IBM Research

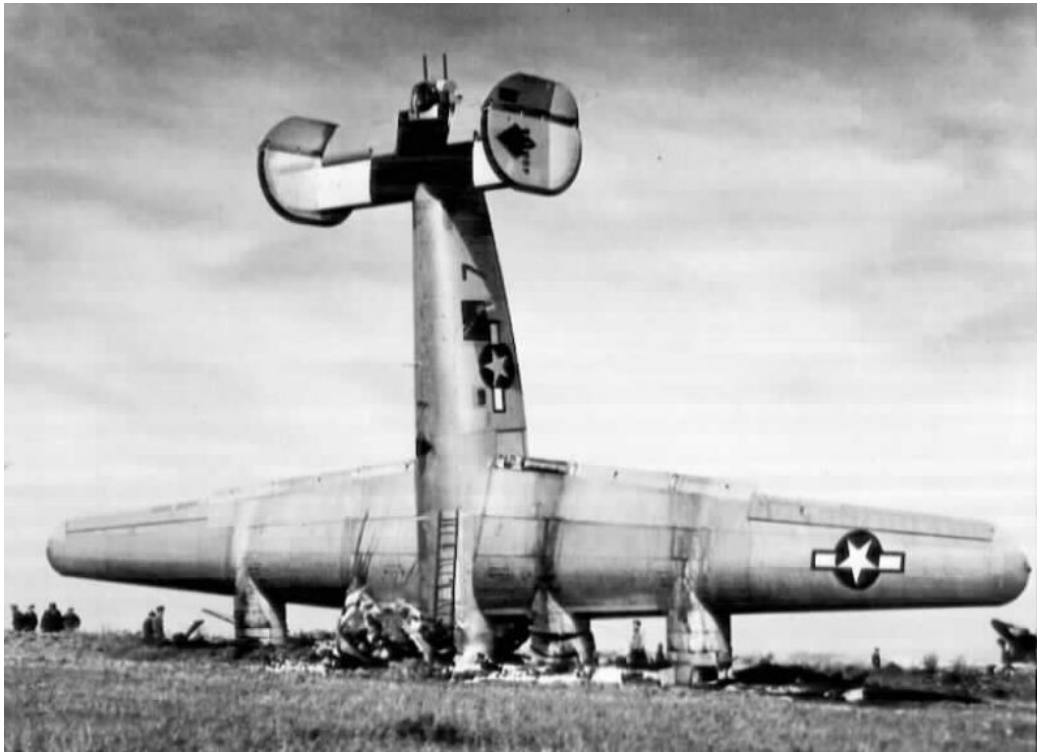
Security Research: Hardware Foundations

David Safford
safford@us.ibm.com

Outline

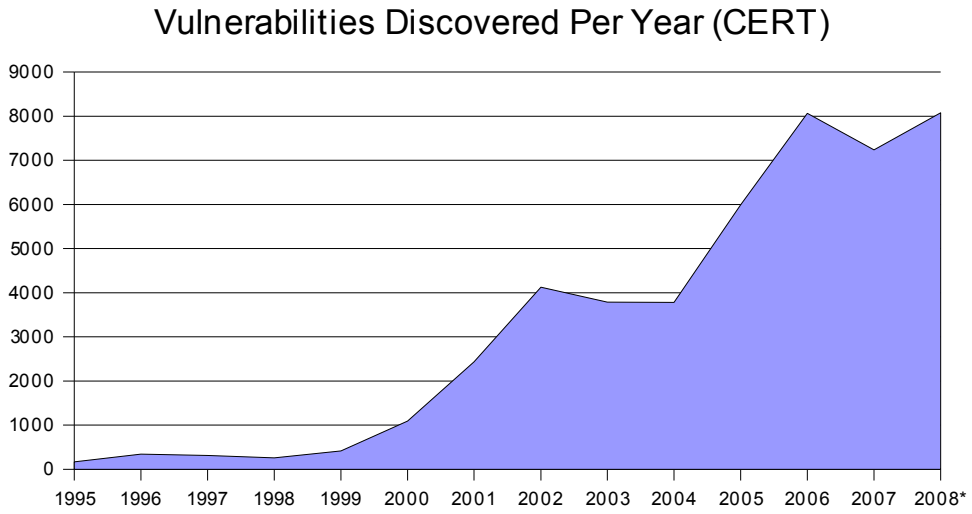
- Software security impossible
- Hardware Root of Trust to
  - Detect compromise
  - Authenticate without passwords
- Hardware Challenges
  - Badly Designed Hardware (SMM)
  - Buggy Hardware (Errata)
  - Malleable Hardware (microcode patches)
  - Malicious Hardware (underhanded/State sponsored)

Introduction: State of Computer Security



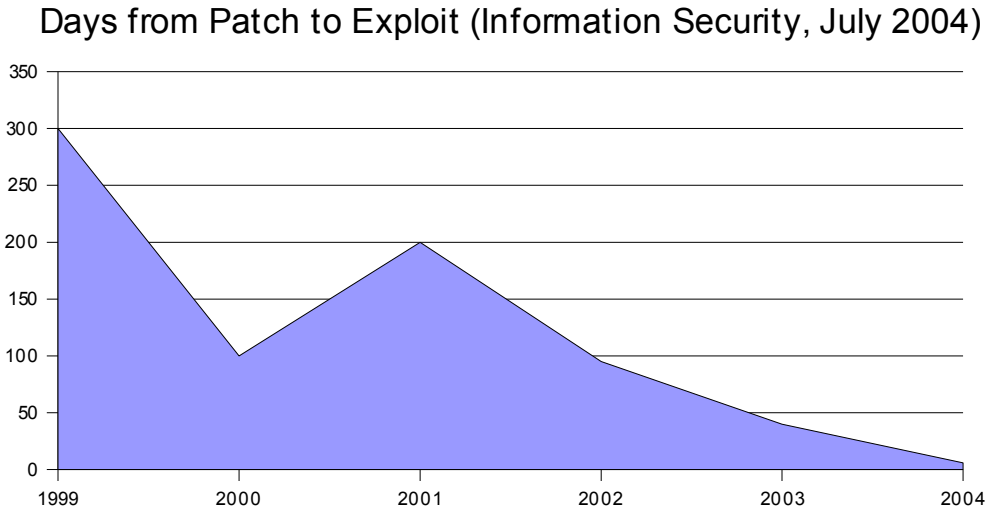
“The sky isn't falling ... it fell a few years ago.”
Roger Grimes, Infoworld Security Advisor, 2006

1. We've Lost the Software Vulnerability War



More and More Vulnerabilities
(roughly 20 per day)

Less and Less Time to Patch
(zero day exploits)



Secure Software is HARD

- So far, every software system has failed
  - Apollo Command Module Computer (16K words) failed on every flight
- Studies shows at least 1 bug per K lines of code (LOC)
  - IBM internal study, 2000
  - Information Week Jan 21 2002, p23
  - Reasoning, Inc 2003
  - coverity.com 2008
- Linux and WinXP with Office each have > 200MLOC
  - 400K bugs would take 80 years @ 5000/year to fix
  - But we are writing roughly 50K new ones per year!
- Can model this as an infinite supply of security bugs.
  - Must design our systems to confine compromise

The Ease of Application Hacking

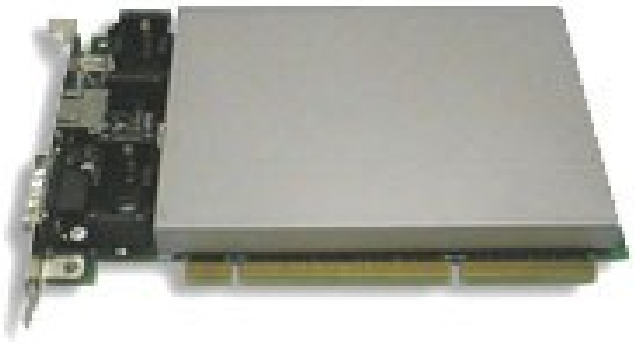
- Attacking Servers:
  - 97% web sites vulnerable to SQL injection or XSS.
    IBM ISS
- Attacking Clients:
  - Chinese Hacking
    - Spear phishing with Word and PDF exploits
    - 1,295 (known) PC's in 103 Countries
    - High value targets
    - Remarkably simple, effective attacks

The Failure of Secrecy

- “Three may keep a secret, if two of them are dead.”
  Benjamin Franklin, 1735
- Benjamin was a hopeless optimist.
  - Individuals seem delighted to give away their secrets.
  - Phishing/pharming
  - Gartner: $3.2B losses, 3.6M victims of phishing in 2007
- “One may keep a secret, if he doesn't know what it is.”
  Dave Safford, 2004
  TPM

Hardware

IBM PCI-X Cryptographic Coprocessor (PCIXCC)



- Announced in September, 2003
- Greatly improved performance
- PCI-X and network interface
- Same physical / logical security feature set as 4758
- Received FIPS 140-2 Level 4 validation
- Support for IBM zSeries (mainframes) today

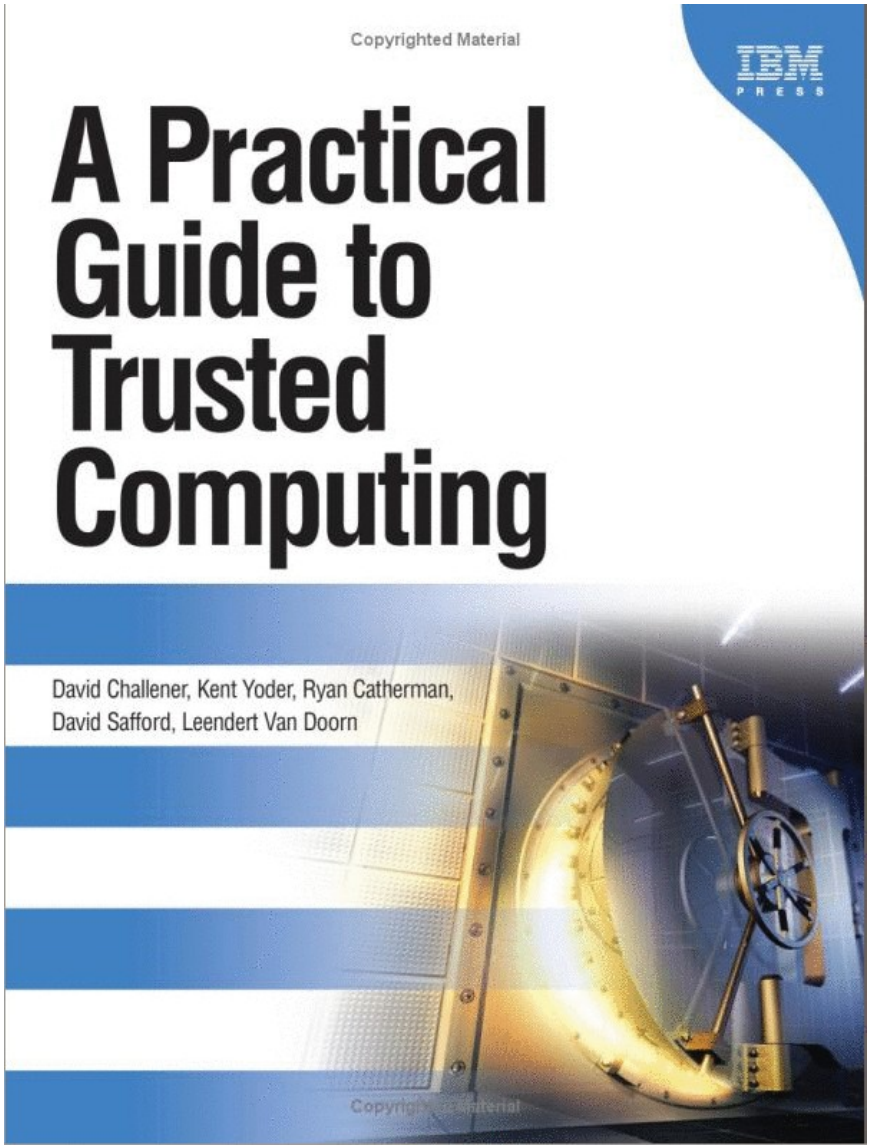
Trusted Platform Module (TPM)

- RSA crypto
  - key generation, signature, encrypt, decrypt
- Secure storage
  - private keys
  - master keys (eg loopback)
- Integrity measurement
  - Platform Configuration Registers (PCR)
  - compromise detection
  - Tie key use to uncompromised environment
- Attestation
  - host based integrity/membership reporting
  - (RSA 2004 Demo)

- IDC: “by 2010, all pc's will come with a TPM”
- http://trustedcomputinggroup.org

A Blatant Plug

- Programming
  - BIOS
  - Device Driver
  - TPM
  - TSS
- Applications
  - Trusted Boot
  - Key Management
  - Authentication
  - Attestation



TPM as a Root of Trust

- Static Root of Trust (SRTM)
  - Immutable BIOS measures mutable BIOS
  - Each step thereafter measures the next stage
- Dynamic Root of Trust (DRTM)
  - Atomic measure/load/execute bootstrap
  - Not dependent on BIOS
  - But: Rutkowska, “Attacking Intel's Trusted Execution Technology” Blackhat 2009 (See later slide)

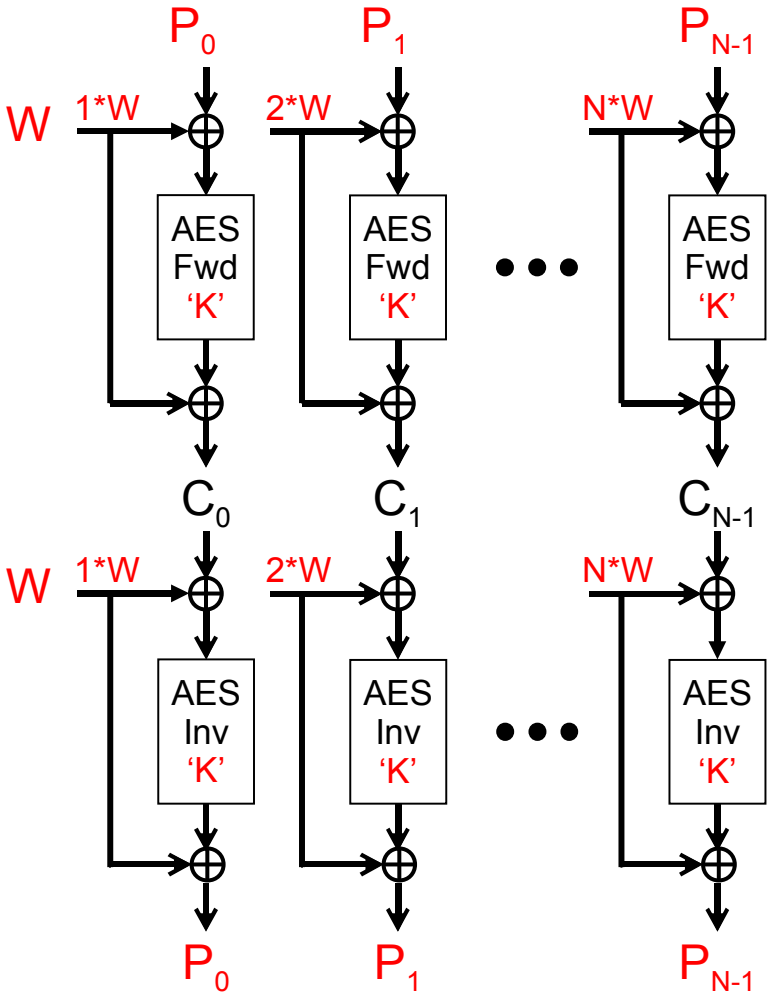
Integrity Measurement Architecture (IMA)

- Trusted Computing Group Trust Architecture
  - Chain of trust – measure files before accessed/executed
  - Store measurements in kernel list
  - Extend measurements into TPM/vTPM PCR
  - Attest all measurements to third party, signed by TPM/vTPM
  - Malware cannot take measurements back from TPM/vTPM
- IMA is linux kernel module which implements this model
  - Policy based for which files to measure
  - High performance with measurement caching
  - In Linus' git tree for 2.6.30

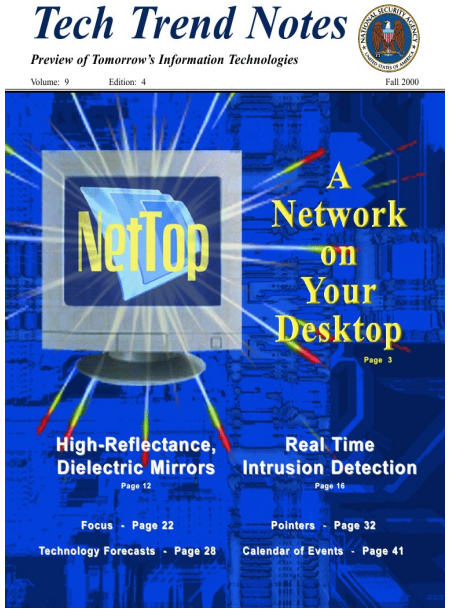
Secure Hardware

Integrity Aware Parallelizable Mode (IAPM)

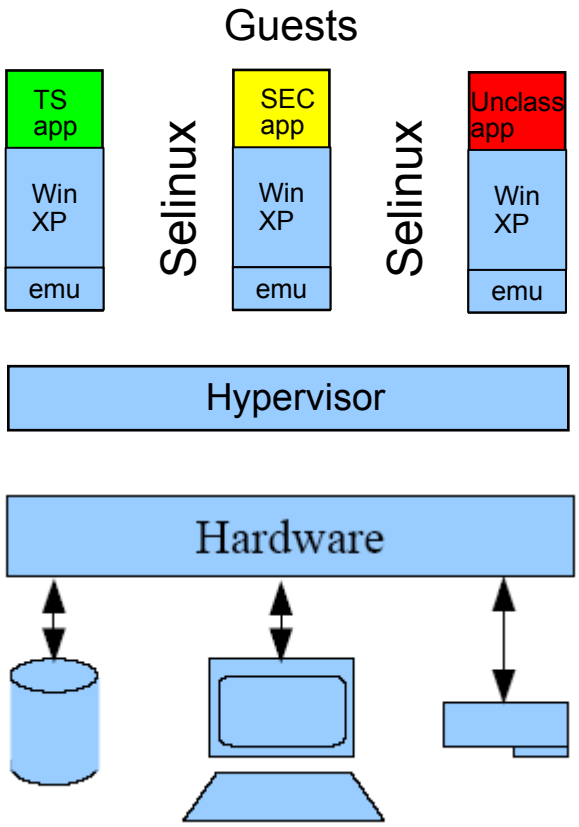
- Originally developed for network communications
  - With “almost free” integrity
- Use “whitening” with pairwise independence
  - Builds “location sensitivity” into ciphertext
- Processed in parallel and/or pipelined engines
  - Both encryption & decryption
- Submitted to NIST for evaluation as a block cipher mode



NetTop/HAP 1 Architecture: Client Consolidation

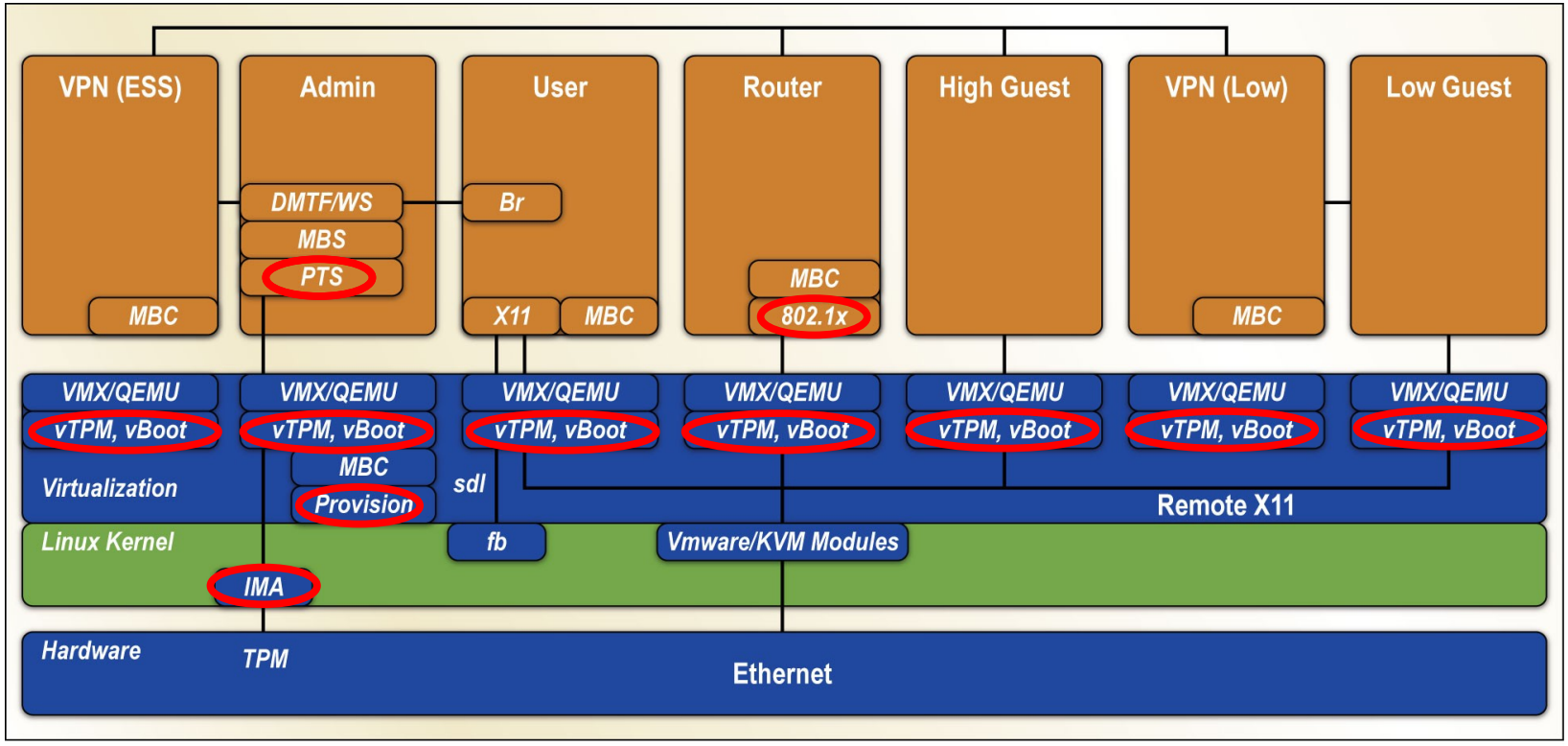


NSA 2000



VMWare Workstation
RHEL 4

Adding TPM based Attestation to HAP



Key Research Components: PTS, IMA, vTPM, vBoot, Provision, 802.1x-PTS, Vmware/KVM configuration

Attestation 802.1x-TNC-PTS

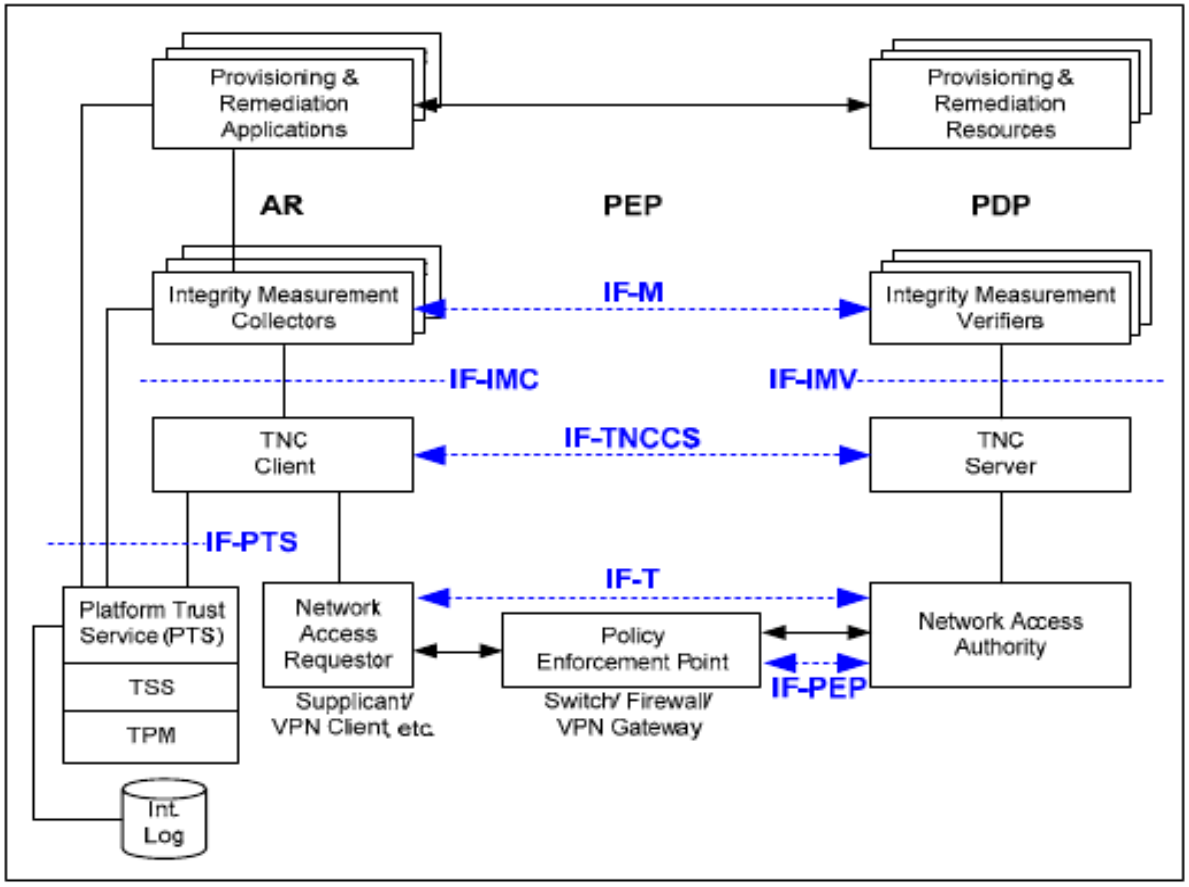


Figure 5: The TNC Architecture with the Trusted Platform Module (TPM)

Hardware Challenges

The modern threat

"Nation states, however, have the technical and operational capabilities to orchestrate the full range of adversarial cyber operations through a combination of such means as recruiting insiders, setting up front companies, establishing signals collections systems, implanting damaging hardware or software in communications networks and subverting telecommunications, cryptographic defenses and supply chains."

National Science and technology Council, "Federal Plan for Cyber Security and Information Assurance Research and Development", April 2006.

How do you know your hardware doesn't have a back door?

How “Hard” is Hardware?

- Firmware
- microcode/patches
- FPGA
- BIOS
- SMI/SMM
- All of these can be attacked

How many gates in an undetectable CPU backdoor?

- Underhanded Hardware competition
  http://isis.poly.edu/csaw/embedded

How many gates in an undetectable CPU backdoor?

- Underhanded Hardware competition
  http://isis.poly.edu/csaw/embedded

- 1341 (mainly for cryptographic triggering)
  Samuel King, Designing and Implementing Malicious Hardware, leet08

How many gates in an undetectable CPU backdoor?

- Underhanded Hardware competition
  http://isis.poly.edu/csaw/embedded

- 1341 (mainly for cryptographic triggering)
  Samuel King, Designing and Implementing Malicious Hardware, leet08

- 0 (just exploit design errors)
  Loic DuFlot, Using CPU System Management Mode to Circumvent Operating System Security Functions, Cansecwest 2009

How many gates in an undetectable CPU backdoor?

- Underhanded Hardware competition
  http://isis.poly.edu/csaw/embedded

- 1341 (mainly for cryptographic triggering)
  Samuel King, Designing and Implementing Malicious Hardware, leet08

- 0 (just exploit design errors - SMM)
  Loic DuFlot, Using CPU System Management Mode to Circumvent Operating System Security Functions, Cansecwest 2009

- 0 (just use the existing errata)
  Kris Kaspersky, Remote Code Execution through Intel CPU Bugs, HITBSecConf2008

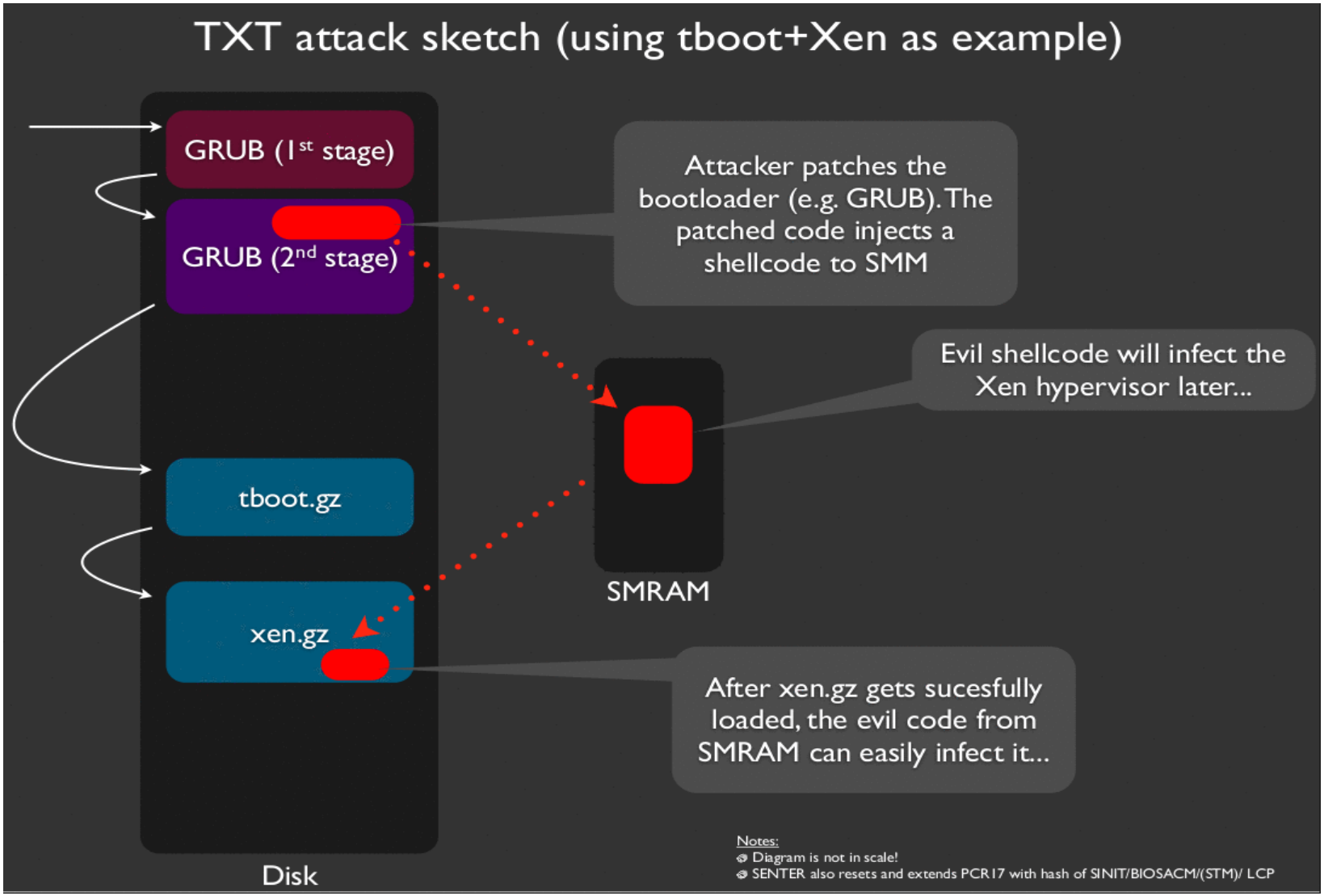
How many gates in an undetectable CPU backdoor?

- Underhanded Hardware competition
  http://isis.poly.edu/csaw/embedded
- 1341 (mainly for cryptographic triggering)
  Samuel King, Designing and Implementing Malicious Hardware, leet08
- 0 (just exploit design errors)
  Loic DuFlot, Using CPU System Management Mode to Circumvent Operating System Security Functions, Cansecwest 2009
- 0 (just use the existing errata)
  Kris Kaspersky, Remote Code Execution through Intel CPU Bugs, HITBSecConf2008
- 0 (just steal Intel's microcode patch signing key)

How many gates in an undetectable CPU backdoor?

- Underhanded Hardware competition
  http://isis.poly.edu/csaw/embedded
- 1341 (mainly for cryptographic triggering)
  Samuel King, Designing and Implementing Malicious Hardware, leet08
- 0 (just exploit design errors)
  Loic DuFlot, Using CPU System Management Mode to Circumvent Operating System Security Functions, Cansecwest 2009
- 0 (just use the existing errata)
  Kris Kaspersky, Remote Code Execution through Intel CPU Bugs, HITBSecConf2008
- 0 (just steal Intel's microcode patch signing key)
- 0 (force the microcode signature verification – who's going to check?)

SMM Attack on DRTM (Rutowska, Blackhat 2009)



Summary

Summary

- Software security impossible
- Hardware Root of Trust to
  - Detect compromise
  - Authenticate without passwords
- Hardware Challenges
  - Badly Designed Hardware (SMM)
  - Buggy Hardware (Errata)
  - Malleable Hardware (microcode patches)
  - Malicious Hardware (underhanded/State sponsored)