Trusted Computing: Putting a security module on every desktop

Chris Mitchell
Information Security Group
Royal Holloway, University of London
(Visiting Erskine Fellow, University of Canterbury)

Contents

- What is trusted computing?
- The TCG
- TCG – TPM and TSS
- Software security – How can trusted computing help?
- Using trusted computing functionality
- Conclusions

Contents

Trusted Computing

- We start by introducing the notion of Trusted Computing.
- The notion originates from the Trusted Computing Group (TCG) – in fact from its predecessor body, the TCPA.
- The first fruits of what has been a large scale research and development effort are now visible in the form of a secure chip on the motherboards of many new PCs.
- Microsoft Vista incorporates support for these chips, and uses them as the basis for certain novel security functions.
- Open source software also exists that is capable of exploiting this hardware.
- However, the full potential of the hardware remains to be exploited.

A trusted system

- A trusted system or component is one that behaves in the expected manner for a particular purpose.

  [Trusted Computing Group – www.trustedcomputinggroup.org]
- This is difficult to achieve this for a PC – where typically there is no way of telling whether the 'real' (uncorrupted) Windows is running.
- As a result there is no way of getting any confidence in the correct running of applications. [Even if the operating system says that everything is OK, then this does not help because it cannot be believed].
- It is even more difficult to prove to a third party that the state of a PC is as claimed.

Fundamental requirements

- First we need a way of achieving assurance that the operating system has booted correctly.
- This requires assuming that the PC hardware has not been modified; this is made difficult, but not impossible, for the attacker by embedding key functions in a dedicated chip – the Trusted Platform Module (TPM).
- Need a way of checking the boot process.
- The component that checks the initial boot must be trusted – the 'Core Root of Trust' – this is hardware-based.
- If the loaded software has been checked (and hence is reliable), it can check the next software to be loaded, and again there is a solid basis for trust; this process is iterated.

Monitoring the checking

- As well as performing checks during the boot process, there needs to be a reliable way of recording the results of each of these checks.
- The trusted hardware incorporates hardware registers which store hash-codes of software that has been loaded – these registers provide a reliable record of all the software that has been executed on the trusted platform.
- Anyone wishing to check the state of the platform only needs to be given the contents of these registers (as long as they know what the values 'ought to be').

Building on the trusted base

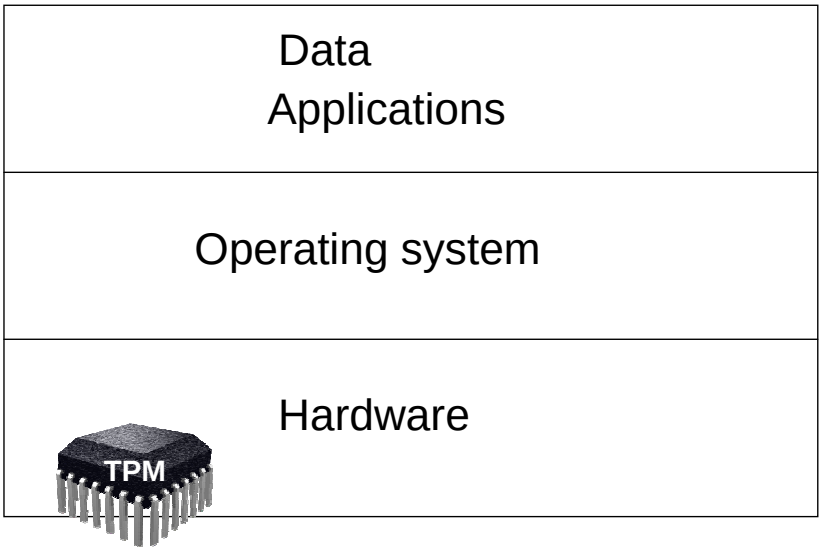
- This base of trust can be used to support two fundamental trusted computing functions:
  - **Attestation**, where a PC can reliably attest to its software state to a third party (by describing the contents of the registers which store hashes of software state);
  - **Secure storage**, where a PC can store data in such a way that only if the PC is in a specific trusted state will the data be decrypted and available to an application (by linking the decryption keys to specific register contents).
- We now look in a little more detail at the set of technical functions provided by trusted computing (as needed to support the fundamentals we have outlined).

Components of a trusted computing framework

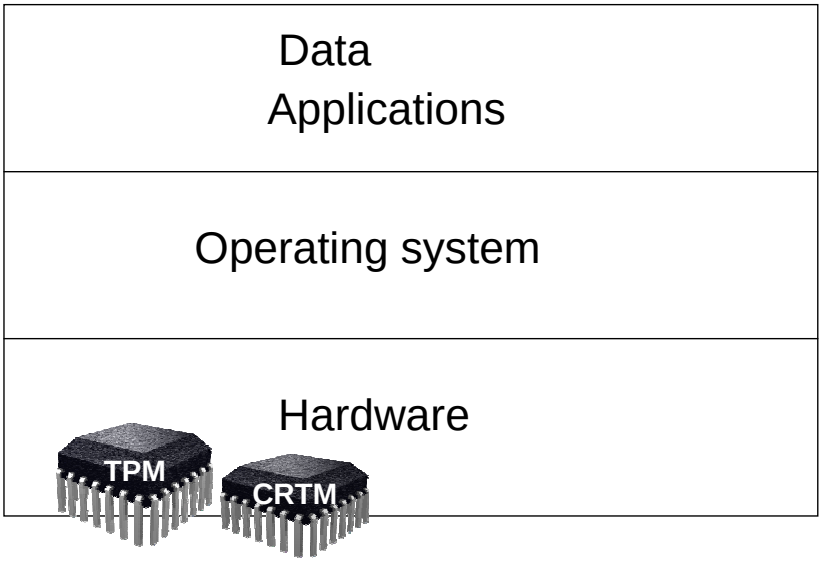
- Shielded locations and protected capabilities:
  - Protected capabilities are those capabilities whose correct operation is necessary for the platform to be trusted;
  - Shielded locations are areas in which data is protected against interference or snooping;
  - Only protected capabilities have access to shielded locations.
- Attestation:
  - Attestation by the TPM;
  - Attestation to a trusted platform (incorporating a TPM);
  - Attestation of a trusted platform;
  - Authentication of a trusted platform.
- Integrity measurement, storage and reporting.

[TCG specification Architecture Overview]

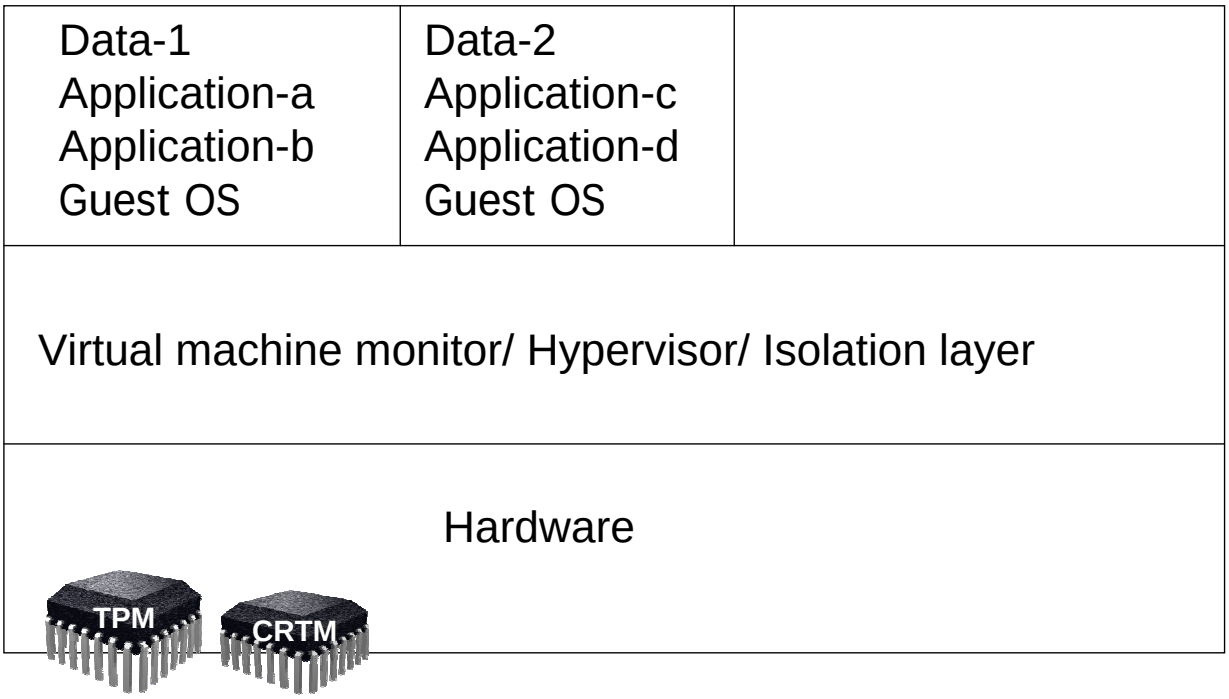
Current platforms with integrated TPMs



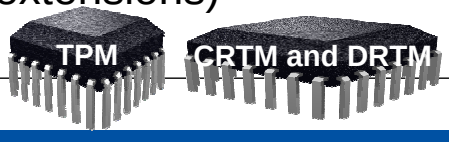
Envisaged trusted platforms (stage 1)



Envisaged trusted platforms (stage 2)



Envisaged trusted platforms (stage 3)

Data-1 Application-a Application-b Guest OS	Data-2 Application-c Application-d Guest OS	
Virtual machine monitor/ Hypervisor/ Isolation layer		
Hardware (including hardware support for isolation – CPU, chipset, keyboard, mouse, video graphics card extensions) 		

Contents

The TCPA

- TCPA (Trusted Computing Platform Alliance): An industry working group.
- Focus: Enhancing trust and security in computing platforms.
- Originally an alliance of promoter companies (HP, IBM, Intel and Microsoft). Founded in 1999.
- Initial draft standard unveiled in late 1999.
- Invitation then extended to other companies to join the alliance.
- Specification eventually became an open industry standard.
- By 2002 the TCPA had over 150 member companies.

The TCG

- TCG: announced April 8, 2003.
- TCPA recognised TCG as successor organisation for the development of trusted computing specifications.
- TCG adopted the specifications of the TCPA.
- Aims:
  - To extend the specifications for multiple platform types;
  - To complete software interface specifications to facilitate application development and interoperability;
  - To ensure backward compatibility.

The TCG main specifications

- TCG TPM main specification (general platform specification) version 1.2:
  - Design principles;
  - Structures of the TPM;
  - TPM commands.
- TCG software stack (TSS) specification version 1.2.
- TCG software stack (TSS) specification header file.
- Specifications available at:
    - www.trustedcomputinggroup.org

Contents

The trusted platform subsystem (TPS)

- The TPS is composed of three fundamental elements:
  - The root of trust for measurement (RTM);
  - The trusted platform module (TPM), which is the root of trust for storage (RTS) and the root of trust for reporting (RTR); and
  - The TCG software stack (TSS), which encompasses the software on the platform that supports the platform's TPM.

Roots of trust

- The RTM:
  - The RTM is a computing engine which accurately generates at least one integrity measurement representing a software component running on the platform;
  - The measurement digest is then recorded in a platform configuration register (PCR) in the TPM;
  - Details of the measuring process, namely the measured value, is then recorded to the stored measurement log (SML) outside the TPM.

Roots of trust

- For the foreseeable future, it is envisaged that the RTM will be integrated into the normal computing engine of the platform, where the provision of additional BIOS boot block or BIOS instructions (the Core Root of Trust for Measurement, or CRTM) cause the main platform processor to function as the RTM.
- Ideally, however, for the highest level of security, the CRTM would be part of the TPM.

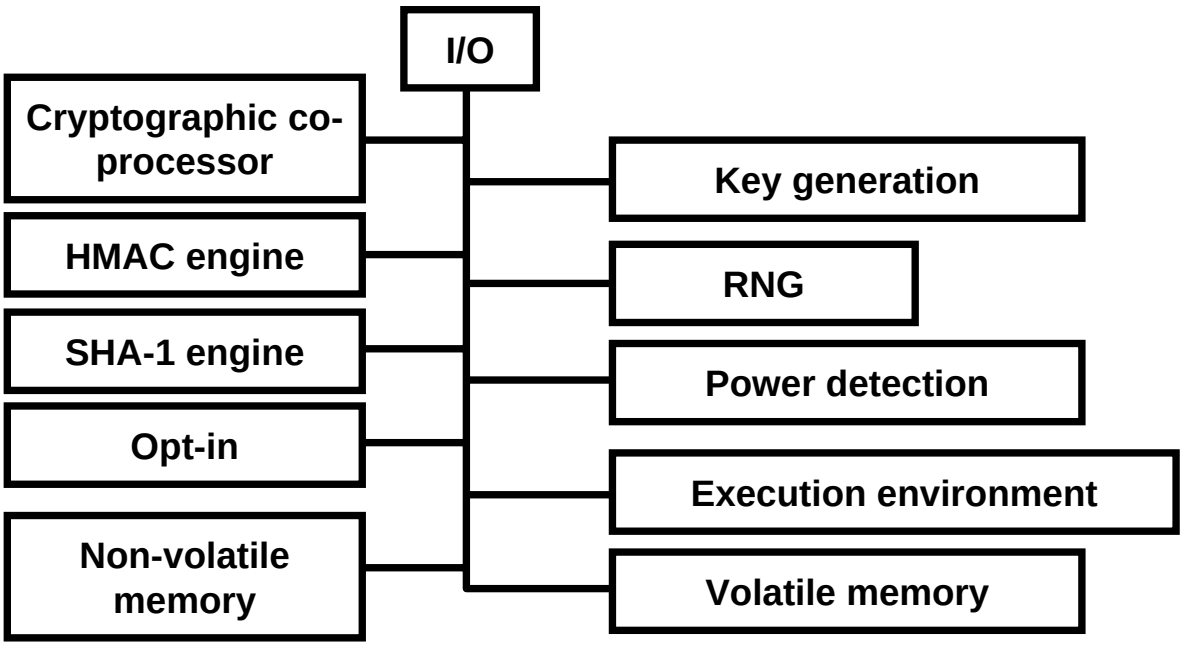
Roots of trust

- The RTS and RTR:
  - The RTS is a collection of capabilities which must be trusted if storage of data inside a platform is to be trusted:
    - The RTS provides integrity and confidentiality protection to data used by the TPM but that is stored externally;
    - It also provides a mechanism to ensure that the release of certain data only occurs in a named environment.
  - The RTR is a collection of capabilities that must be trusted if reports of integrity measurements which represent the platform state are to be trusted.

The TSS

- The TCG software stack (TSS) is the software on the platform which supports the TPM.
- The challenger must determine whether TSS functions can be trusted by examining integrity metrics.
- The TSS architecture consists of a number of software modules, which provide fundamental resources to support the TPM:
  - The TPM Device Driver;
  - TPM Core Services;
  - TPM Service Provider.

The TPM components



Limits to TC hardware capabilities

- The notion underlying trusted computing is to reliably measure and report on the software running on a machine.
- This is fine for a simple machine, for which software will not often change (e.g. dedicated systems).
- However, for a PC this is infeasible.
- The operating system alone (e.g. Windows) is incredibly large and complex, and has a very large number of versions.
- If applications are added to this, then the problem of deciding whether or not a given state is trustworthy becomes impossible.

Isolation layer

- Instead, the idea is to measure all software only up to a certain point, and then to rely on the software to ‘look after itself’.
- If the measured software provides the basis for virtualisation and secure compartments for individual processes, then we should be in good shape.
- This is the idea behind the isolation layer.
- An isolation layer is a small, secure, mini-operating system, which is measured by the trusted computing hardware, and which takes care of the security of subsequently run applications.
- Microsoft has described what its isolation layer would be like (NGSCB), and there are a variety of open source initiatives (including OpenTC).

Contents

- What is trusted computing?
- The TCG
- TCG – TPM and TSS
- Software security – How can trusted computing help?
- Using trusted computing functionality
- Conclusions

Software security – What TC cannot do

- Software vulnerabilities result from both:
  - Design errors;
  - Coding errors.
- TC technology will not prevent vulnerabilities, or aid in the development of secure software without vulnerabilities.
- Vulnerabilities can be attacked by viruses and worms at any time.
- TC technology will not stop viruses/malicious code being written or circulated

The isolation layer – What TC can do

- Security of the isolation layer code itself:
  - Execution of the isolation layer in ring -1:
    - Physical separation of the isolation layer;
    - Size of isolation layer – relatively small number of lines of code;
    - (possibly) provably secure.

  Helps prevent a potential attack by malicious software against the isolation kernel.

The isolation layer – What TC can do

- Security of software running in protected domains supported by the isolation layer:
  - Confidentiality and integrity of application code and data:
    - Memory protection to prevent software attack during execution;
    - Sealing to enable the detection of software modification during storage;
    - DMA-protection to prevent physical attacks which may allow software controls to be bypassed, thereby enabling an attack by malicious software;
    - Protected inter process communication (IPC) – a program should be able to exchange data with another program so that the integrity and confidentiality of the data is assured.

  Helps prevent a potential attack by malicious software.

Peripheral security – What TC can do

- Trusted path to the user in order to ensure the confidentiality and integrity of user input:
  - Prevents malicious applications from displaying a faked dialogue, e.g. to capture a user password;
  - Prevents user input from being read/copied or altered by a malicious application.

  Helps prevent a potential attack by malicious software.
- Secure channel to output devices to ensure integrity of output can be assured.

  Helps prevent a potential attack by malicious software.

The TPM – What TC can do

- Persistent storage:
  - Encrypted data protected from malicious code;
  - Insurance that data can only be accessed within a certain environment.

  Helps prevent some of the fall out from an attack by malicious software.
- Secure boot:
  - While not described within the TCG v1.2 specifications, all the necessary elements are in place to implement such a service.

  Helps prevent the fall out from an attack by malicious software.

The TPM – What TC can do

- Attestation:
  - Enables a platform challenger to verify what versions of software are running on a platform;
  - Can be used to check whether or not the latest anti-virus definitions have been downloaded.

  Helps prevent some of the fall out from an attack by malicious software.

The TPM – What TC can do

- Software may be built to leverage the TPM security mechanisms:
  - Many software security problems arise from misuse of cryptography:
    - Misuse of randomness:
      - many programs require sources of randomness;
      - most common method of generating “randomness” is to use a deterministic pseudo-random generator;
      - must be designed and implemented well – simply counting the milliseconds since midnight on the system clock is not normally good enough!
    - Poor key management:
      - cryptographic key management is a complex issue;
      - cannot properly protect long cryptographic keys with potentially weak short passwords.
    - Customised cryptography.

Contents

- What is trusted computing?
- The TCG
- TCG – TPM and TSS
- Software security – How can trusted computing help?
- Using trusted computing functionality
- Conclusions

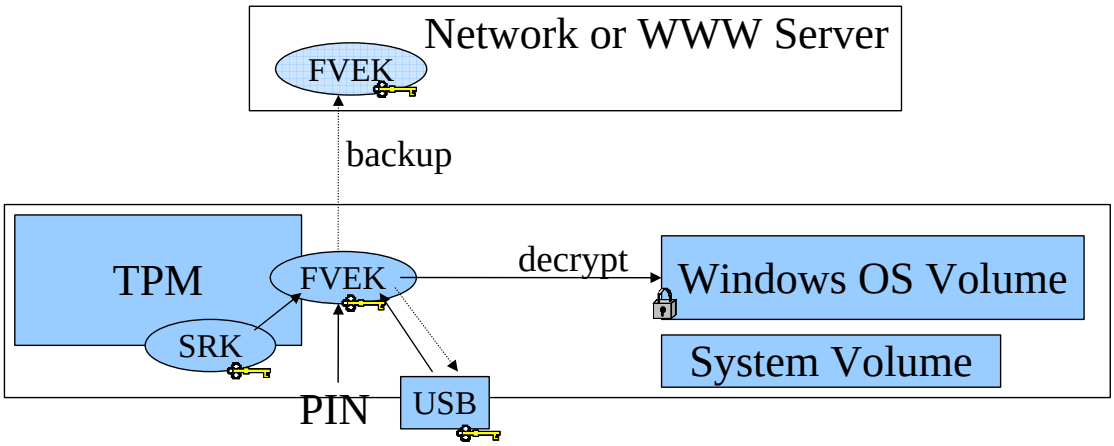
Microsoft Vista security features

- BitLocker – secure drive encryption using TPM features.
- BitLocker only available in Enterprise version of Vista.
- Almost certainly because it is very dangerous to users unless a proper backup strategy is also deployed.
- Visa also supports a TPM-based ‘partial’ secure boot.

Windows Vista BitLocker (1)

- BitLocker Drive Encryption (BDE) designed to protect data from offline viewing – uses a v1.2 TPM:
  - There is a potentially huge threat from offline attacks against PC data, particularly on notebook PCs;
  - Bonus: secure decommissioning by deleting the keys!
- Two volume categories:
  - System volume (unencrypted)
    - MBR, Boot manager and utilities
  - OS volume
    - OS, page/temp/hibernation file, data
- Five default key storage options:
  - TPM, TPM+PIN, TPM+USB, USB, Recovery password

Windows Vista BitLocker (2)



- When first starting BDE:
  - BDE verifies the partition layout and that the TPM is activated;
  - User selects his/her desired recovery backup method;
  - BDE encrypts the OS volume.

A crypto chip in every PC

- Putting a TPM on every PC motherboard means that every PC will have a crypto chip, with secure key storage, a random number generator, ...
- Possible security applications for such a chip are almost endless.
- For example, currently there are PC crypto boards available.
- These can be used to make a PC into a secure system, e.g. to:
  - run a Certification Authority as part of a PKI;
  - to perform key management functions for a company network;
  - ...
- In some cases, the TPM may be sufficiently secure to avoid the need for a separate crypto board.

Managing distributed systems

- In the long term, one of the key roles envisaged for trusted computing is to enable the secure management of distributed systems (especially in a corporate setting).
- One node in the distributed system can test the level of security offered by another node before deciding what types of task it can safely delegate to that node.
- That is, security policies can be automatically enforced.
- However, there is a long way to go ...

Other applications

- A huge variety of applications have been suggested for trusted computing functionality.
- Examples include:
  - secure signature generation;
  - digital rights management (DRM);
  - secure identities for peer-to-peer computing;
  - control of personal information;
  - ...
- However, what will actually happen is far from clear!

Contents

Resources

- www.trustedcomputinggroup.org
- http://www.microsoft.com/windowsvista/default.aspx
- http://www.intel.com/technology/security/
- http://os.inf.tu-dresden.de/L4/LinuxOnL4/
- http://www.opentc.net/
- Siani Pearson (editor), *Trusted Computing Platforms – TCPA Technology in Context*, HP Invent.
- Chris Mitchell (editor), *Trusted Computing*, IEE (London), 2005.

Acknowledgements

- Must thank Eimear Gallery and Stéphane Lo Presti for preparing many of the slides in this presentation.

The Open-TC project is co-financed by the EC.

If you need further information, please visit our website www.opentc.net or contact the coordinator:

Technikon Forschungs- und Planungsgesellschaft mbH
Richard-Wagner-Strasse 7, 9500 Villach, AUSTRIA
Tel. +43 4242 23355 – 0
Fax. +43 4242 23355 – 77
Email coordination@opentc.net