Trusted Computing

William A. Arbaugh
Department of Computer Science
University of Maryland
waa @ cs.umd.edu
http://www.cs.umd.edu/~waa

Getting Started

- Would you like to know what software is running on your computer?
- If you don't, then you should.
- If you do, then how do you do it?

Who said?

- "Trust but Verify"

  _____ __ _____

- "Trust is good, but control is better"

Who controls the information?

- Owners of information want to control it:
  - Keeping your medical information private
  - Mickey mouse
  - Preventing the release of damaging info, e.g. Pentagon papers.
- Users want to be able to control the information
  - Back-up copies
  - Whistle blowers, e.g. Pentagon papers

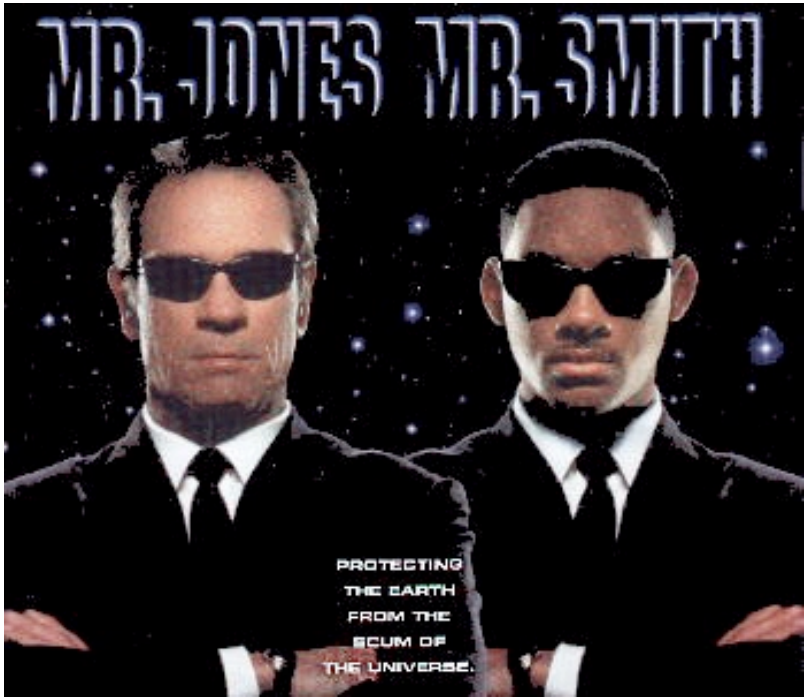
A matter of law

- I'm NOT going to address any further the issue of who controls the information. This is really a matter of law and not technology.
- This is essentially the primary reason for the current debate.

My Goals

- Introduce the technology
- Present the debate while trying to remain unbiased
- Allow you to make your own decision

Black Helicopters?



- A great deal of emotionalism is involved.
- Not all of it is well founded.
- But, we do need to be vigilant to ensure the "right thing" is done.

Talk Outline

- What is trusted computing?
- History of trusted computing
- Reference Monitor
- TCG
- Pre-boot methods
- Post-boot methods
- Examples
- The debate
- Analysis and Predictions
- Conclusions

Trusted Computing?

- Many definitions exist. I prefer one based on Peter Neumann's definitions

An object is trusted if and only if it operates as expected.

An object is trustworthy if and only if it is proven to operate as expected.

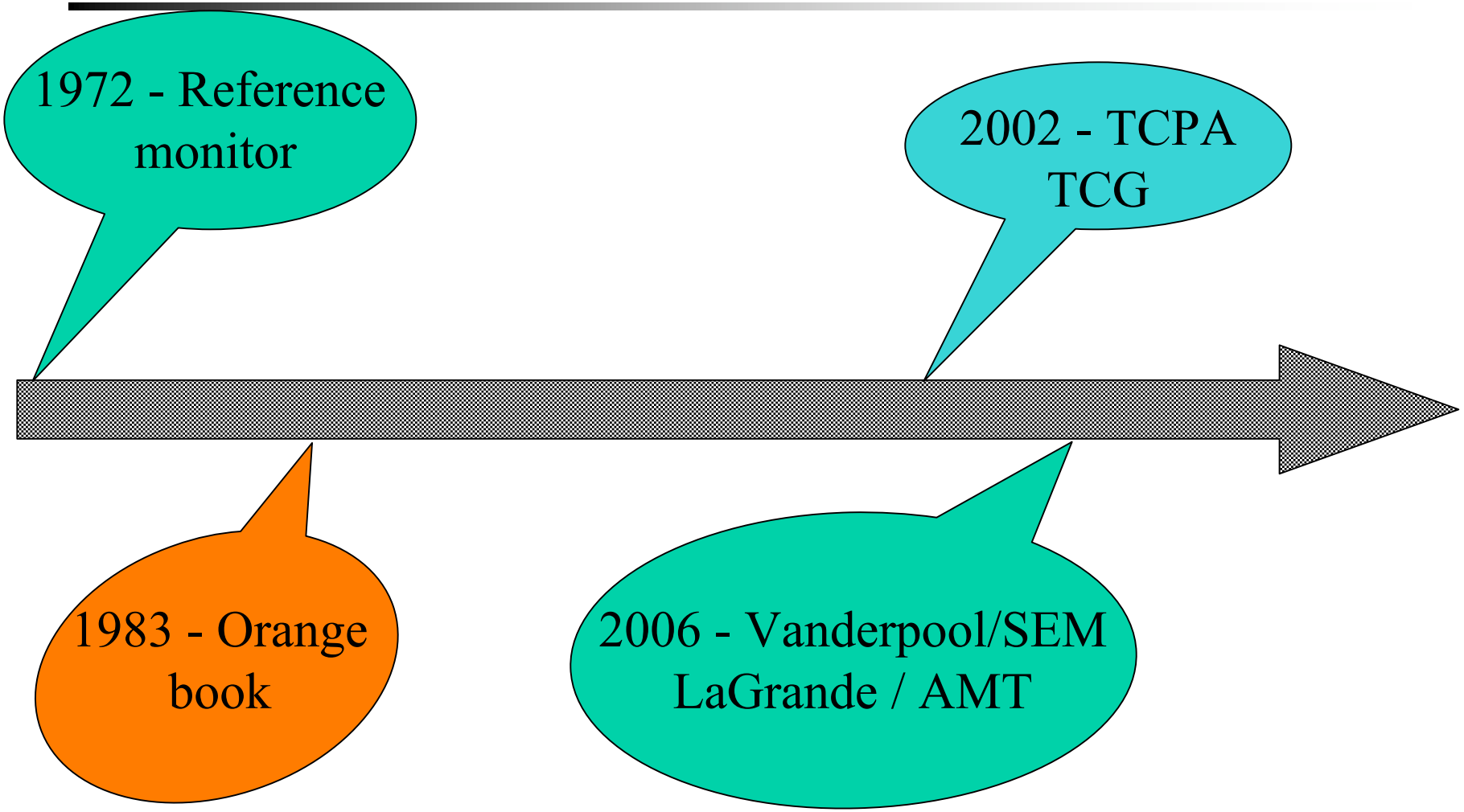
Trusted computing is therefore

- When you computer operates as expected!
- Notice that expectations are not defined here.
  - Those against will say the computer operates as the vendor/IP owner expects.
  - Those in support will say as the owner/operator expects.

Trusted Computing Base

- Aka the TCB - the totality (hardware, firmware, software) of the components responsible for enforcing a security policy.

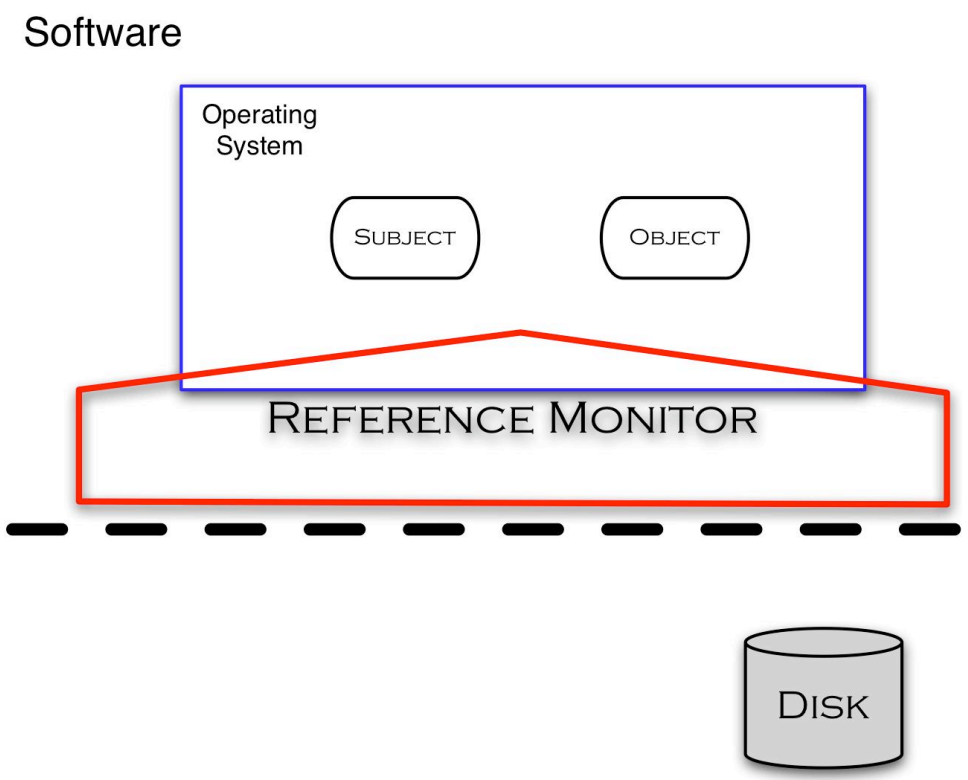
History


1972 - Reference monitor
2002 - TCPA TCG
1983 - Orange book
2006 - Vanderpool/SEM LaGrande / AMT

Reference Monitor

- Idea attributed to Jim Anderson, 1972.
- Is an access control concept of an abstract machine that mediates ALL accesses to objects from subjects.
- A reference validation mechanism (RVM) is an implementation of a reference monitor that is tamperproof and can never be bypassed. The RVM must be small enough to be analyzed and tested well.

Reference monitor



Trusted Computing Group

- Core element is the Trusted Platform Module (TPM)
- The TPM is a passive device. It only does something if commanded over the bus.

TPM Functionality

- Protected storage
  - TPM's shielded locations provide both "on-device" and "off-device" protected storage
  - Multiple identities allowed, but only one device/platform identity permitted
- Protected execution
  - Provides an environment for protected cryptographic functions to execute without modification or exposing key information
- Attestation
  - Attest to current status of both the TPM and the platform on which it resides

TPM PCR register

- Platform Configuration Registers (PCR)
  - Held in volatile storage in TPM
  - Size is 160 bits
  - Initialized to zero at TPM_Init
- NEVER written to directly; ALWAYS extended
  - PCR_{new} = SHA1 (PCR_{old} || Extend value)

Attestation

- A third party entity requests a machine to attest to its configuration along with a nonce.
- TPM signs a PCR value along with the nonce and sends it to the requestor

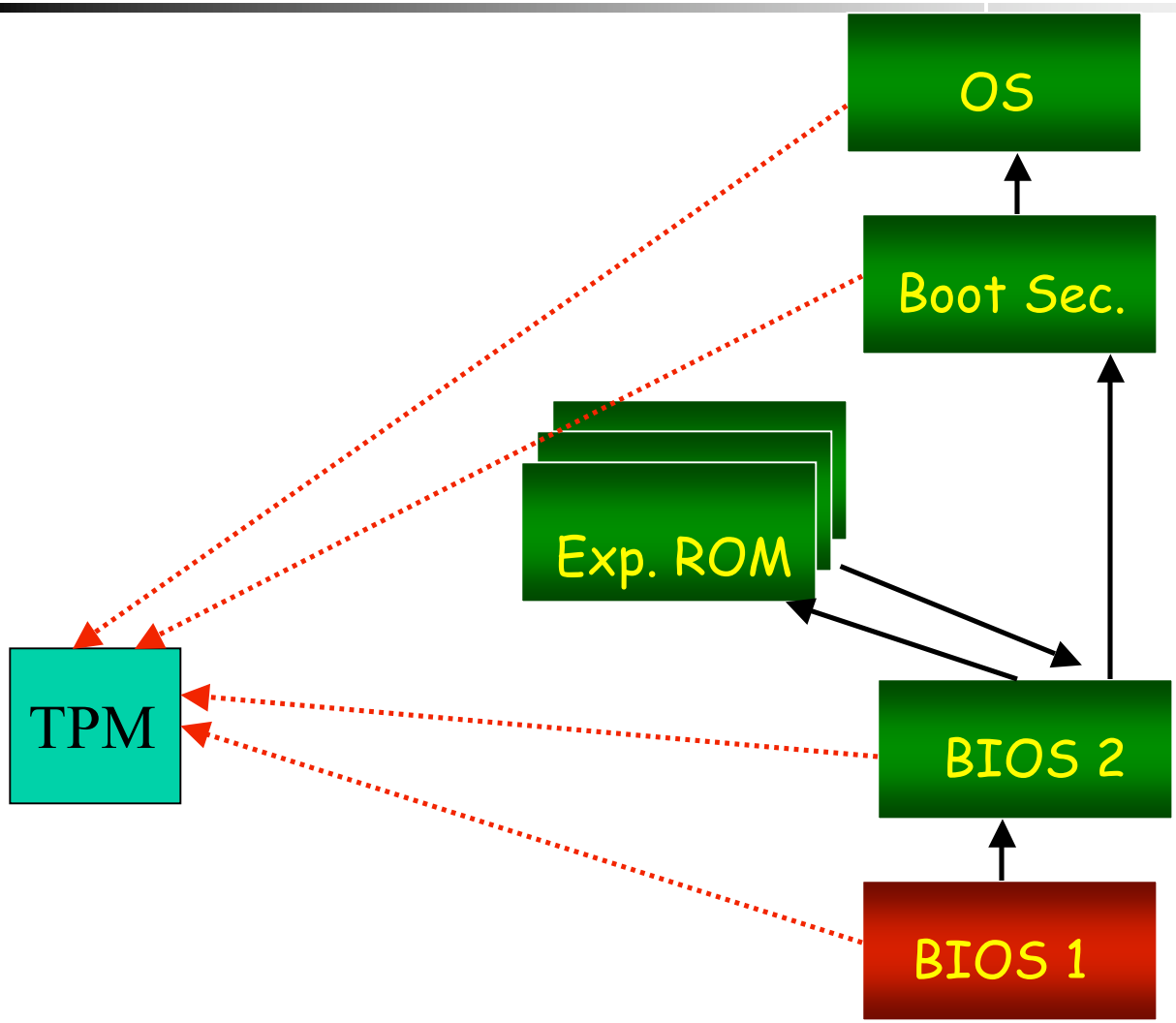
Pre-boot methods

- Authenticated boot
- Secure boot
- Trusted boot

Authenticated boot vs. Secure boot

- Several similarities and differences
- Both ONLY ensure a secure initial state, i.e. at t_0.
- TCG only provides authenticated boot
- Both assume that measured software is *trustworthy*.

Authenticated boot



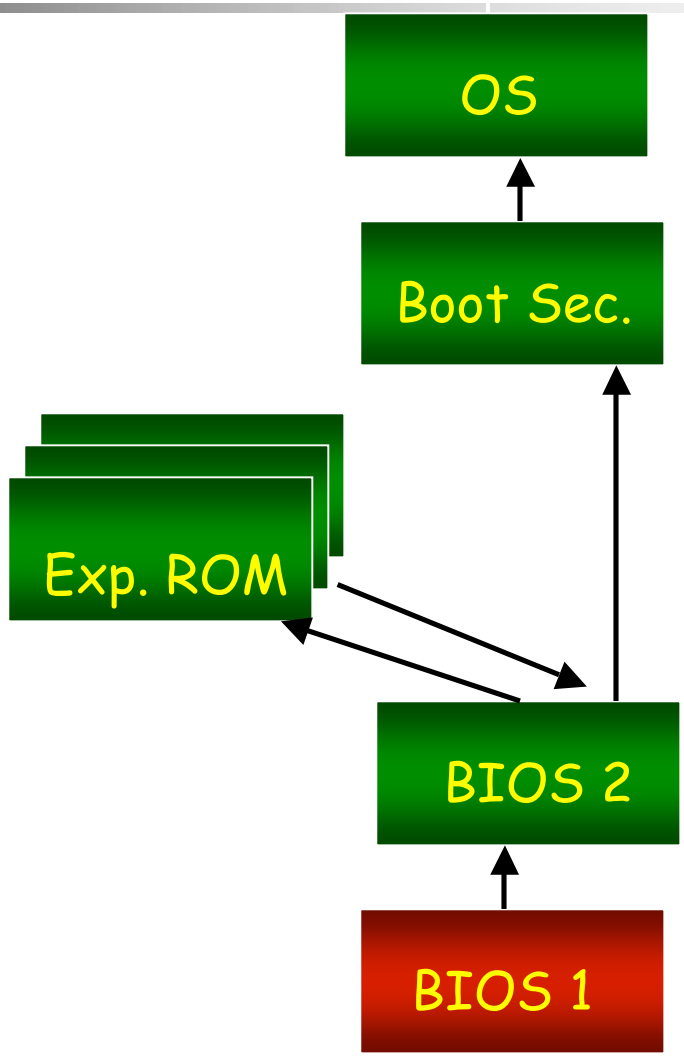
Authenticated boot

- Passive method
- Integrity measures are stored securely
  - Uses a *write once* register (PCR) in the TPM
- Provides proof to a third party of the configuration initialization, t_0, via attestation.
- Why can't the system determine its configuration is verified?
  - Lack of a trusted path to the user from the TPM
  - Proof by contradiction

Secure boot

- Active, i.e. can prevent malice from executing.
- Proof to the system is existential
  - *I've started therefore I'm in the correct configuration*
- Unable to prove configuration to a third party

Secure boot



Authenticated boot++

- The biggest limitation of authenticated boot is that it provides absolutely NO VALUE to the user, i.e. the user has no proof their system is in a known configuration.
- With the addition of a trusted path from the TPM to the user, the TPM can prove to the user it is in a known configuration.

Authenticated boot++

- The user boots a "clean" system and stores a secret into the TPM and locks it based on the system's PCR value.
- The secret is now only available when the PCR indicates a clean system.
- The trusted path allows the TPM to deliver the secret to the user without modification.

What do we need?

- Trusted boot
  - Authenticated + Secure boot
- Why?
  - There are times when proving your configuration to a third party is helpful. (NOTE: There are abuses of courese)
  - You don’t want malice to execute if you can help it… no matter how good you think your protection is

Post boot methods

- IBM's extension of TCG into run-time
- Virtualization
- LaGrande (Intel) / Secure Extension Mode (AMD)
- Active Management Technology (Intel)

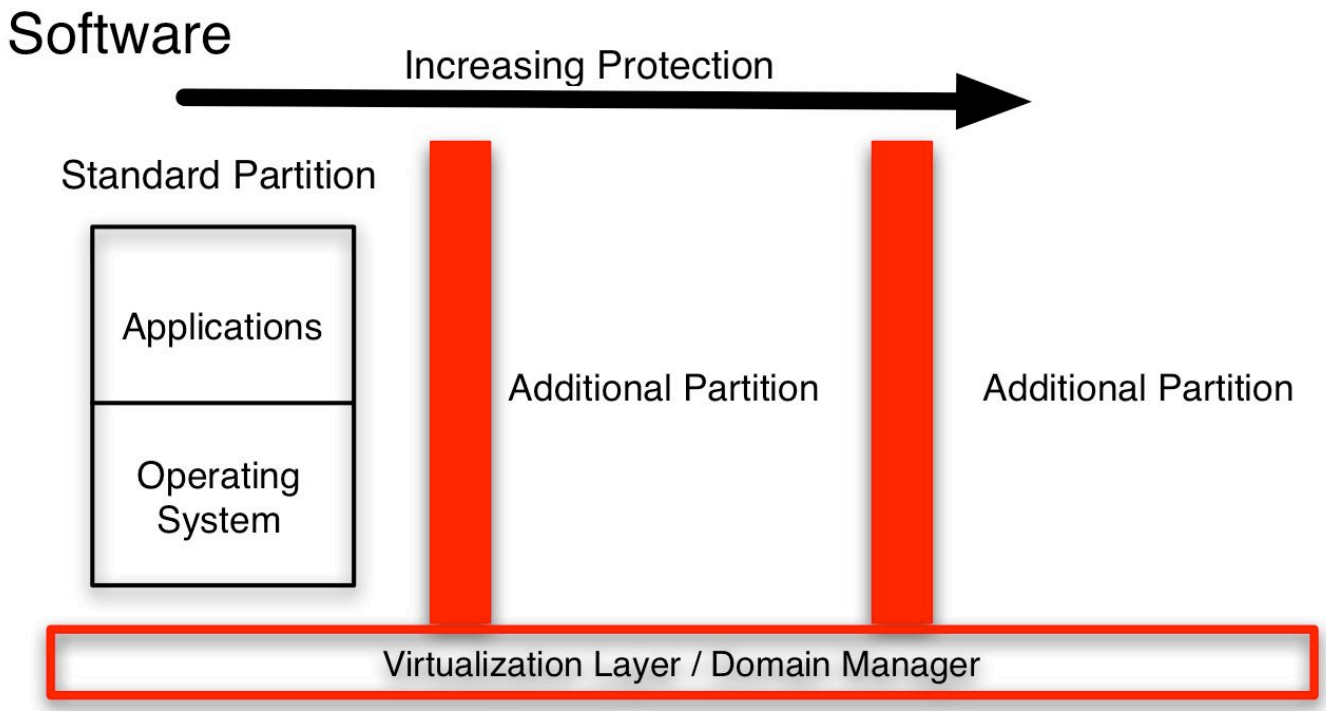
Extending the TCG

- *Design and Implementation of a TCG-based Integrity Measurement Architecture*. Sailer, Zhang, Jaeger, van Doorn. USENIX Security 2004
- Essentially everything loaded/executed is measured along with a list of objects measured. The list is maintained in kernel data. The measured value in a PCR.
- Only works if ALL software is trustworthy as buffer overflows to code within an already loaded image will not be detected.

Virtualization

- Both Intel and AMD are proposing virtualization modifications to their processor line. In addition to virtualizing the instruction set, they are adding essentially a "ring -1".
- A domain manager such as Xen runs in "ring -1" while OS's continue to work (or not ;-)) as they do now. The protection is such that the OS can't write to the domain manager, but the domain manager can read/write to the OS.

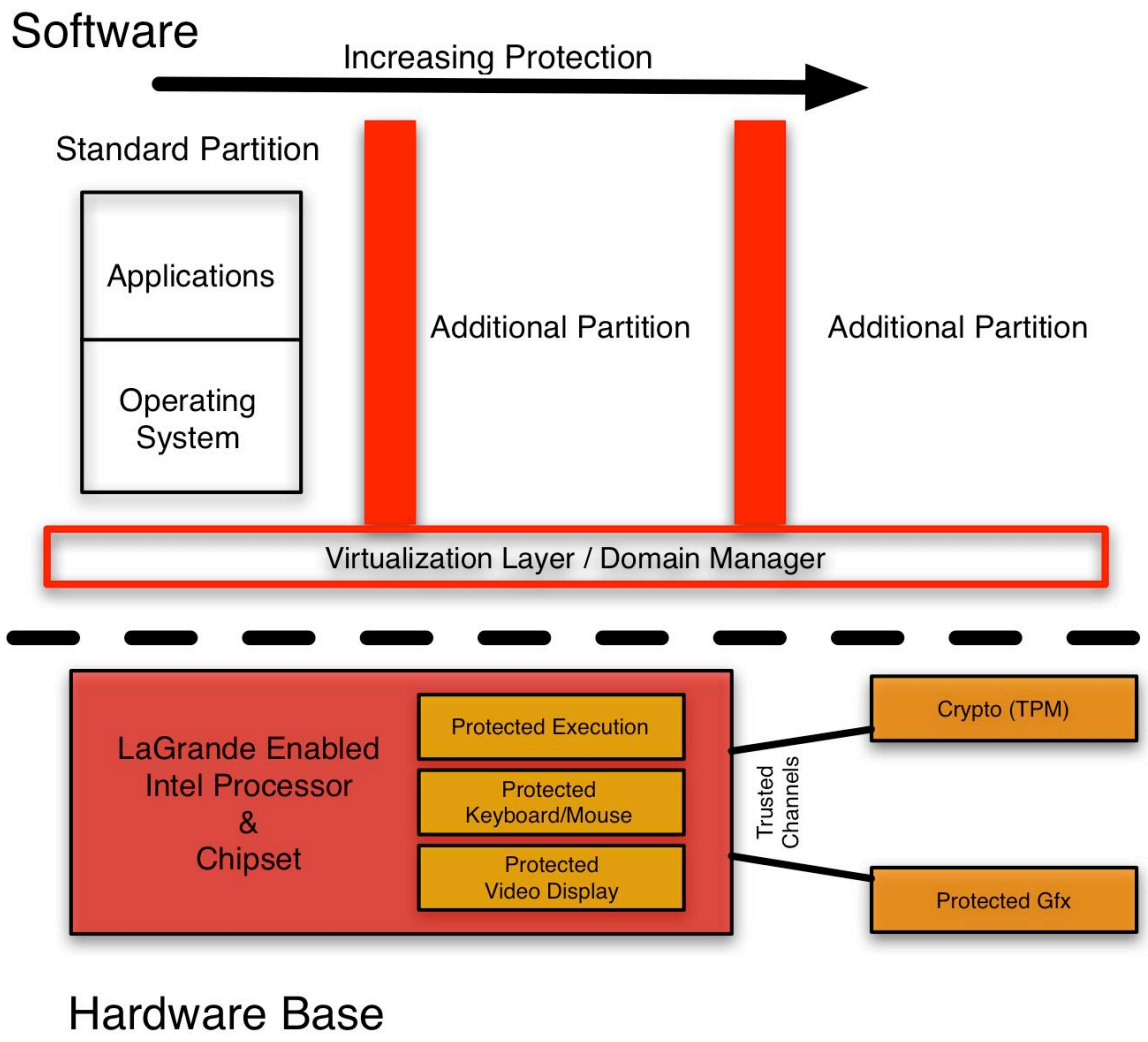
Virtualization notion



LaGrande

- Processor and IO chipset modifications to increase security
  - Trusted IO paths for video and keyboard
  - Protected execution
  - Additional memory protection
- Presumably available in ‘06.

LaGrande with VT



AMT

- New initiative just announced by Intel with few technical details available.
- The basic idea is to use an independent and isolated processor to manage and monitor the host.
  - "*Copilot- A Coprocessor based Kernel Integrity Monitor*", Petroni, Fraser, Molina, and Arbaugh. USENIX Security 2004.
  - "Using Independent Auditors as Intrustion Detection Systems", Molina, and Arbaugh. ICICS 2002.
  - "Active Systems Management: The Evolution of Firewalls", Arbaugh. IWISA 2002.

Example

- (GOOD) Electronic voting
  - Attestation combined with trusted boot is exactly what you want with each voting machine attesting to a judge.
  - Post boot methods are likely too costly and potentially overkill.
- (BAD?) This can also enable DRM with additional HW.

Example

- (Good) Peer to Peer content and software
  - Can be used to id and prevent those providing tainted content
- (Bad) DRM

More Examples

- Can be used to lock files
  - Good: Protect your keys
  - Bad: Lock files to applications to limit competition
- Can provide strong authentication of platform
  - Good: Parental controls
  - Bad: Loss of anonymity (note: 1.2 of the TCG allows for anonymous identities)

False claim(1)

- Delete files on your computer
  - This is in the software and can be done now! Vendors don’t need trusted computing.

False claim (2)

- Reduces the usefulness of GNU software
  - Claim is that software that requires an endorsement key such as software certified to an EAL level will not run after being modified unless the software is recertified and issued a new key.
  - This is true. But, this is a function of the evaluation process.
  - The software will still run on TCG and non-TCG platforms. You can issue your own key.
  - It is just that no one will recognize your machine as running an approved EAL(99) platform.

False claim(3)

- The TCG alone provides protection against viruses.

False claim (4)

- Trusted computing will make you go bald!

Analysis and Predictions

- Improvements in trusted computing will come from virtualization.
- LaGrande will likely not survive.
  - Market does not understand the need for trusted paths
- This stuff will be hacked
  - Look at the Xbox. Hacking hardware requires a different skill set. Granted some of the tools are more expensive.

Conclusions

- All technology is essentially dual use. It can be used for good or evil.
- Laws and policies attempt to limit the evil uses, but the evil uses can not be completely eliminated.
- You have to decide for yourself does the good outweigh the bad.