[34] Electronic Privacy Information Center
[35] http://www.xenatera.com/bunnie/proj/anatak/
[36] Huang, "The Trusted PC…, p. 103

Huang also suggested some better, already available, architectural techniques such as using guarded pointers and data tags to provide security at the hardware level.

Intel
Intel has several initiatives underway:[37]

> **Centrino** (formerly Banias)[38]
> Released March 12 of this year, it is a Pentium M processor and an 855 chipset with an Intel PRO/Wireless 2100 network connection. It will eventually incorporate a TPM and other security technology such as Checkpoint VPN-1® SecureClient™ and VeriSign's Personal Trust Agents.
>
> **LaGrande**
> This technology is supposed to cordon off specific areas of hard-drive data, keyboard, display and interconnects within the PC[39], but there is no hard information on it currently available to the public.
>
> **Springdale**
> The Springdale chipset will reportedly contain a TPM.[40]

American Megatrends Inc.[41]
AMIBIOS8 includes both 32- and 16-bit code to interact with a TCPA-compliant TPM. The code is optional if the system builder wants to use it, and should work with any operating system.

Wave Systems[42]
Wave Systems provides the EMBASSY (EMBedded Application Security Subsystem) in NEC's Packard Bell Secure PC. This product was rolled out in Belgium, France and the Netherlands in November 2002 - cost is about $1,400. These systems are geared toward secure transactions for e-commerce.

IBM[43]
IBM provides the TCPA-compliant Embedded Security Subsystem (ESS) on some ThinkPad, NetVista, and ThinkCentre systems.

---

[37] http://www.intel.com/design/security/tcpa.htm
[38] http://www.intel.com/apac/eng/home/mobile/centrino/index.htm
[39] Kanellos
[40] Magee
[41] http://www.ami.com/support/doc/AMIBIOS8_TCPA_whitepaper.pdf
[42] http://www.wave.com/technology/trustedpc_1.html
[43] http://www.pc.ibm.com/us/security/

Chip Makers

There are chipmakers already producing TPMs and chips that have TPM-like features.

Company	Product
AMD	Opteron[44]
ATMEL[45]	AT97SC3201 TPM[46]
Infineon	SLD 9630TT1.1 TPM[47]
National Semiconductor	SafeKeeper PC21100[48]
ST Micro	ST19XP18[49]
Transmeta	Crusoe[50]
VIA	C3 (containing Padlock™ encryption engine)[51]

Conclusion

Trusted computing methods can definitely provide functionality that is useful in the security arena. The hardware and software is already becoming available in various forms, therefore it is unlikely that the movement will be stopped cold, regardless of its problems and critics. However, exactly how trusted computing will look in the future depends ultimately on the consumer. Who will they trust and what will they buy?

[44] http://www.amd.com/gb-uk/Corporate/VirtualPressRoom/0,,51_104_543_552~840,00.html
[45] http://www.atmel.com/products/Embedded/
[46] http://www.atmel.com/dyn/resources/prod_documents/2015s.pdf
[47] http://www.infineon.com/cgi/ecrm.dll/ecrm/scripts/prod_ov.jsp?oid=29049&cat_oid=-9313
[48] http://www.national.com/pf/PC/PC21100.html
[49] http://us.st.com/stonline/books/pdf/docs/9351.pdf
[50] http://investor.transmeta.com/news/20030114-99407.cfm
[51] http://www.via.com.tw/en/viac3/padlock.jsp

References

American Megatrends Inc. “TCPA and AMIBIOS8” January 28, 2003. URL: http://www.ami.com/support/doc/AMIBIOS8_TCPA_whitepaper.pdf (June 23, 2003).

Anderson, Ross. “The Economics of Trusted Computing” November 7, 2002. URL: http://www.netproject.co.uk/presentations/TCPA/ross_anderson.pdf (June 22, 2003).

Bajikar, Sundeep. “Trusted Platform Module (TPM) based Security on Notebook PCs – White Paper” June 20, 2002. URL: http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf (May 30, 2003).

Cox, Alan. “Trusted Computing and Open Source” November 7, 2002. URL: http://www.netproject.co.uk/presentations/TCPA/alan_cox.pdf (June 22, 2003)

Dudley, Brier. “Microsoft Gives Up on ‘Palladium’ Trademark. January 25, 2003. URL: http://seattletimes.nwsource.com/html/businesstechnology/134621649_microsoftpalladium25.html (May 30, 2003)

Electronic Privacy Information Center. “Microsoft Palladium” November 11, 2002. URL: http://www.epic.org/privacy/consumer/microsoft/palladium.html (June 22, 2003).

Everett, Dr. David B. “Trusted Computing Platforms” November 7, 2002. URL: http://www.netproject.co.uk/presentations/TCPA/david_everett.pdf (June 22, 2003)

Evers, Joris. “Microsoft drops ‘Palladium’ code name” January 27, 2003. URL: http://www.infoworld.com/article/03/01/27/hnPalladium_1.html?development (June 23, 2003).

Foley, Mary Joe. “Microsoft to Demo ‘Palladium’ at WINHEC” March 26, 2003. URL: http://www.microsoft-watch.com/article2/0,4248,976208,00.asp (June 23, 2003).

Gerck, Ed. “Trust as Qualified Reliance on Information” January, 2002. URL: http://nma.com/papers/it-trust-part1.pdf (May 26, 2003).

Glass, Brett. “Microsoft’s Palladium: Security for Whom?” June 24, 2002. URL: http://www.extremetech.com/article2/0,3973,263367,00.asp (June 23, 2003).

Huang, Andrew. "Keeping Secrets in Hardware" Presentation to CHES2002, August 15, 2002. URL: http://ece.gmu.edu/crypto/ches02/talks_files/Huang.pdf (June 23, 2003).

Huang, Andrew. "The Trusted PC: Skin-Deep Security." IEEE Computer October 2002: pp. 103 -105.

Huang, Andrew. Keeping Secrets in Hardware: the Microsoft Xbox Case Study" May 26, 2002. URL: http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf (June 23, 2003).

Intel. "Intel Otellini Cites Silicon As The Engine Of Convergence" September 9, 2002. URL: http://www.intel.com/pressroom/archive/releases/20020909corp.htm (May 30, 2003).

Kanellos, Michael. "Intel: Hyperthreading to speed desktops" September 9, 2002. URL: http://news.com.com/2100-1001-957194.html (June 23, 2003).

Krill, Paul. "Linux boost expected for Trusted Computing Scheme" (January 29, 2003). URL: http://www.infoworld.com/article/03/01/29/hntcpa_1.html (June 23, 2003).

Lemos, Robert. "Tech Titans Team for Trusted Computing" , Cnet News.com, June 9, 2003. URL: http://zdnet.com.com/2100-1105-996032.html (June 22, 2003).

Lemos, Robert. "Trust or Treachery?" CNET News.com. November 7, 2002. URL: http://news.com.com/2102-1001-964628.html (June 21, 2003).

Lettice, John. "Inside Microsoft's Secure OS Project Palladium" November 12, 2002. URL: http://www.extremetech.com/article2/0,3973,837726,00.asp (June 23, 2003).

Magee, Mike. "Trusted Computing Platform becomes real in Springdale" February 24, 2003. URL: http://www.theinquirer.org/?article=7942 (June 23, 2003)

Manferdelli, John. "Trustworthy Computing and Palladium" November 7, 2002. URL: http://www.netproject.co.uk/presentations/TCPA/john_manferdelli.pdf (June 22, 2003).

Microsoft. "Microsoft 'Palladium': A Business Overview" August 2002. URL: http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp (June 23, 2003).

Microsoft. "Microsoft Next-Generation Secure Computing Base – Technical FAQ". February, 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/NGSCB.asp (May 30, 2003).

Pearson, Siani. "How Can You Trust the Computer in Front of You?" September, 13, 2002. URL: http://www.informit.com/isapi/product_id~{CF3B6143-9D8C-4181-BAED-DB05910E6000}/session_id~{204CBB75-FC9F-4E92-B020-7408537907A7}/content/index.asp (June 22, 2003).

Pearson, Siani. "Trusted Computing Platforms, the Next Security Solution". August 30, 2002. URL: http://www.informit.com/isapi/product_id~{59C1E494-389B-460B-8DDC-519A8CFEAD6B}/session_id~{204CBB75-FC9F-4E92-B020-7408537907A7}/content/index.asp (June 22, 2003).

Powell, Charles Scott. "Foundations for Trusted Computing" November 7, 2002. URL: http://www.netproject.co.uk/presentations/TCPA/charles_powell.pdf (June 22, 2003)

Proudler, Graeme. "What's in a Trusted Computing Platform?" August 23, 2002. URL: http://www.informit.com/isapi/product_id~{85459B72-87F3-4433-ACE8-D462E7F533F3}/session_id~{204CBB75-FC9F-4E92-B020-7408537907A7}/content/index.asp (June 22, 2003).

Schneier, Bruce. "Crypto-Gram Newsletter" August 15, 2002. URL: http://www.counterpane.com/crypto-gram-0208.html#1 (June 23, 2003).

Schoen, Seth. "Notes on Microsoft Meeting" July 5, 2002. URL: http://vitanuova.loyalty.org/2002-07-05.html (June 23, 2003).

Spooner, John G. "Phoenix targets security, ease of use" February 18, 2003. URL: http://news.com.com/2100-1001-984896.html?tag=rn (June 23, 2003).

Spooner, John G. "Via chips away at security issues" January 21, 2003. URL: http://news.com.com/2100-1040-981394.html (June 23, 2003).

TCG, "Frequently Asked Questions" 2003. URL: http://www.trustedcomputinggroup.org/about/faq (June 16, 2003).

TCG. "TCG Main Specification Version 1.1b" February 22, 2002. URL: http://www.trustedcomputinggroup.org/downloads/tcg_spec_1_1b.zip (June 22, 2003).

TCG. “TCG PC Specific Implementation Specification Version 1.00” September 9, 2001. URL: http://www.trustedcomputinggroup.org/downloads/tcg_pc_specification_1_0.pdf (June 22, 2003).

TCPA, “Building a Foundation of Trust in the PC” January 2000,. URL: http://www.trustedcomputing.org/docs/TCPA_first_WP.pdf (June 16, 2003).

TCPA. “Credible Interoperability” February, 7, 2002. URL: http://www.trustedcomputing.org/docs/Credible_Interoperability_020702.pdf (June 23, 2003).

TCPA. “TCPA Frequently Asked Questions, Rev 5.0” July 3, 2002. URL: http://www.trustedcomputing.org/docs/Website_TCPA%20FAQ_0703021.pdf (June 22, 2003).

TCPA. “Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile Version 1.9.7” July 1, 2002. URL: http://www.trustedcomputing.org/docs/TCPA_TPM_PP_1_9_7.pdf (June 22, 2003).

TCPA. “Usage Models – Trusted Computing in Action” February 7, 2002. URL: http://www.trustedcomputing.org/docs/USAGE_MODELS_020702.pdf (June 23, 2003).

Vaughan-Nichols, Steven J. “How Trustworthy is Trusted Computing?” IEEE Computer March 2003: pp. 18-20.

Zaba, Stefek. “A Vendor’s Perspective” November 7, 2002. URL: http://www.netproject.co.uk/presentations/TCPA/stefek_zaba.pdf (June 22, 2003).

Last Updated: May 24th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced