Trusted Computing for Military Applications

Rich Goyette

Introduction

- Evolution of trusted computing technologies.
- Digital Rights Management
- Trusted Computing Initiatives
- Virtualization Technologies
- Tying it all together – Benefits for the Military and Corporate World

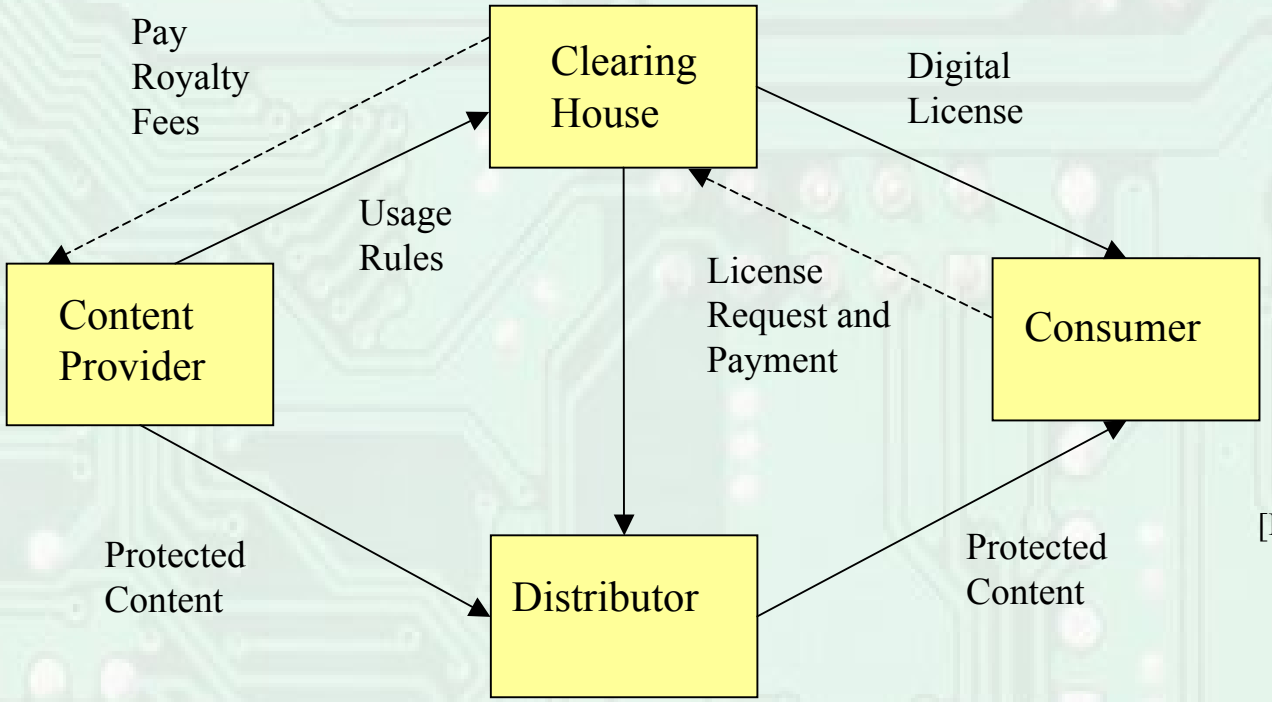
Digital Rights Management

Digital Rights Management

- DRM: "a collection of technologies that enable technically enforced licensing of digital information" [Koe04]
- DRM promises finer-grained control of content usage but:
  - Severely challenges currently accepted models of "fair use"; and
  - Invokes privacy concerns.

Digital Rights Management

Academic Model



[Liu03-1]

Digital Rights Management

- Moving Picture Experts Group (MPEG) is seeking to build DRM standards. MPEG-21 std will:
  - understand, integrate, and standardize all of the disparate elements that exist *now* for DRM
  - perform a gap analysis; and
  - fill in where standards appear to be lacking
- MPEG-21 is attempting to build the "big picture" of digital rights management

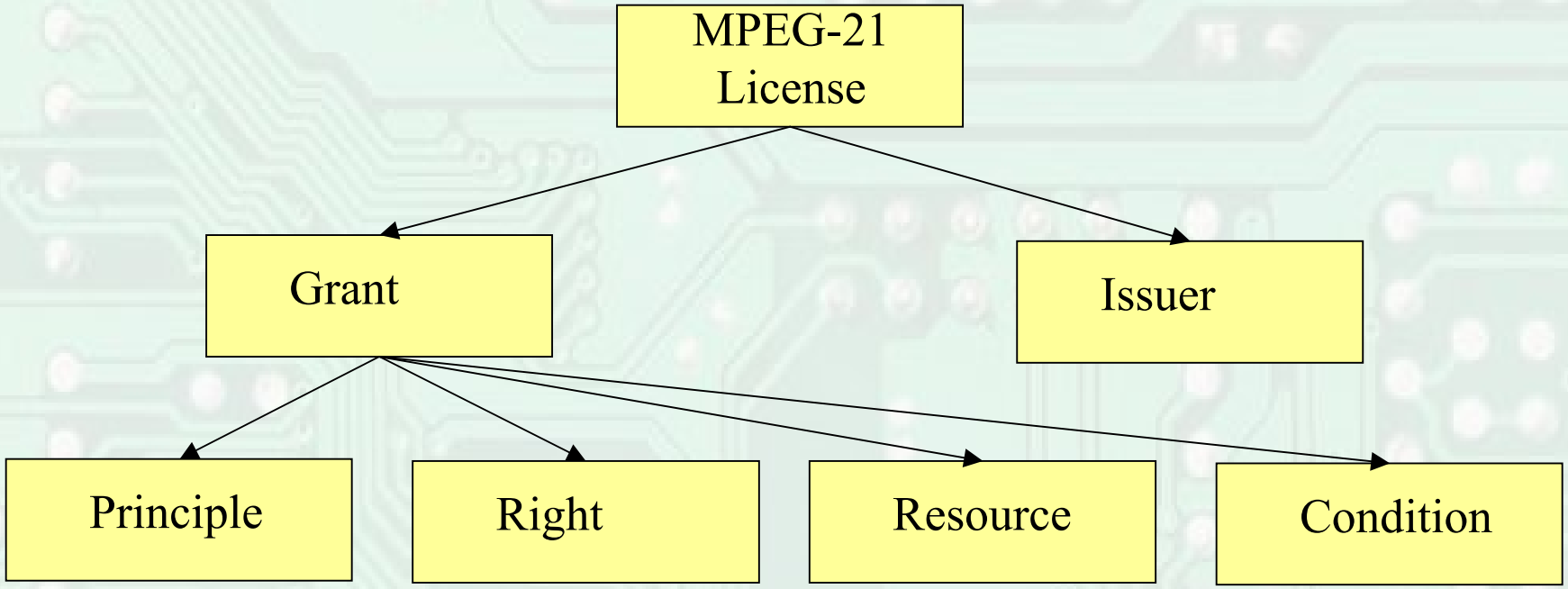
Digital Rights Management

- MPEG-21 Parts:
  - Vision, technologies, and strategies (introduction);
  - Digital Item Declaration (DID);
  - Digital Item Identification (DII);
  - Intellectual Property Management and Protection (IPMP) (continues MPEG-4 hooks to proprietary systems)
  - Rights Expression Language (REL);
  - Rights Data Dictionary (RDD); and
  - Digital Item Adaptation (DIA);

Digital Rights Management

- MPEG-21 Rights Expression Language (REL):
  - Based on ContentGuard's XrML
  - Achieved standard status in early 2004.
  - A *License* is the most important concept in the REL.

Digital Rights Management



[Wang-1]

Digital Rights Management

- Trusted Computing is the "lynch-pin" of all DRM systems. The *client* must ensure that:
  - The consumer obeys the rules set out in the DRM license; and
  - The client cannot separate the rights from the payload and thereby "free" the content.
- Music and video industry have been "burned" already.
- Other industries (e.g., books) don't want to let their content go digital until it is safe…

Digital Rights Management

- DRM "Quick History"
  - December 2001, MS receives patent rights for a DRM OS (patent #6,330,670)

> A digital rights management operating system protects rights-managed data, such as downloaded content, from access by untrusted programs …
>
> …the digital rights management operating system refuses to load an untrusted program into memory while the trusted application is executing…
>
> …also limits the functions the user can perform on the rights-managed data and the trusted application…

[Crypt02]

Digital Rights Management

- DRM "Quick History"
  - Summer 2002 MS initiates "Palladium" which it claims will:
    - Stop viruses and filter spam;
    - Store personal data within an encrypted folder;
    - Depend on hardware that has either a digital signature or a *tracking number;*
    - Incorporate Digital Rights Management technologies for media files of all types (music, documents, e-mail communications).

[Epic02]

Digital Rights Management

- DRM "Quick History"
  - Palladium requires hardware support;
  - MS recruits Intel and AMD to provide this support;
  - Intel gets "burned" on the market when it implements a track-able serial number in its CPUs;
  - Privacy and "fair use" issues cause adverse public reaction and sink the Palladium effort.

[TC03]

Digital Rights Management

- DRM "Quick History"
  - Issues with Palladium that draw fire:
    - Identity – individuals can be tracked by industry or governments;
    - Policing –
      - Computer can turn in individuals running pirated applications;
      - Police can effect warrants to freeze or report content;
    - End of Fair Use – tighter grained control possible;
    - Vendor (MS) lock-in;

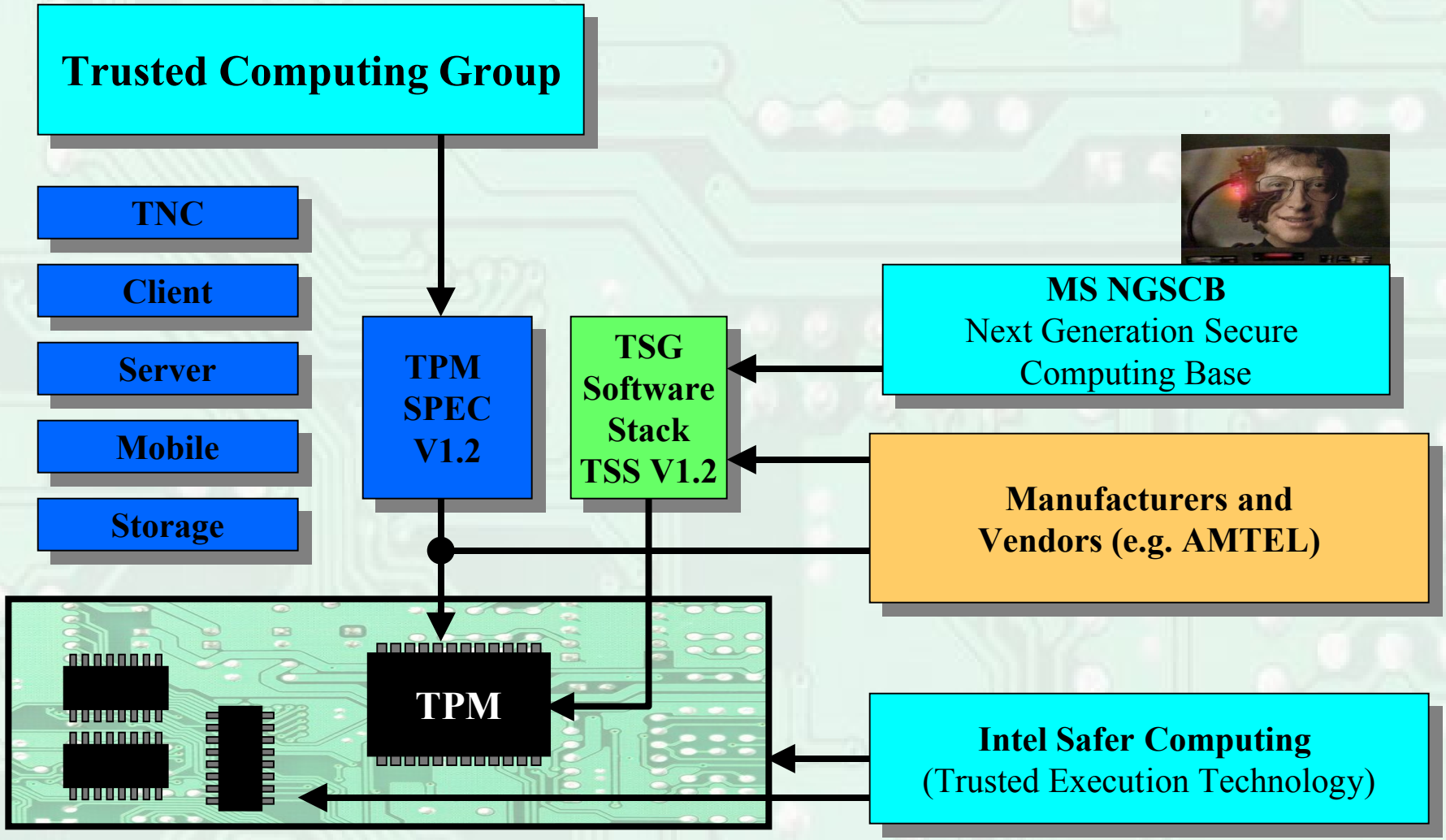
Digital Rights Management

- DRM "Quick History"
  - MS/Intel/AMD etc scramble after Palladium;
  - Eventually "seek safety in numbers" [TC03] by forming Trusted Computing Platform Alliance (TCPA);
  - To keep public off-balance, TCPA is incorporated in 2003 and changes name to Trusted Computing Group (TCG);
  - TCG takes "security of platform" approach and attempts unsuccessfully to shake association with DRM.

Trusted Computing

Current Initiatives

Trusted Computing Initiatives



Trusted Computing Group (TCG)

- Consortium of AMD, HP, IBM, Intel, MicroSoft, Sun.
- Responsible for TPM and TSS upon which other technologies based.

TCG Mission

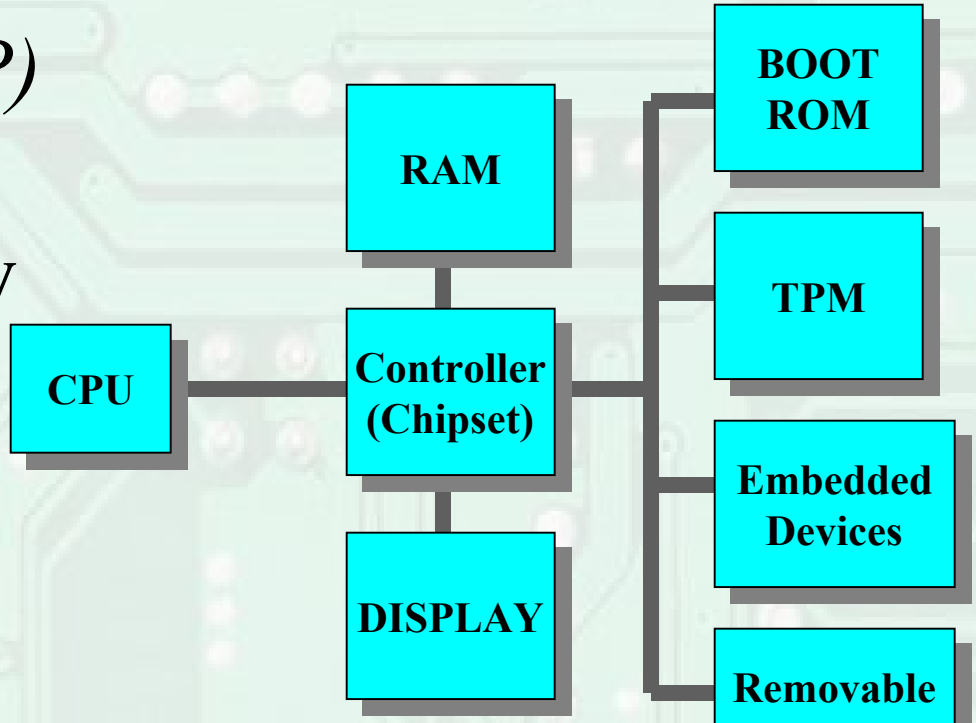
- Mission: to develop *specifications* for a *trusted computing platform*.
- Specifications:
  - Open specifications for architectures, functions, and interfaces independent of platform implementation; (picture)
  - Specifications for specific platform implementations (such as PDA, PC, cell phone, etc)

The Trusted Platform (TP)

- Trusted Platforms (TPs) are computing platforms that include a set of built-in hardware components which are used as a basis for creating trust in software processes.
- Trusted Components are:
  - Core Root of Trust for Measurement (CRTM); and
  - Trusted Platform Module (TPM).
- Trusted Components are hardwired to the motherboard or embedded in firmware. [bruschi]

The Trusted Platform (TP)

- *Trusted platform (TP)* combines hardware and software security to provide trusted client device.
- Trust originates at TPM.



Reference PC Architecture

Fundamental TP Features

- A trusted platform should provide the following:
  - Protected Capabilities
    - TPM
  - Integrity Measurement and Storage
    - Roots of Trust
    - Trusted Building Blocks (TBB)
  - Integrity Reporting
    - Attestation

Fundamental TP Features TPM

- Protected Capabilities:
  - A set of commands with exclusive permission to *shielded locations*.
  - Shielded locations – places (memory, registers, etc,) where it is safe to operate on sensitive data. adjust
  - **TPM** is used to provide protected capabilities and shielded locations to the trusted platform.

Fundamental TP Features TPM

- **TPM** – physically attached to motherboard;
- Function:
  - Protected processing (crypto functions, SHA-1, RSA);
  - Protected storage – used to create, store, manage crypto keys;
- Comes with pre-installed with unique *Endorsement* and *Storage* keys (EK and SK);

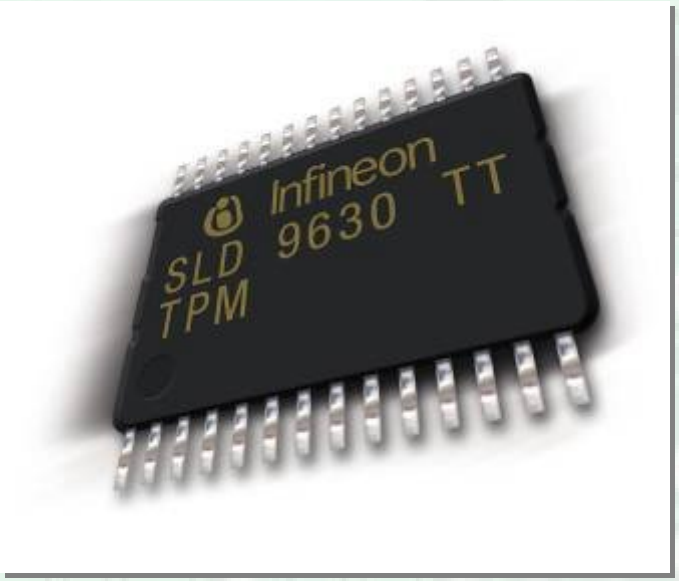
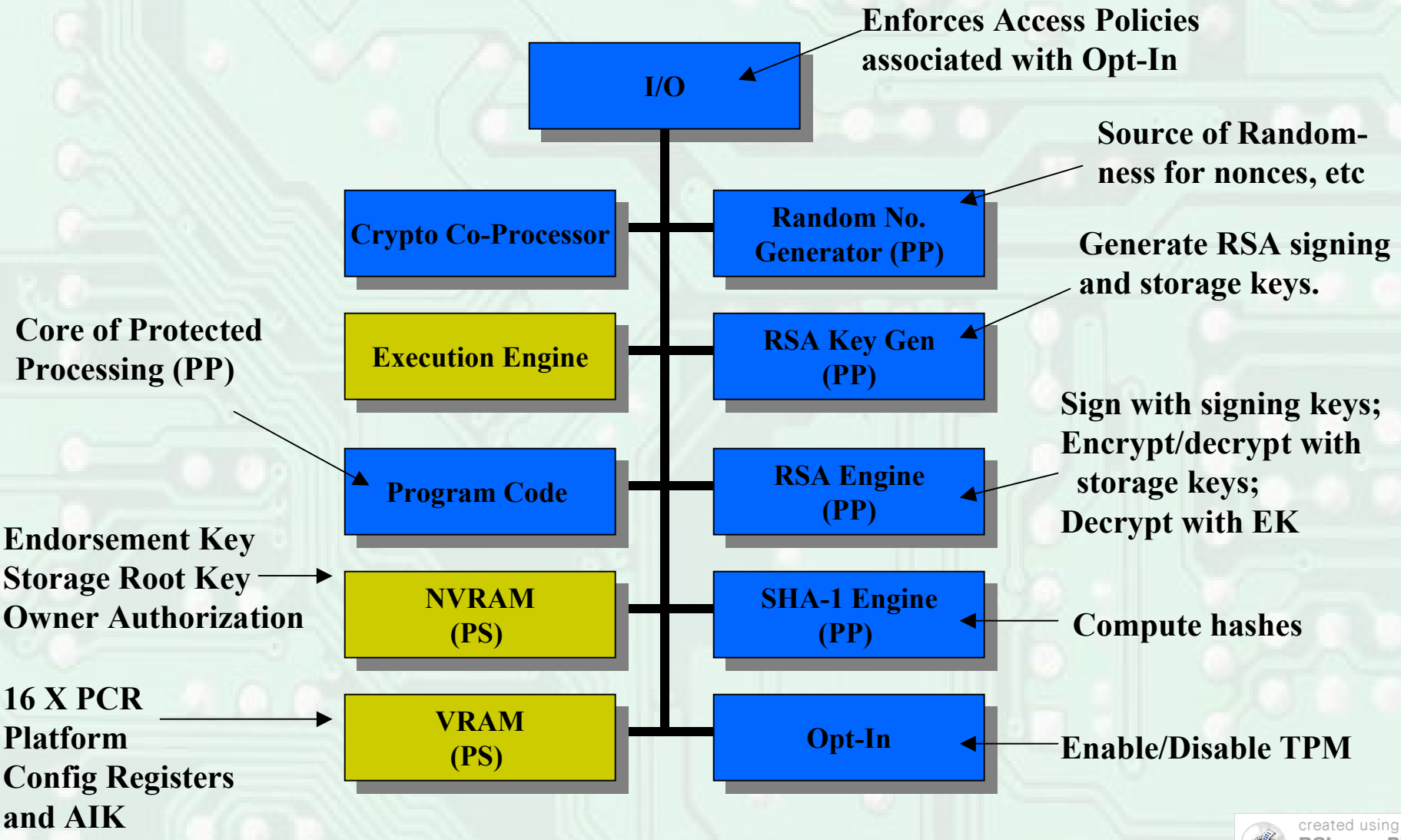


Figure from: TW04053_WINHEC2004.ppt

Fundamental TP Features TPM

- TPM provides:
  - Protected Storage of secrets and "measurements" made of software/hardware;
  - Protected Processing;
- TPM is a hardware component. The conclusion is:
  - Can't be moved or swapped (easily); and
  - Extremely tamper resistant.

Fundamental TP Features TPM



Fundamental TP Features TPM

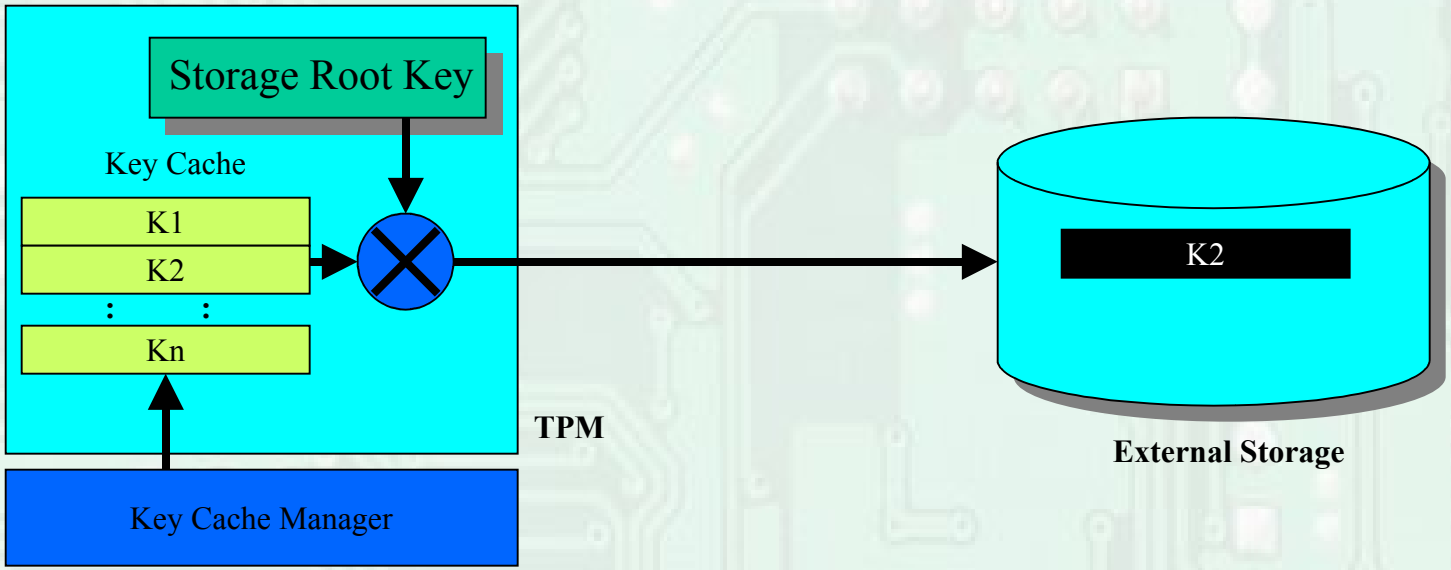
- Endorsement Key:
  - 2048 bit RSA key pair created and embedded at manufacture time.
  - Used for attestation and for encrypting data for the TPM.
  - Can be disabled by owner (privacy).

Fundamental TP Features TPM

- Storage Root Key:
  - 2048 bit RSA key pair.
  - Embedded at manufacture.
  - New pair can be created as part of TPM-TakeOwnership command.
- Owner Authorization Secret Key (not built-in):
  - 160 bit secret shared with owner of TPM.
  - Loaded as part of TakeOwnership.
  - Used to authorize sensitive owner commands

Fundamental TP Features TPM

- TPM facilitates unlimited protected storage through external key cache management.



Fundamental TP Features

- A trusted platform should provide the following:
  - Protected Capabilities
    - TPM
  - Integrity Measurement and Storage
    - Roots of Trust
    - Trusted Building Blocks (TBB)
  - Integrity Reporting
    - Attestation

Fundamental TP Features IM

- Roots of Trust
  - Components that **must** be trusted because mis-behaviour won't be detected otherwise.
  - Trusted by virtue of correct design, inspection, and evaluation (e.g. EAL).
- TCG defines three roots of trust:
  - RTM – root of trust for measurement.
  - RTS – root of trust for storage.
  - RTR – root of trust for reporting.

Fundamental TP Features IM

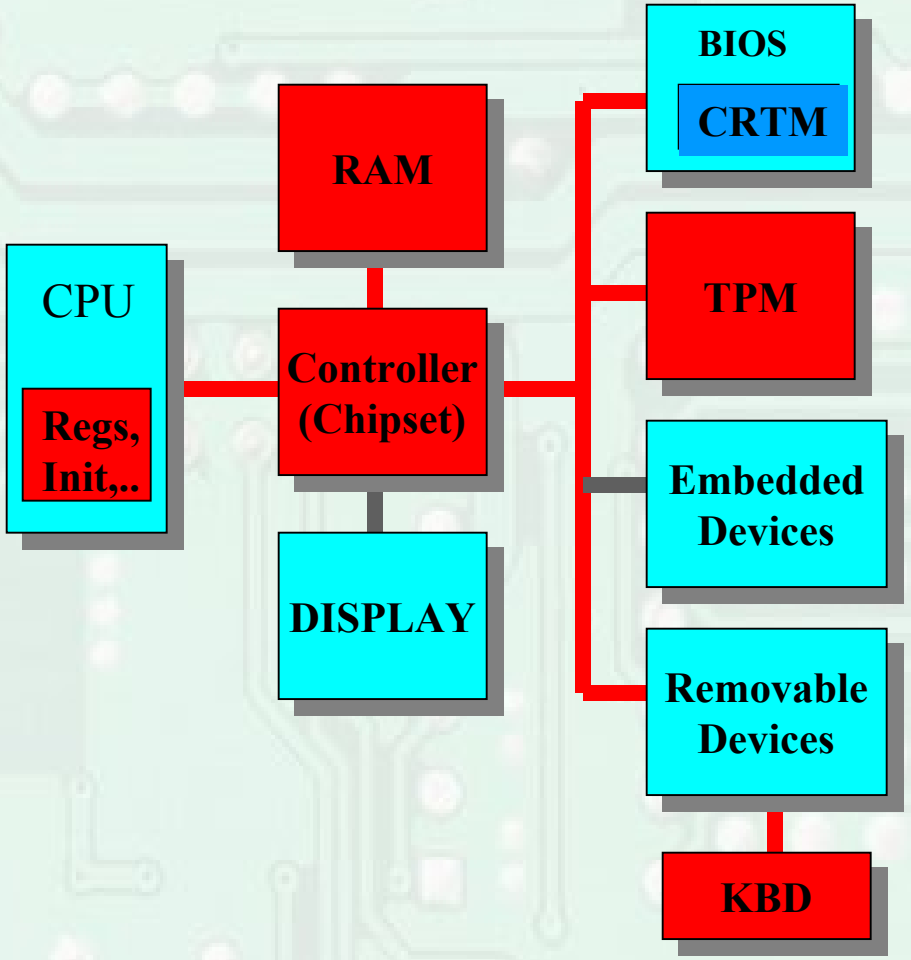
- What is Integrity Measurement (IM)?
  - IMs are hash computations on certain static software and/or hardware values;
  - IMs are securely stored in TPM PCR (protected storage register).
  - *Philosophy* of IM storage and reporting:
    - "A platform can enter any state (including undesirable or insecure states) but the platform is not permitted to lie about the states that it was in." [ref??]

Fundamental TP Features IM

- IM starts at a *root of trust for measurement*:
  - *Static* RTM starts from a well-known state (e.g. POST);
  - *Dynamic* RTM transits from un-trusted to trusted state;
- IM requires a Root of Trust for Measurement (RTM) which is:
  - A computing engine capable of reliable measurement;
  - Consists of normal platform computing environment under control of a *Core Root of Trust for Measurement* (CRTM);
- Root of Trust for Measurement requires *trusted building blocks or TBBs*.

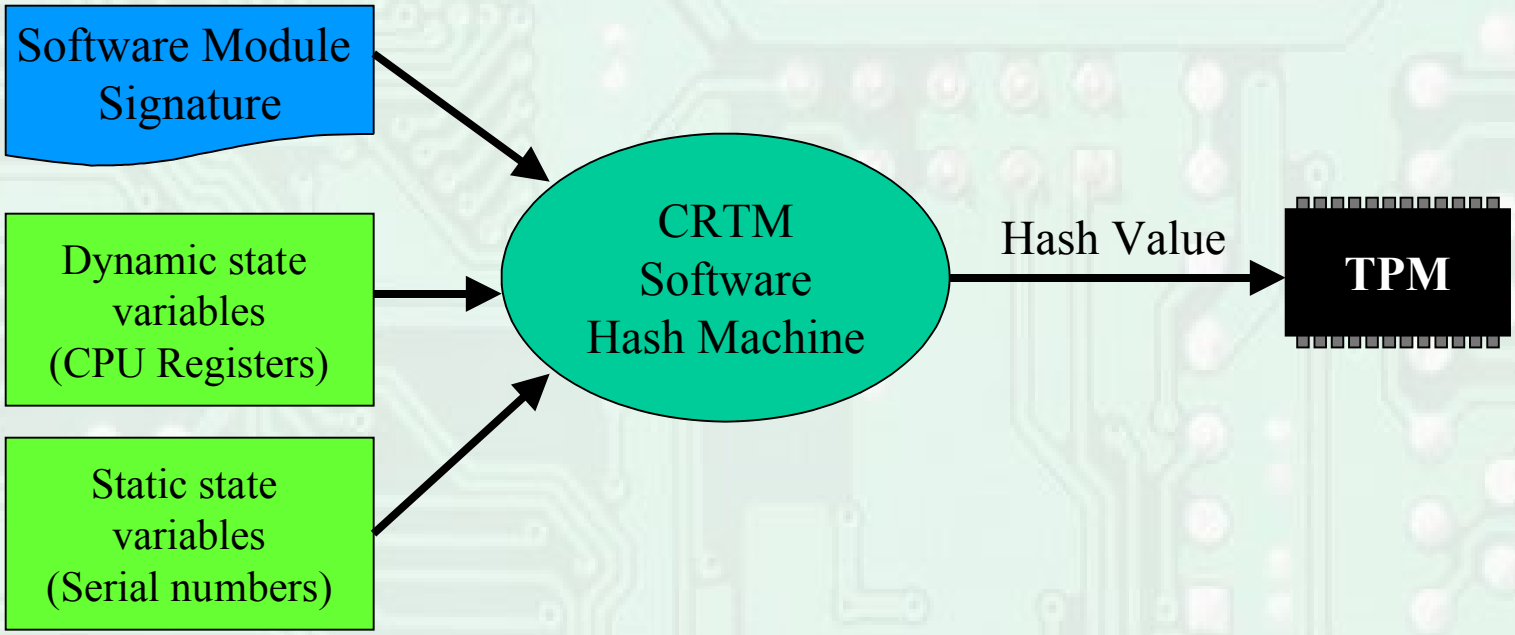
Fundamental TP Features IM

- TBBs *do not* yet have shielded locations or protected capabilities for *some* of their components;
- TBBs are "trusted" (by virtue of design and evaluation)to behave in a way that does not compromise security.

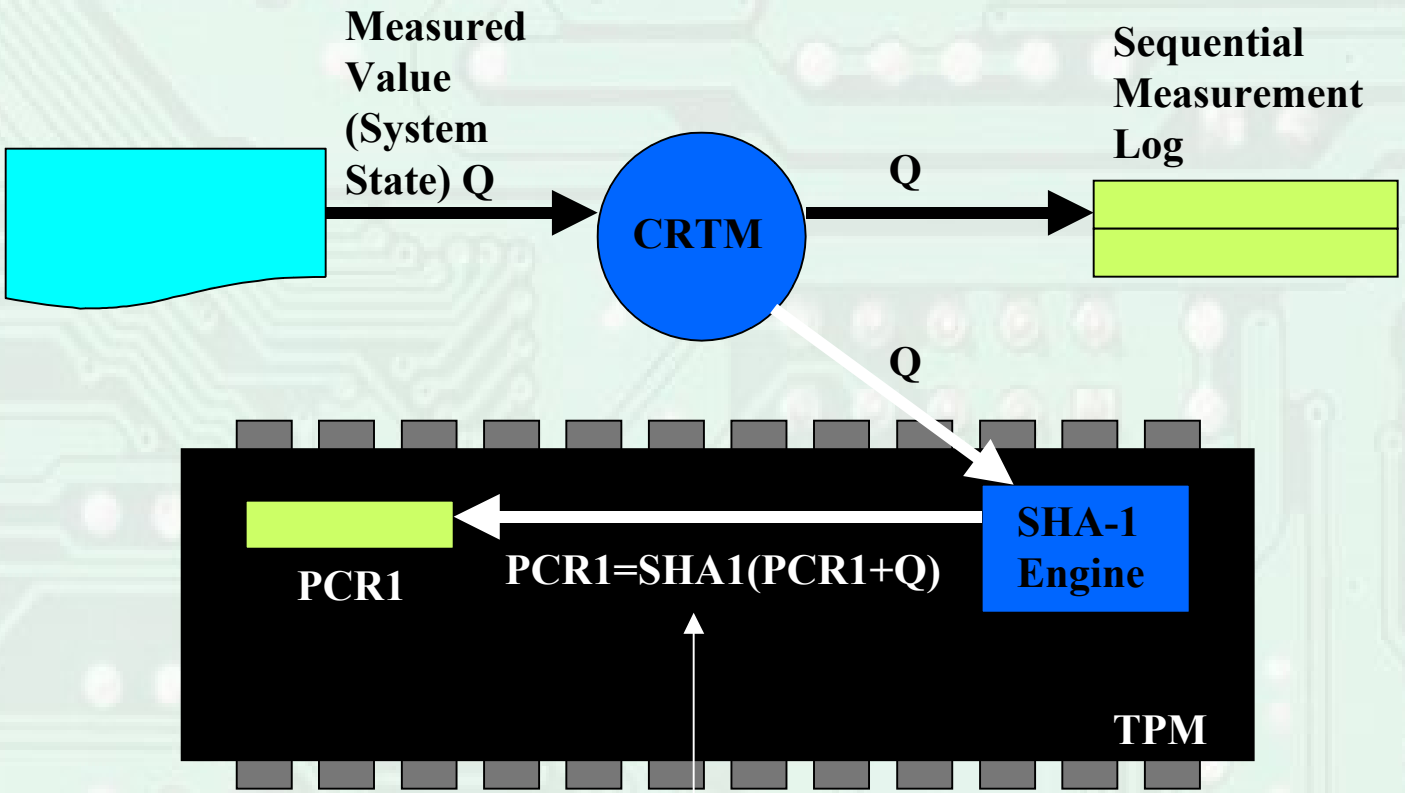


Fundamental TP Features IM

- A semi-worked example of an integrity measurement:

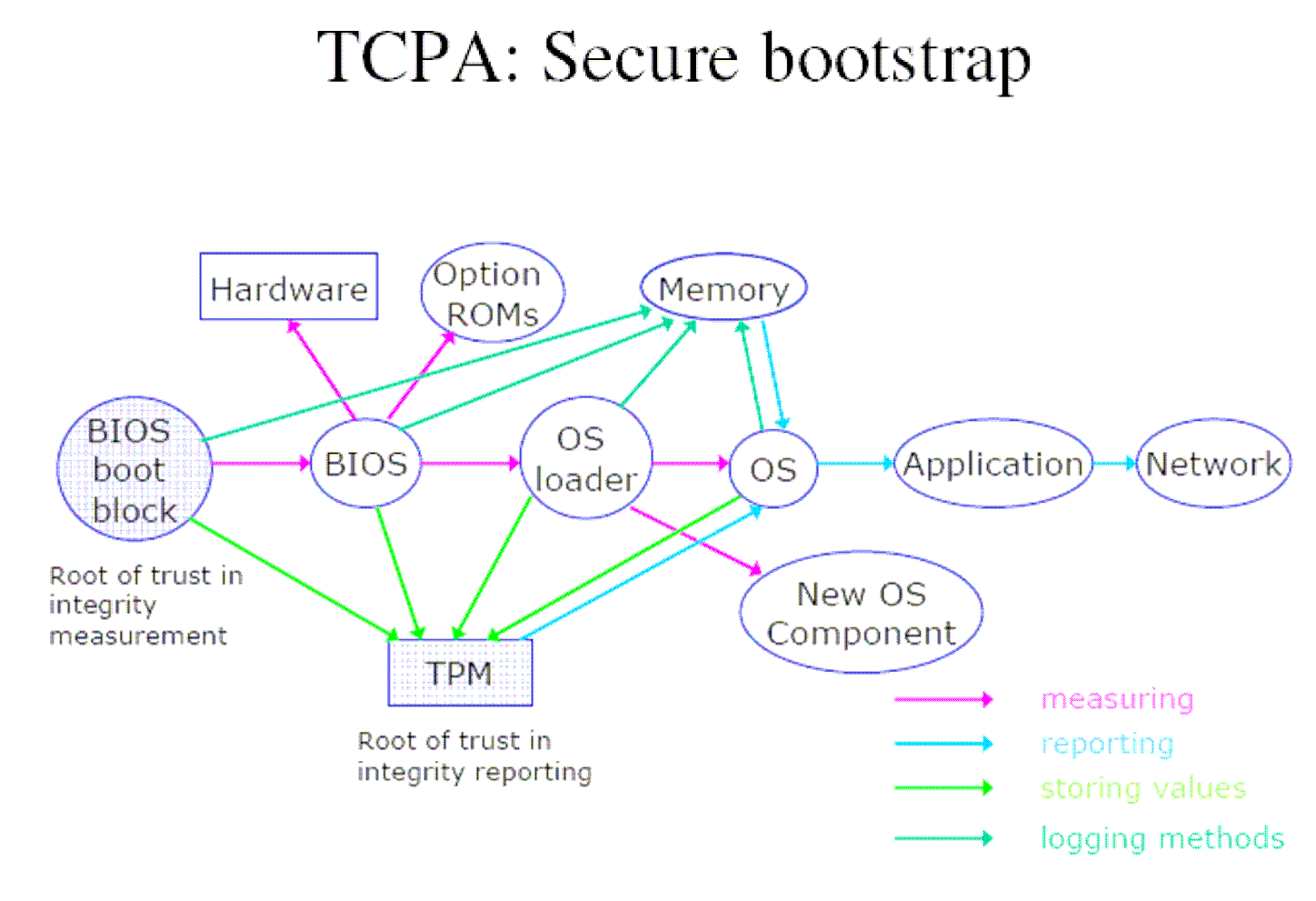


Fundamental TP Features IM



Preserves order and reduces
memory requirement in TPM

Fundamental TP Features IM



Fundamental TP Features

- A trusted platform should provide the following:
  - Protected Capabilities
    - TPM
  - Integrity Measurement and Storage
    - Roots of Trust
    - Trusted Building Blocks (TBB)
  - Integrity Reporting
    - Attestation

Fundamental TP Features ATT

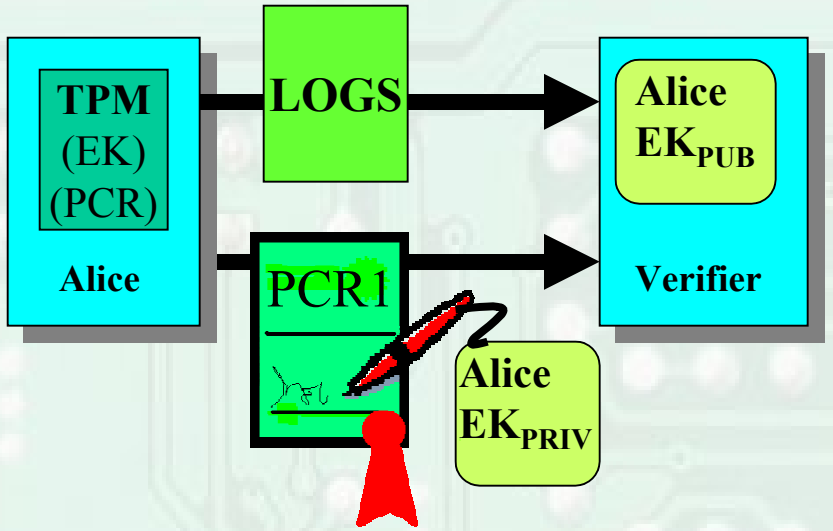
- Attestation – the cornerstone of trust.
  - Process of vouching for the accuracy of information.
  - Attestation:
    - By the TPM;
    - To the trusted platform;
    - Of the platform;
  - Authentication of the platform;

Fundamental TP Features ATT

- **Attestation – by the TPM**
- Provide proof of data known to the TPM;
- Data signed using Attestation Identity Key (AIK – TPM V1.1) or Direct Anonymous Attestation (DAA – TPM V1.2);
- AIK generated by Privacy CA or by other protocol;
- *Verifier* determines acceptability of integrity measurement and AIK

Fundamental TP Features ATT

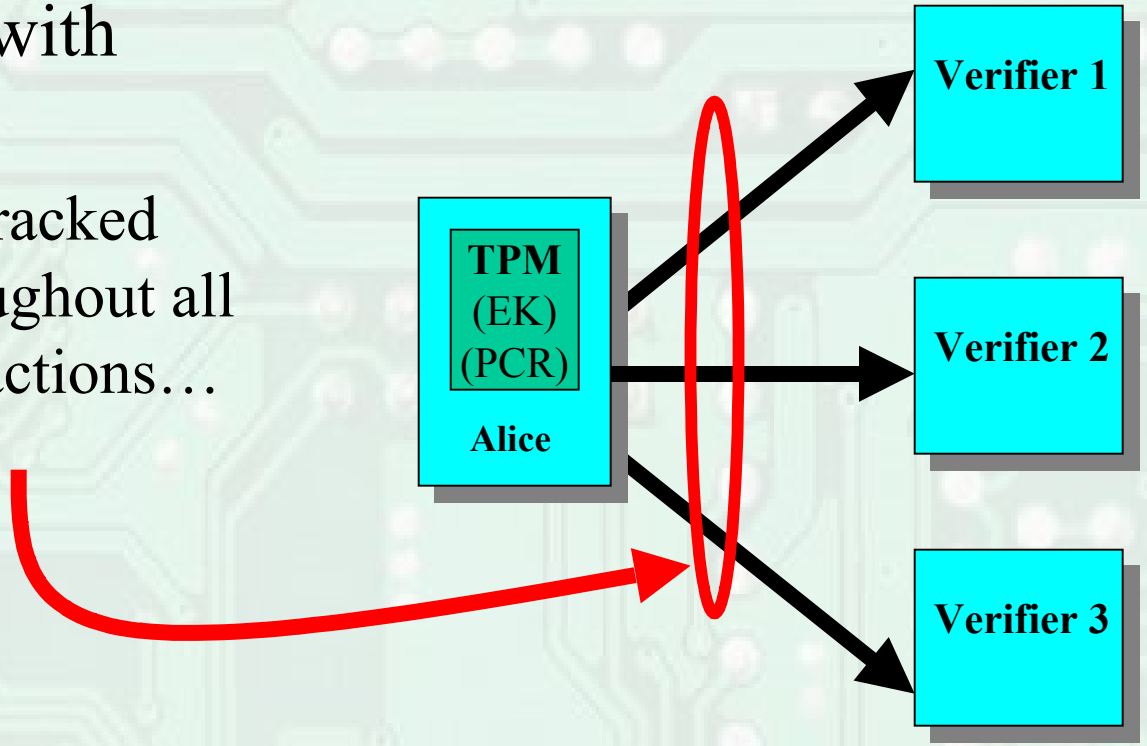
- Attestation using the Endorsement Key (EK)
  - Verifier says “Alice, prove your OS is secure.”
  - Alice says “Here’s my measurement log and a cumulative hash (from a PCR) of the measurements signed with my endorsement key (private EK).
  - Note: Verifier must have received public portion of EK securely or has a copy signed by a CA which is publicly available.



Daa-slides-ZISC.pdf

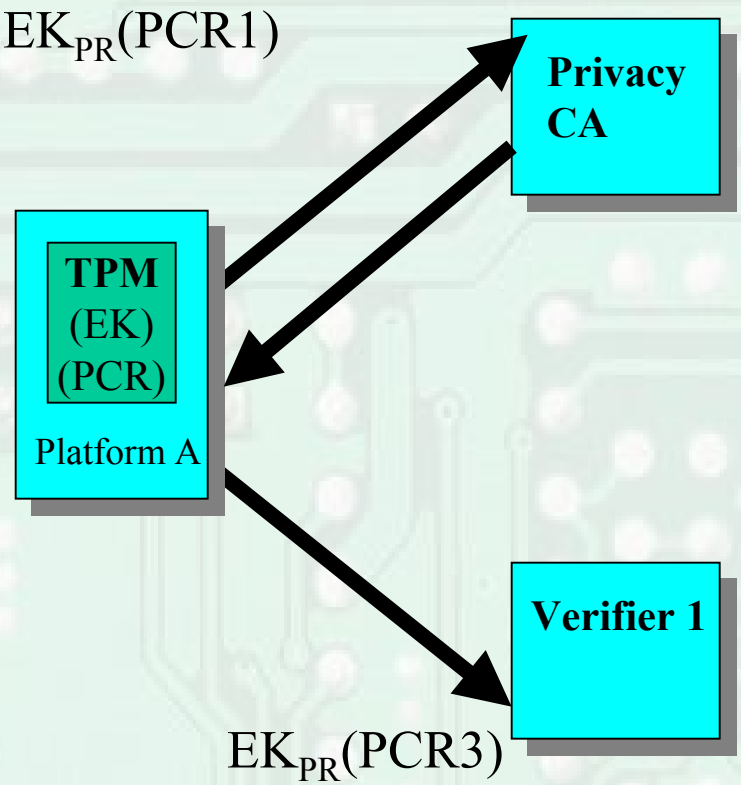
Fundamental TP Features ATT

- **Privacy issue** with using the EK:
  - Alice can be tracked uniquely throughout all of these transactions…



Fundamental TP Features ATT

- The Privacy CA (TPM V1.1):
  - **Alice** generates Attestation Identity Keys (AIK);
  - **Alice** Sends EK and AIK_{PUB} to Privacy CA who verifies good standing of **Alice**.
  - P_{CA} signs AIK, encrypts with EK, and returns to Alice.
  - **Alice** uses signed AIK to attest to Verifier 1.

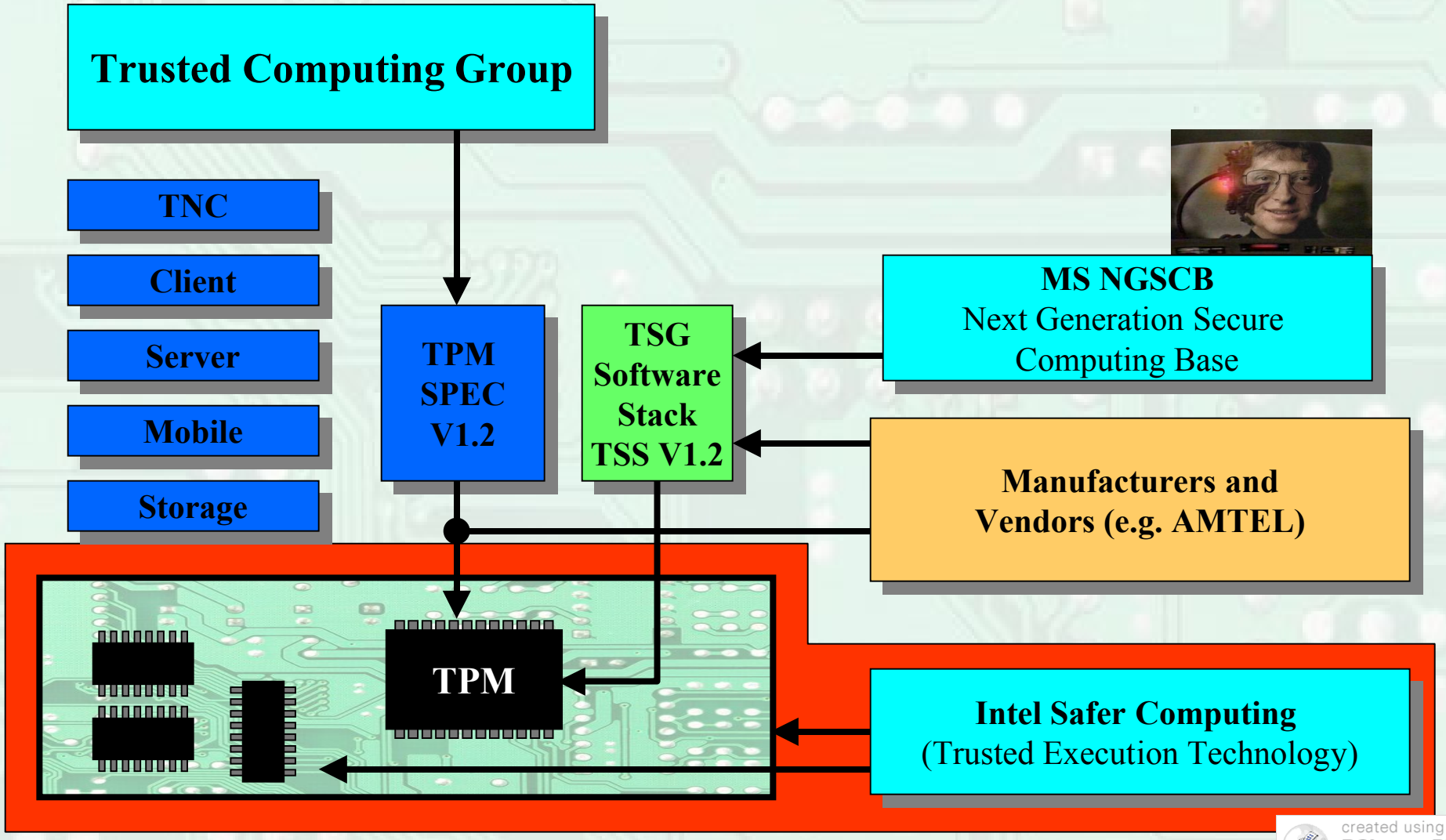


Daa-slides-ZISC.pdf

Fundamental TP Features ATT

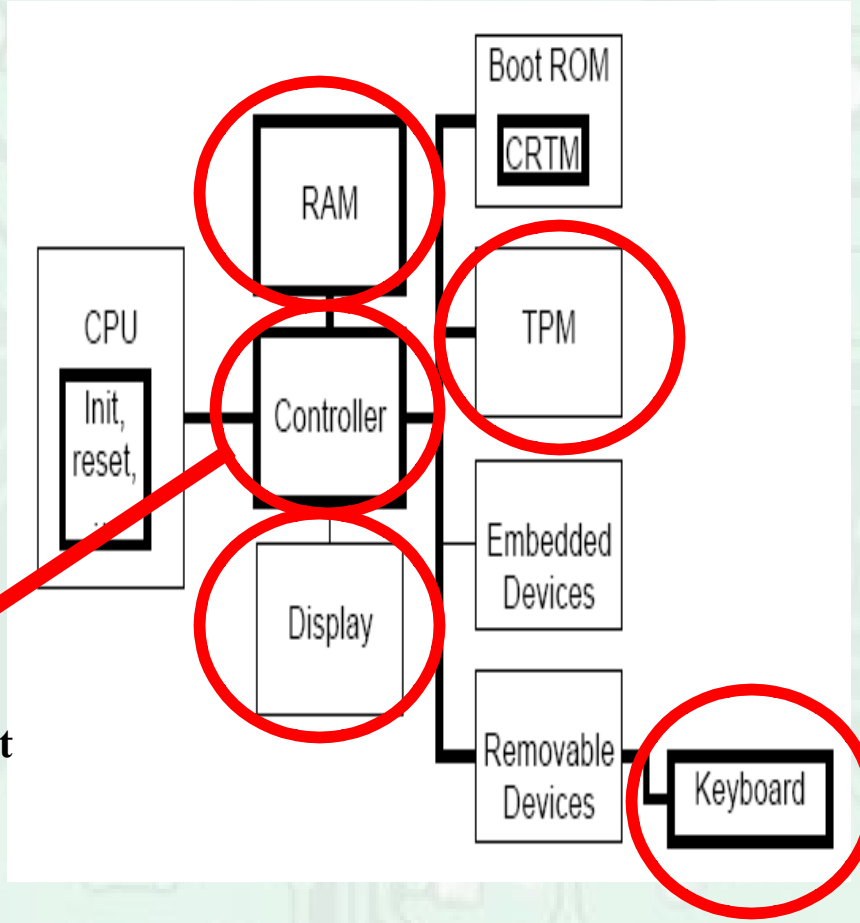
- Privacy CA is problematic:
  - Need for centralized infrastructure;
  - Privacy CA can still supply transaction records to government and police;
- Version 1.2 of TPM uses Direct Anonymous Attestation (DAA) to remove need for Privacy CA.
- DAA is better but not perfect.

Trusted Computing Initiatives



Intel TXT

- TXT is:
  - A set of enhanced hardware components designed to help protect sensitive information from software and certain hardware based attacks.



Chipset Enhancements Provide:

Memory Access Policy Enforcement
Protected access to Graphics
Protected access to I/O
Protected access to TPM

Intel Trusted Execution Technology

- TXT (LaGrande) technology is also promising hardware support for secure virtualization.
- This points to a Multiple Independent Levels of Security (MILS) capability.
- Intel/AMD pushing the hardware virtualization as support to server rationalization.

Virtualization

Virtualization - Definition

- Virtualization is the process of running more than one OS on a single CPU at a time;
- The CPU and system level resources are time-division-multiplexed;
- The “code” that controls the sharing of the system between OSes is variously known as the separation kernel, hypervisor, and virtual machine monitor.

Virtualization - History

- The concept of virtualization has been around since the 70's.
- Virtualization has not been practical until now due to processing speed constraints on the CPU (context switching overhead is high).
- Many *flavours* of virtualization available (Xen, VMWare, Integrity OS, etc).

Virtualization – Server Driven

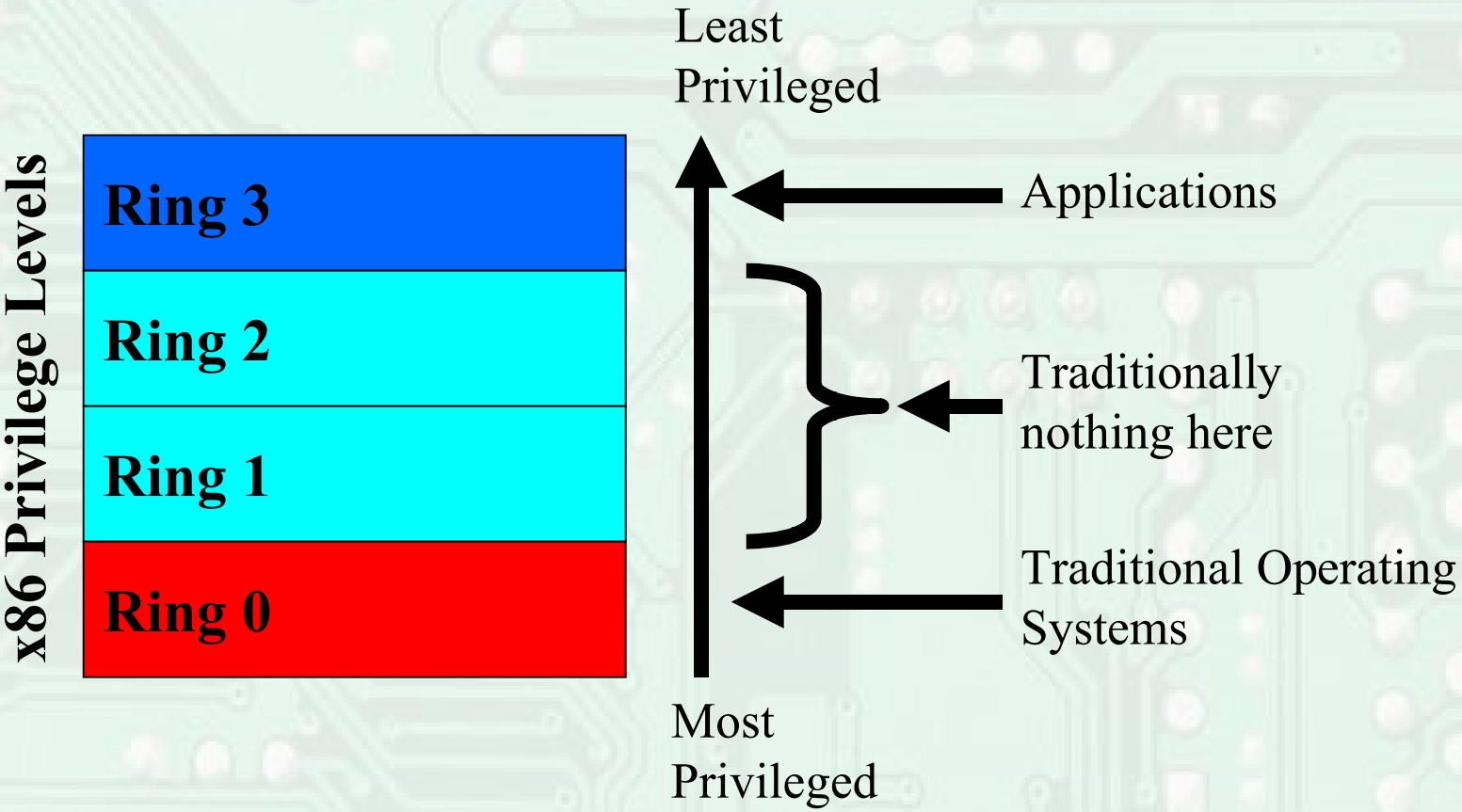
- Virtualization market is being driven primarily by server rationalization.
- Virtualization reduces TCO:
  - Improved utilization;
  - Reduced number of servers;
  - Reduced operating costs (AC, power, etc);
  - etc

[Ber06][Ven06][Bin06]

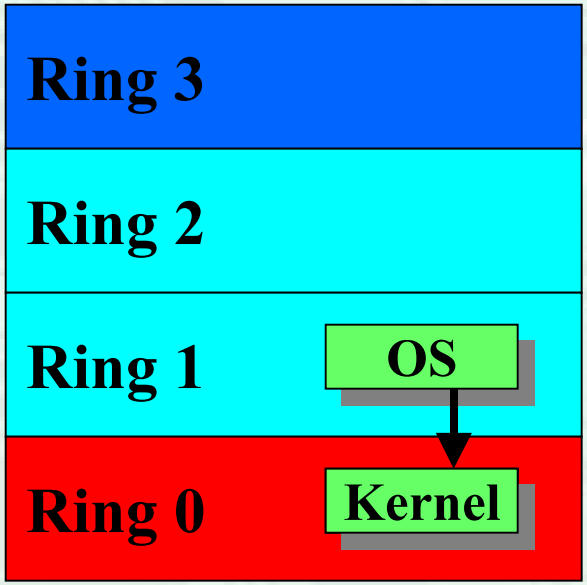
Virtualization - Software

- Software Virtualization is difficult on x86 architectures;
  - x86 CPU's implement "rings" of privilege;
  - OS kernels traditionally expect direct and most privileged control over the CPU;
  - This interferes with virtualization kernel (hypervisor) operation;

Virtualization - Software



Virtualization - Software



- Software virtualization involves ring “de-privileging”.
- Move OS to Ring 1 and intercept “Ring 0 privileged ” instructions.
- Two approaches to de-privileging:
  -Para-virtualization;
  -Binary patching

Virtualization - Software

- Para-virtualization:
  - Create a “hypervisor” that emulates behavior of privileged x86 machine instructions;
  - Modify source code of OS to call emulated instructions and recompile;
  - This only works with an open source OS or OS vendors who are inclined to make para-virtualized versions;
  - Examples: Xen, IBM mainframe Linux clusters

[Dor05][Hud05]

Virtualization - Software

- Binary patching:
  - Perform machine code scanning while OS is running;
  - Dynamically replace privileged machine code with “hypervisor-safe” code;
  - Cache modified binary modules where possible to increase performance;
  - Examples: VMWare, WinXP DOS emulation;
  - Performance is an issue;

[Dor05][Hud05]

Virtualization - Software

- Issues with pure software virtualization:
  - Computing power required:
    - Excessive faulting;
    - CPU state context switching
  - Ring aliasing;
  - Non-trapping instructions;

[Nar05]

Virtualization - Hardware

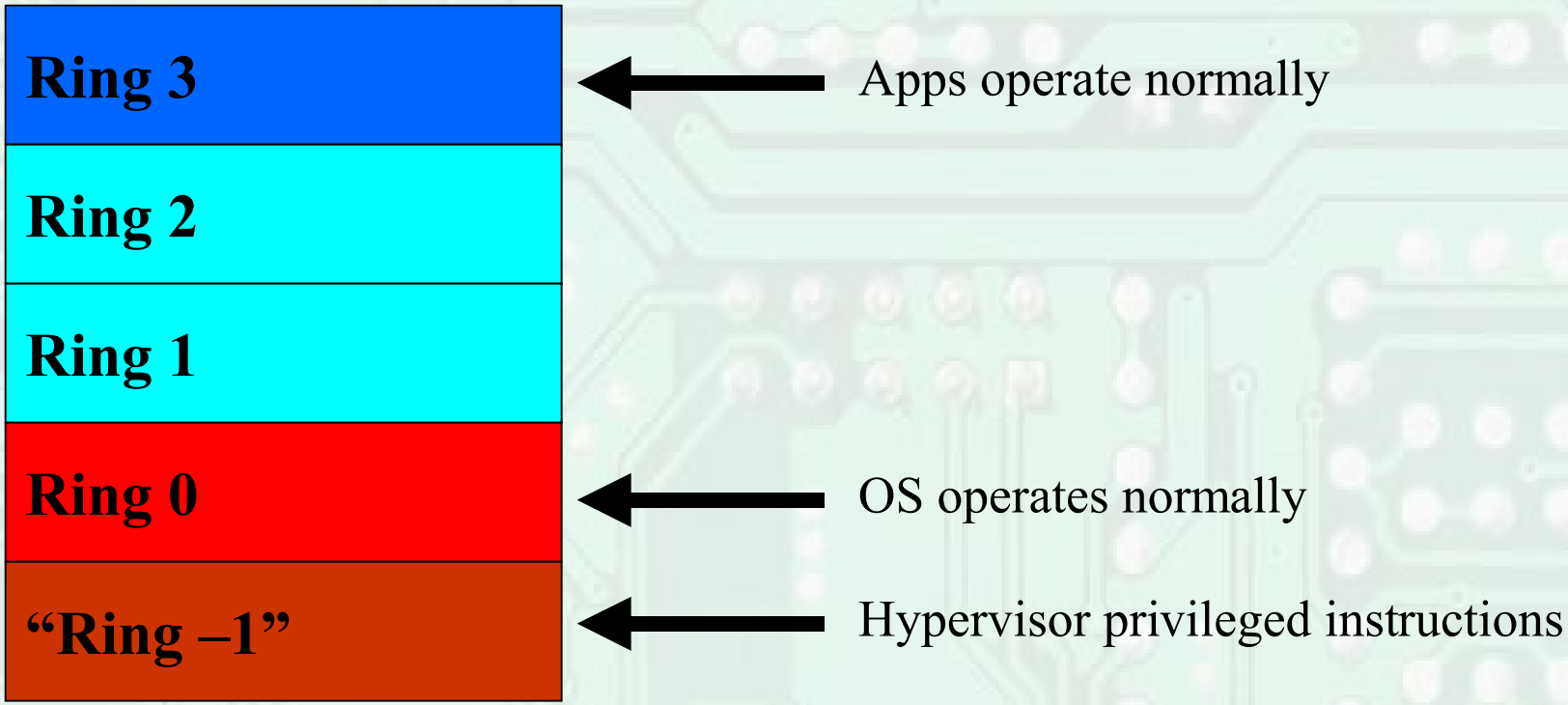
- Concept: implement CPU extensions to make virtualization easier and more secure;
- AMD and Intel have implemented extensions already on some CPUs;
- These extensions are leftovers originating from the original Palladium adventure;

Virtualization - Hardware

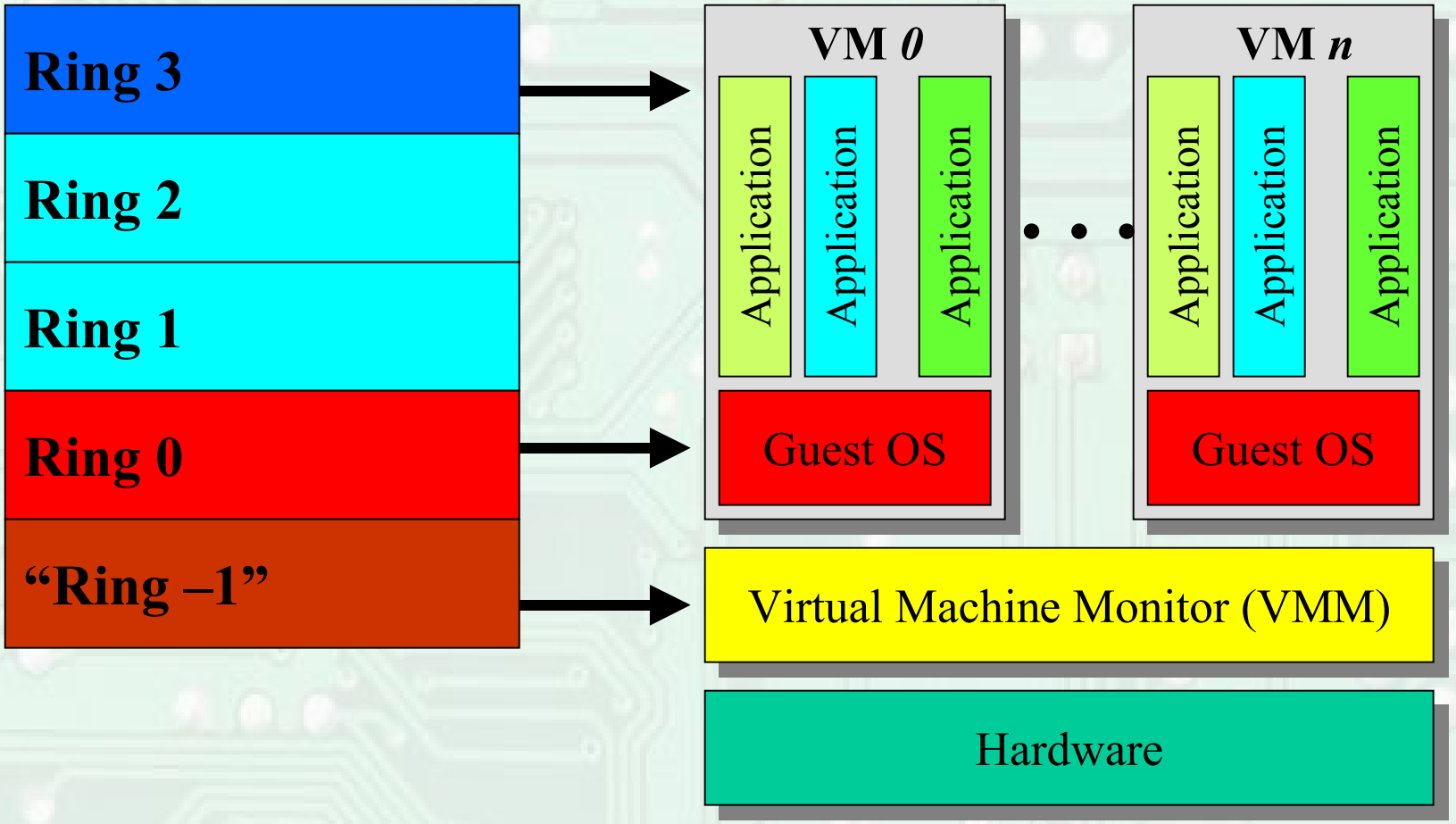
Intel Technology	AMD Technology	Notes
VT-x (aka Vanderpool and Silverdale). Nine new instructions.	**Pacifica** Secure Virtual Machine (SVM) Nine new instructions.	• Intel is targeting secure desktops. AMD is after virtualized servers. • AMD has a slight edge – memory management is on-chip.
Trusted Execution Technology (LaGrande)	Presidio Security Technology	• Encrypted I/O and integration between the TPM and hardware virtualization support.

[Dor05 - 1]

Virtualization - Hardware



Virtualization – Hardware, Intel

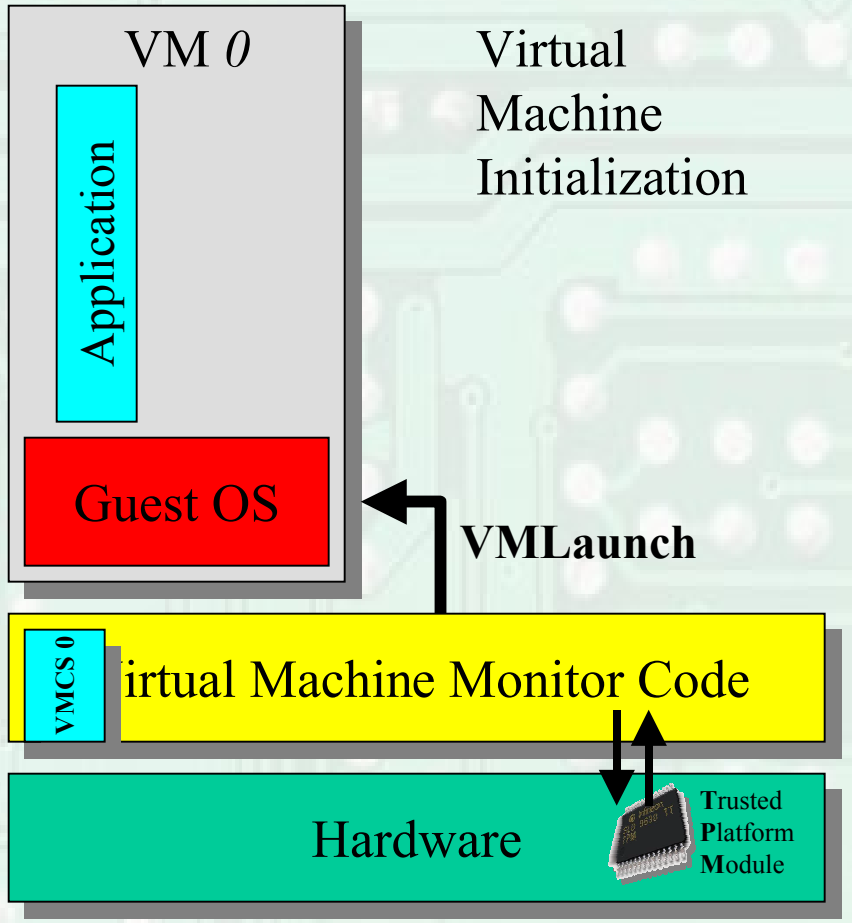


Virtualization – Hardware, Intel

- Intel CPU exists in one of two "modes":
  - VMX Root (Ring –1)
    - This is mode intended for VMM (hypervisor);
    - Fully privileged operation;
  - VMX non-Root (Ring 0)
    - Regular running mode for unmodified guest OSes
  - Certain *key machine code instructions* or events that occur in non-root mode will cause a transition to root mode.

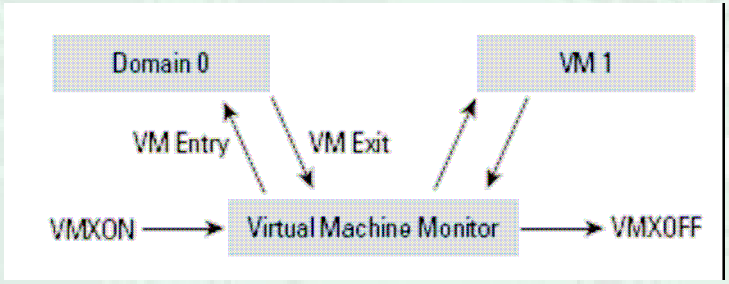
Virtualization – Hardware, Intel

- VMM code boots securely using BIOS and TPM.
- VMM starts guest OS with VMLaunch instruction.
- VM launch creates VMCS for each VM containing:
  - VM execution, exit and entry controls;
  - Guest and host state;
- Guest OS boots application



Virtualization – Hardware, Intel

- VM "Entry"
  - VMM transfers control to VM (non-root).
  - VMLaunch command on first entry;
  - VMResume command on scheduled resume.
- VM "Exit"
  - VM exits transfer control to an entry point specified by the VMM;
  - VM exits are **scheduled or event driven**;
  - VM exits save guest state into VMCS and load VMCS for VMM.



[Dell05-1]

Conclusion

References

[1] R. Sailer, X. Zhang, T. Jaeger, and L. van Doorn. Design and Implementation of a TCG-based Integrity Measurement Architecture. In Proceedings of the 13th Usenix Security Symposium, pages 223–238, August 2004.

[2] W. A. Arbaugh, D. J. Farber, and J. M. Smith. A secure and reliable bootstrap architecture. In SP '97: Proceedings of the 1997 IEEE Symposium on Security and Privacy, pages 65–71. IEEE Computer Society, 1997.

[Fras04] K. Fraser, S. Hand, R. Neugebauer, I. Pratt, A Warfield, M Williamson, Safe hardware access with the xen virtual machine monitor,

[Ber06] S. Berger, R Caceres, K. Goldman, R Perez, R. Sailer, L. van Doorn, vTPM: Virtualizing the Trusted Platform Module, IBM Research Report RC23879 (W0602-126), Feb 2006.

[Nar05] N. Sahgal, D. Rogers, Understanding Intel Virtualization Technology, PowerPoint presentation at xxxx,

[Dor05] A. Dornan, Intel VT vs AMD Pacifica, IT Architect Magazine, Nov 05.
http://www.itarchitectmag.com/shared/article/showArticle.jhtml?articleId=172302134

[Dor05-1] Table 1 from [Dor05]

[Dell05] T. Abels, P. Dhawan, B. Chandrasekaran, An overview of Xen Virtualization, *Dell Power Solutions,* August 2005.

[Dell05-1] Figure 2 from [Dell05].

References

[Koe04] R. Koenen, J. Lacy, M. Mackay, and S. Mitchel, "The long march to interoperable digital rights management," Proceedings of the IEEE, vol., 92, no. 6, June 2004.

[Liu03] Q. Liu, R. Safavi-Naini, and N. Sheppard, "Digital rights management for content distribution," Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003, vol. 21, pp 49-58.

[Liu03-1] Figure 2.1 of [Liu03].]

[28]* P. Biddle, P. England, M. Peinado, and B. William, "The darknet and the future of content distribution," in *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, ed E. Becker, W. Buhse, D. Gunnewig, N. Rump (Springer-Verlag, 2003).

[End04] R. Enderle, "Trusted computing: maligned by misrepresentations and creative fabrications," Storage Pipeline e-magazine, 02 May 2004 (attached).

[O'Rei01] T. O'Reilly, "Microsoft patents 'Digital Rights Management Operating System'", 13 Dec, 2001, available at www.oreillynet.com/cs/user/view/wlg/956 (attached).

[Coy] K. Coyle, Digital Rights Management – Part 4. Available at www.kcoyle.net/drm_basics4.html (attached).

[Wang] X. Wang, T. DeMartini, B. Wragg, M. Paramasivam, C. Barlas, The MPEG-21 rights expression language and rights data dictionary, IEEE Trans on Multimedia, Volume 7, Issue 3, June 2005, pp. 408 – 417.

[Wang-1] Figure 2 from [Wang].

[Epic02] http://www.epic.org/privacy/consumer/microsoft/palladium.html

[Crypt02] http://cryptome.org/ms-drm-os.htm

[TC03] R. Anderson, Trusted Computing FAQ, Version 1.1, http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html, 2003.