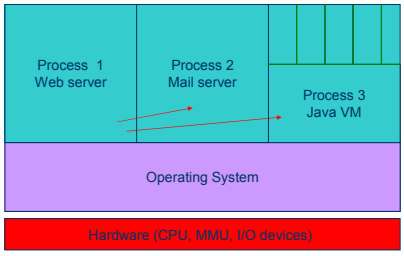
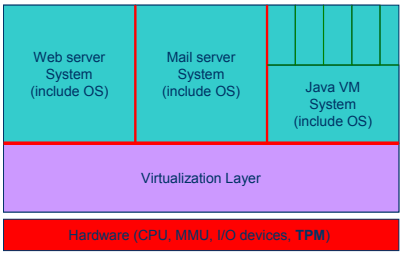
Trustworthy Computing

Trent Jaeger
February 18, 2004

Systems View -- Current



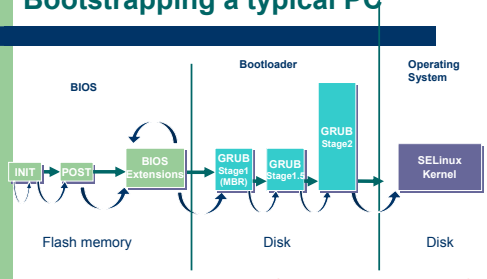
Systems View -- Target



TC Advantages

- Authentication: Application → Root of trust
- Access Control: Process separation → System separation
- Patches/Attestation: Ad hoc → Identify high integrity apps
- Hardening: Ad hoc → Identify hardened configs
- Audit: Integrate in OS → See in VMM (e.g., ReVirt)
- Intrusion Detection: Open to compromise → Protected

Bootstrapping a typical PC



What can go wrong before the kernel runs?

Boot Guarantees

- Secure Boot
  - Ensure only a secure system is booted
  - Operating system that is bootstrapped is based on a untampered foundation (*integrity guarantee*)
  - Initially not a problem, but nowadays field upgradable FLASH memory is used
  - Arbaugh et al. [1996] state that the integrity of a layer can only be guaranteed if-and-only-if:
    - Base layer is immutable
    - The integrity of the base layer is verified
    - Transition to higher layer only occurs after valid verification
- Key points
  - Computer is stopped if secure boot guarantee is violated
  - Not provable to remote systems

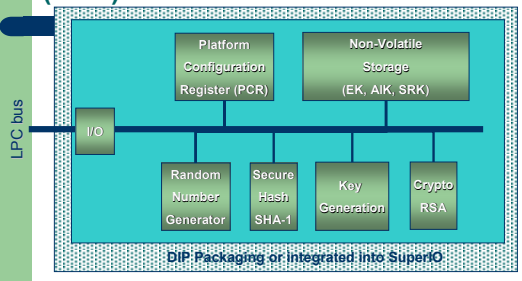
Boot Guarantees (con't)

- Trusted (Authenticated) Boot
  - Measure system during boot for remote verification
  - Operating system is booted based on a measured system (*integrity verifiable*)
  - Enable verification of boot:
    - Base layer is immutable
    - The integrity of the base layer is measured
    - Transition to higher layer only occurs after valid measurement
  - Remote party can verify measurements to determine integrity
- Key points
  - Computer is *not* stopped if secure boot guarantee is violated
  - Provable to remote systems
  - Requires root of trust

Trusted Computing Group

- TCG (formerly known as TCPA) goal is to add secure platform primitives to each client (now the focus is also on servers, cell phones, PDAs, etc.)
- Industry consortium by IBM, Intel, HP, Microsoft, …
- These secure platform primitives include:
  - Platform integrity measurements
  - Measurement attestation
  - Protected storage
- These can be used to provide trusted boot (as opposed to secure boot)
- TCG is considered very controversial, but lets defer that discussion until we understand what it is …

TCG Trusted Platform Module (TPM)



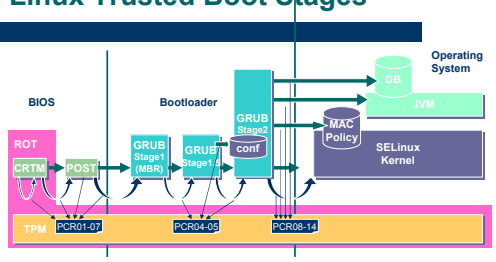
Basic TPM Functions

- Integrity measurements
  - Enables measurement of the firmware, bootstrap loaders, operating system
  - Chains measurements to protect their integrity
- Remote attestation
  - Constructs statements for remote verification of these integrity measurements
- Protected storage
  - Provide "secure" data storage (think smartcard)

Platform Integrity Measurements

- The TPM contains a set of program configuration registers (PCRs) which record integrity measurements
- Operations on PCRs:
  - TPM_Extend(N, S): $PCR_N = SHA1(PCR_N \mid S)$
  - TPM_Read(N): Return contents of PCR_N
  - (only enabled when TPM ownership is established)
- Core Root of Trust Measurement is immutable
- Root of trust measurement is bootstrapped from that
- PCRs cannot be counterfeited, but can be invalidated

Linux Trusted Boot Stages



Platform Attestation

- TPM contains the ability to attest the contents of a PCR
- Each TPM has a unique public endorsement key (EK) which is under control of the owner (enable/disable)
- EK enables machine authentication, attestation = authentication + integrity
- Multiple attestation identity keys (AIK) generated by the TPM, AIK may not be tied to an endorsement key
- TPM_Quote operation is used to sign a $PCR_{N..M}$ value under a specified AIK_i

Protected Storage

- TPM holds a storage root key (SRK) which is kept within TPM
- The SRK is used to wrap keys which are kept outside the TPM and are loaded on demand for crypto or attestation
- Sealed storage, use certain PCR value to unlock protected storage

Problems with Integrity Measurements

- What is the meaning of these aggregate PCR values?
- How do you handle all the different firmware versions, patches, kernel builds? What does a PCR mean in this context?
- The TPM_Extend operation assumes a linear ordered execution sequence (true for bootstrap), but how does that work for the OS where the order in which program are started is non-deterministic?
- This makes PCRs a good mechanism for the owner to verify the integrity of his system (has the bootstrap loader been modified?)
- In its current form PCRs are less suitable for attestation of complex execution patterns

NGSCB Applications

- Corporate document prepared by a trustworthy program is accessible to game or virus
- User's home finance transactions are vulnerable to a Trojan horse
- Authenticated transactions may be from a person running a trusted program or a subverted program.

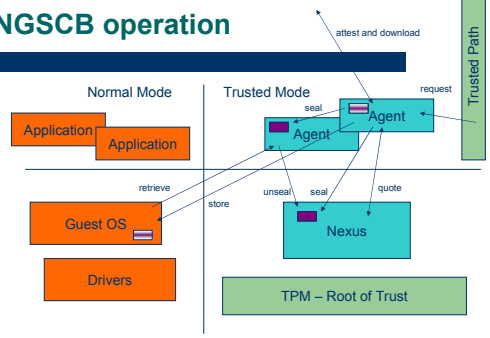
NGSCB Digital Rights Management

- In order for a user to download a media file, the media provider wants to verify
  - that the environment running such programs is trusted not to subvert the program
  - that the media player is trusted by the provider not to leak the media
  - that there is a means to prevent leakage of the media when stored

NGSCB – Key mechanisms

- Sealed storage – built on protected storage
  - Seal(codeID, data)
    - Creates {sealed data, codeID, sealerID}
  - Seal(otherCodeID, data) – discretionary mechanism
  - Unseal(sealed data) → data, sealerID (if authorized)
- Attestation – built on platform attestation
  - Quote(string) → {string, codeID} signed by TPM
  - If string is a certificate, then codeID is associated with a private key
  - A chain of attestations can attest an entire software stack
- Partitioning – based on special processor hardware (ring -1)
- Trusted path – based on special hardware
- DMA control – based on special hardware

NGSCB operation



NGSCB Issues

- Upgrades – reseal secrets for new codeID
- Generic code identity – Interpreter running script → composite codeID
- Backup – delegate to OS
- Privacy – hard to misuse data
- Privacy – easy to learn everything about the platform → third-party identity service providers
- Known plaintext – randomize sealed values

TCG Controversy

- TCG is considered very controversial because it potentially allows content providers to control clients (DRM enforcement)
- This takes away the freedom of the user to use the system as it sees fit (it can be used to lock-out GPL software)
  - Limit GPL by requiring specific customization
  - Problem if limited number of trusted roots of integrity are permitted
- A privacy concern is that TCG can be used to track the user
  - Anonymous user identity certs from Privacy CA
- Are these concerns valid?

TCG Misconceptions

- The TCG designers have been very aware of the concerns and the TPM focus is that the owner of the machine is in control (this could be an individual or enterprise). The service or content provide does not control the TPM
  - Although "extend" is always available
- TPM does not lock-out software, it merely measures it (if enabled)
- It does allow a service/content provider to not service the machine if the attestation statement does not meet its requirements.
- Is this very different from current mechanism where each browser sends browser name, OS, version to the web server ?

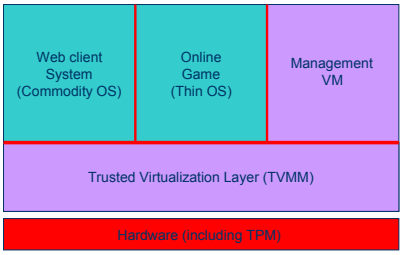
Improving the TCPA (TCG)

- Preserve Fair Use Rights
  - TCG-based implementations should support user copying for personal use
  - Permit users to define their own trusted root for which delegation of sealed storage is possible
- Control of root certificates
  - Need for fair use and to facilitate competition
- Completely disable it
- Pseudo-identities
  - Generate new identities → several open research questions

Some Personal Observations

- TCG 1.2 is the basis for Microsoft NGSCB, but TCG != NGSCB
- As a secure OS builder I like to have secure boot in addition to trusted boot. I want to stop when the bootstrap is compromised because continuing opens up spoofing attacks.
- The value proposition for TCG is not easy

Terra Architecture



Virtual Machine Architecture

- Compatibility
  - Run unmodified OSs
- Isolation
  - Individual VMs in own protection domain
- Extensibility
  - Of original hardware
- Efficiency
  - Virtualizable hardware
  - Optimized VMMs

Terra Architecture Innovations

- Open/Closed box VMs
  - Open: general purpose system
  - Closed: specialized, proprietary system
- Management VMs
  - Resource and access control manager, including VMs
- Security Goals
  - Root secure: closed-box VM integrity and secrecy
  - Attestation: Remote authentication of what's on the closed box
  - Trusted Path: TVMM provides a trusted path between user and a VM

Attestation

- Chain from TPM to application VM that identifies all components
  - Attestable parts: all persistent state of VM
  - Component's public key and application data
- Two chains of trust
  - TPM → application VM
  - CA → application image
- Granularity of measurement is VM

Security Arguments

- Management VM
  - Limited interaction among VMs can be controlled in centralized location
  - Limited to VM-level resources
- Assurance
  - TVMM is small
  - Closed VMs can be small
- Attestation
  - Is a current measurement only
  - What static guarantees can be assumed?

Security Implementations

- Storage
  - Encrypted, integrity checked (see sealed storage)
  - Attested or not
    - Primary identity: VM
    - Secondary identity: firmware and other immutable state
- Attestation
  - Divides entities into blocks – verify lazily (optimistic)
  - VM descriptor is the hash of all hashes
  - 4GB entity of 4kB blocks → 20MB of hashes

Terra Interfaces

- Attestation
  - Cert ← endorse(cert-req) – cert generation
  - Hash ← get-id() – hash of calling VM
  - Attestation = (cert, hash) signed
- Management
  - Dev-id ← create-device(type, params)
  - Connect(dev1, dev2)
  - Disconnect(dev1, dev2)
  - Vm-id ← create-vm(config)
  - Attach(vm1, dev1)
  - Detach(vm1, dev1)

Example – Trusted Quake

- TVMM → VMWare (experimental)
  - Attestation – virtual serial device in TVMM
  - No TCPA
- Secure Storage
  - Interpose read/write at TVMM – dynamic preload lib
  - Ahead-of-time attestation of entire VM files
  - Optimistic attestation as blocks are read (alignment)
- Quake
  - Prevent cheating by altered client, server, or data files
- Trusted Quake
  - Closed-box VM – limits programs to trusted ones (e.g., no shell)
  - User-space IPSec implementation provides attestation/key exchange
  - Data is protected because only attested programs are run and these are trusted

Summary

- Hardware modifications to enable security are here (or are coming)
  - TCPA, DMA control, Trusted path
- Enable system measurement and verification
  - Attestation, sealed storage, system management
- Other systems
  - IBM 4758 – secure boot and trusted boot (Smith, ESORICS 2002)
  - Linux TCPA – driver and measurement infrastructure (IBM Tech Report)