KATHOLIEKE UNIVERSITEIT LEUVEN

Remote attestation on legacy operating systems with trusted platform modules

Dries Schellekens Brecht Wyseur Bart Preneel

Katholieke Universiteit Leuven
Department ESAT/SCD-COSIC

First International Workshop on Run Time Enforcement for Mobile and Distributed Systems
September 27, 2007, Dresden

Outline

1 Remote attestation
- Motivation
- Trusted computing platforms
- Legacy platforms

2 Legacy OS with TPM
- TPM time stamping
- Improved Pioneer Protocol
- Trusted bootloader

3 Conclusions

Outline

1 Remote attestation
- Motivation
- Trusted computing platforms
- Legacy platforms

2 Legacy OS with TPM
- TPM time stamping
- Improved Pioneer Protocol
- Trusted bootloader

3 Conclusions

Motivation

- Communication security
  - Transmitted data: confidentiality, integrity, freshness
  - Involved endpoints: authenticity
- Remote attestation: integrity reporting
- Tamper resistant software: self checking code

Applications

- Peer to peer networks
- Grid computing
- Multiplayer games (e.g., World of Warcraft)
- Digital rights management

Outline

1 Remote attestation
- Motivation
- Trusted computing platforms
- Legacy platforms

2 Legacy OS with TPM
- TPM time stamping
- Improved Pioneer Protocol
- Trusted bootloader

3 Conclusions

TCG overview

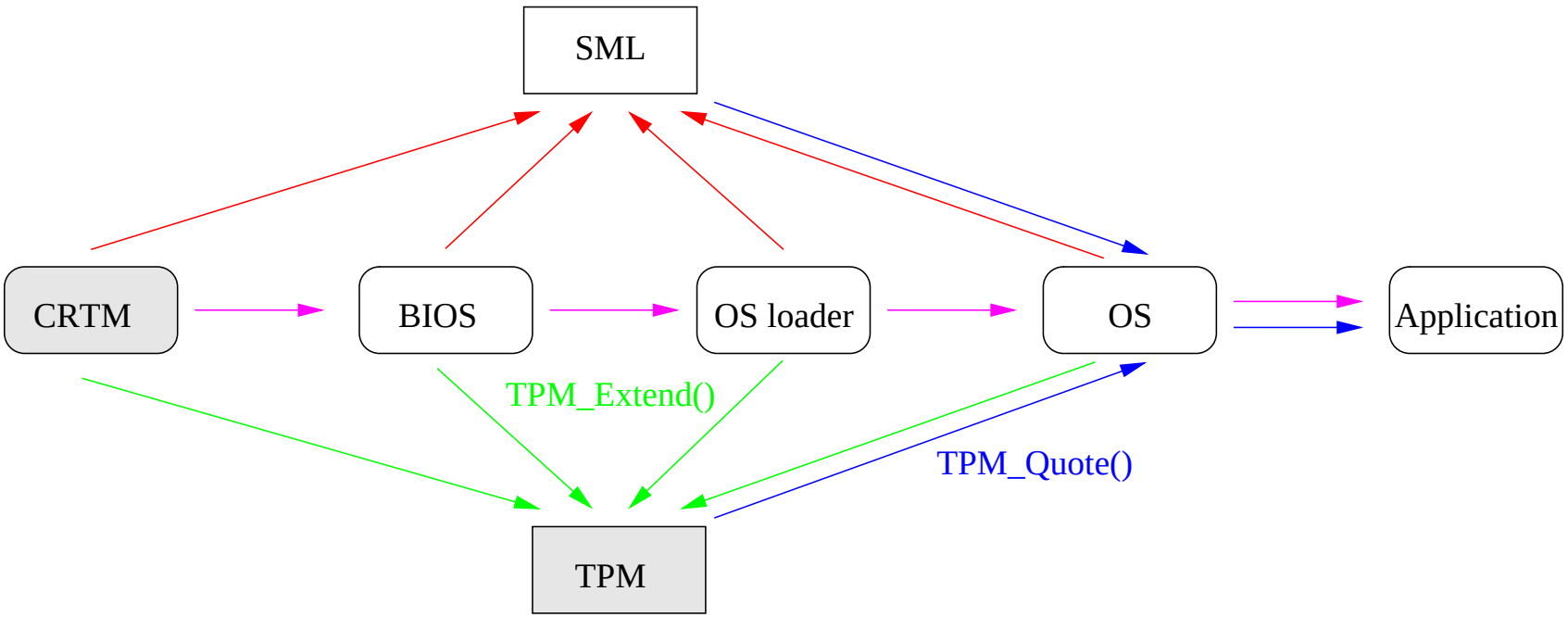
- Three core components
  1. Trusted Platform Module: "smartcard" bound to platform
  2. Core Root of Trust for Measurement: BIOS
  3. TCG Software Stack: software support

TPM features

- Cryptographic functions: RNG, SHA-1, HMAC, RSA
- Non-volatile memory: key storage
- Platform Configuration Registers (PCR)
  - Record configuration measurements (hash values)
  - `TPM_Extend()`: $PCR_{new} \leftarrow SHA\text{-}1(PCR_{old}||M)$

Integrity measurement

- Chain of trust
  1. Measure next component in boot process
  2. `TPM_Extend()` measurement to PCR
  3. Log measurement in Stored Measurement Log



Integrity reporting

- Endorsement Key (EK)
  - Unique TPM identifier
  - Certificate produced by manufacturer
- Attestation Identity Key (AIK): pseudonym for EK
  - Certified by Privacy CA
  - Direct Anonymous Attestation (TPM v1.2)
- Challenge response protocol
  1. Verifier $\rightarrow$ TPA: n
  2. Verifier $\leftarrow$ TPA: $Sign_{AIK}(\overrightarrow{PCR}, n), cert_{AIK}, SML$
- Trusted Platform Agent
  - Operating system service
  - `TPM_Quote()` on selected PCR registers
  - Collect AIK certificate and PCR history from SML

Application level attestation

- Shortcomings of TCG attestation
  - Time difference between measurement and reporting
  - Hash value of binaries
    - New version = new hash
    - Many configurations
- Hybrid attestation schemes: e.g., property based attestation

Operating system requirement

- Legacy OS: monolithic, complex, huge TCB
- Trend within TC initializes
  - Microkernel (e.g., L4) or hypervisor (e.g., Xen)
  - Virtualization for backward compatibility

Outline

1 Remote attestation
- Motivation
- Trusted computing platforms
- Legacy platforms

2 Legacy OS with TPM
- TPM time stamping
- Improved Pioneer Protocol
- Trusted bootloader

3 Conclusions

Checksum functions

Memory copy attack

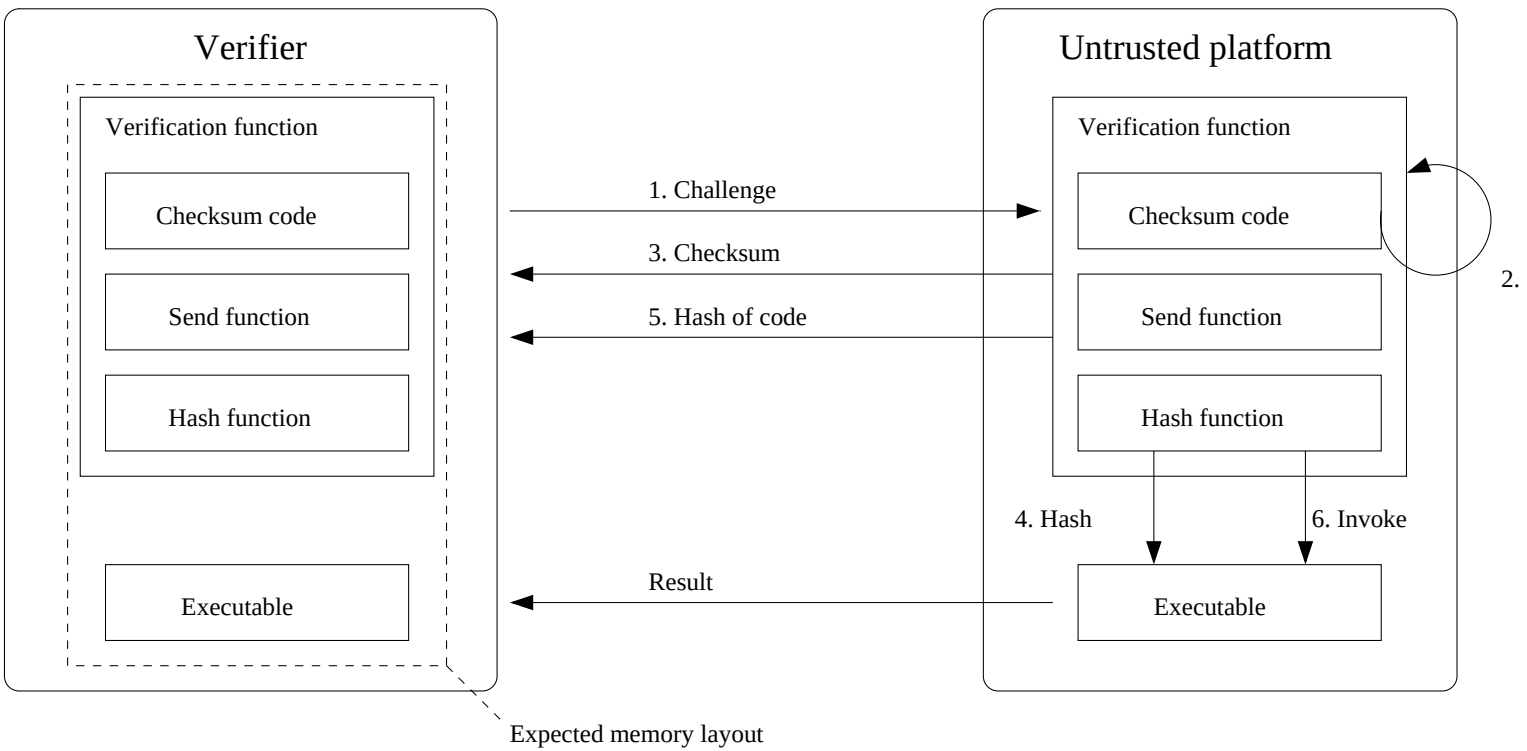
- Three memory operations
  1. Fetch: retrieve instruction from memory for execution
  2. Read: load value from memory
  3. Write: store value in memory
- Redirect fetch to tampered copy, but read from genuine copy
- Minimal overhead if hardware assisted (e.g., split TLB)

Detection of memory copy attack

- Self modifying code: overwrite code and test execution
- Execution time measurement: detect overhead of attack

Pioneer

- at t_1: verifier sends challenge n to verification agent A
- at t_2: verifier gets response $c \leftarrow cksum(n, A)$
- $t_2 - t_1 < \Delta t_{expected} = \Delta t_{cksum} + \Delta t_{network} + \delta t$



Drawbacks of Pioneer

- Fixed hardware configuration (CPU and RAM)
- Fixed verifier address to avoid proxy attack
- Indeterministic network latency ($\Delta t_{network}$)

Requirements for checksum function

- Unpredictable for adversary
  - Pseudo-random memory traversal
  - Seeded by challenge n
- Deterministic execution time: Δt_{cksum} known to verifier
  - Supervisor mode
  - Maskable interrupts disabled
- Time optimal implementation

Outline

1 Remote attestation
- Motivation
- Trusted computing platforms
- Legacy platforms

2 Legacy OS with TPM
- TPM time stamping
- Improved Pioneer Protocol
- Trusted bootloader

3 Conclusions

TPM time stamping

- `TPM_TickStampBlob()` and `TPM_GetTicks()` (TPM v1.2)
- $TS \leftarrow Sign_{SK}(blob||t||TSN)$
- Resolution: max 1 μs, min 1 ms
- On startup
  - Tick counter t reset to 0
  - Tick Session Nonce (TSN) initialized with random value

Experiments

- Infineon SLB 9635 TT 1.2
  - Resolution = 1 ms
- Atmel AT97SC3203
  - Behaves as monotonic counter (TCG compliant?)

Outline

1 Remote attestation
- Motivation
- Trusted computing platforms
- Legacy platforms

2 Legacy OS with TPM
- TPM time stamping
- Improved Pioneer Protocol
- Trusted bootloader

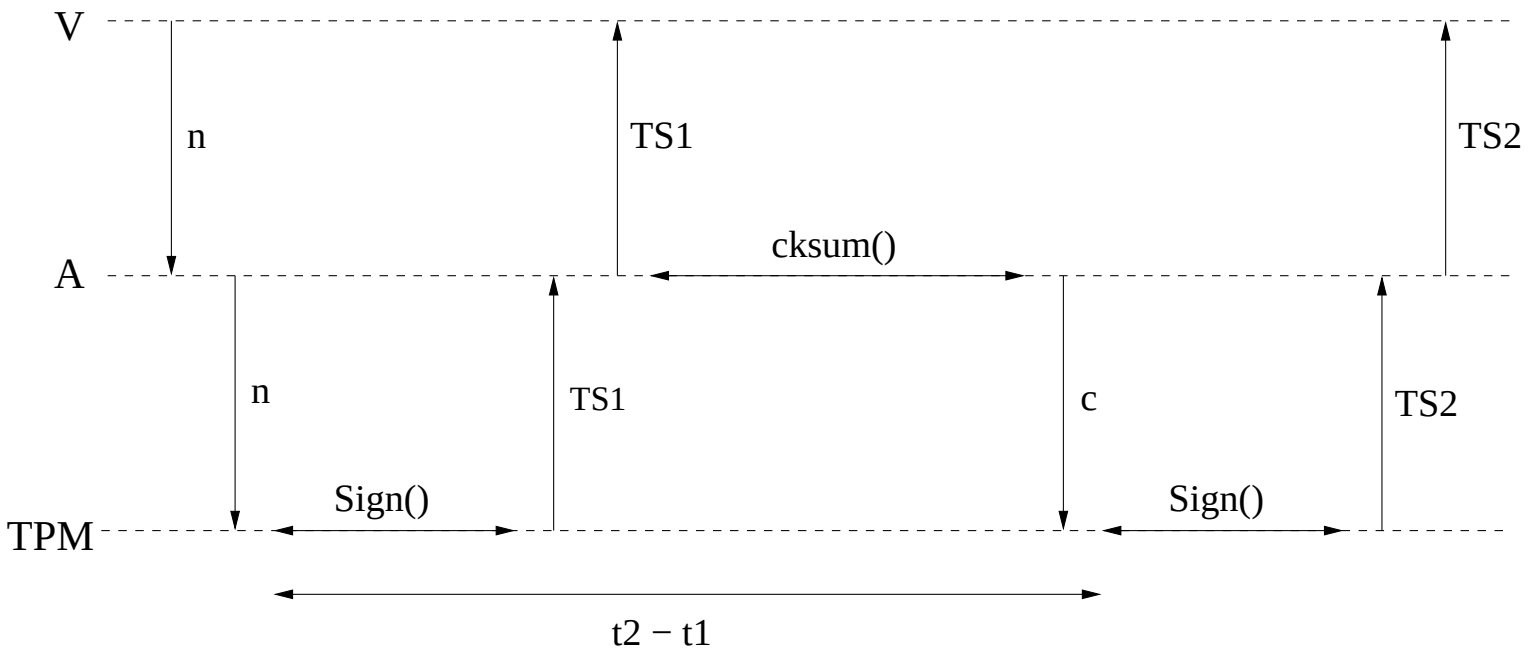
3 Conclusions

Improving Pioneer with TPM time stamping

- Verifier V checks integrity of verification agent A
  1. $V \rightarrow A : n$
  2. $V \leftarrow A : TS_1 \leftarrow Sign_{TPM}(n||t_1||TSN_1)$
  3. $A : c \leftarrow cksum(TS_1, V)$
  4. $V \leftarrow A : TS_2 \leftarrow Sign_{TPM}(c||t_2||TSN_2)$
  5. V:
     - verify TS_1 and TS_2
     - check $TSN_1 = TSN_2$
     - check $t_2 - t_1 < \Delta t_{expected}$
     - verify c
- Verification agent reports integrity of application E
  7. $A : h \leftarrow hash(TS_2, E)$
  8. $V \leftarrow A : h$
  9. V: verify h

Local time measurement

- $t_2 - t_1 < \Delta t_{expected} = \Delta t_{cksum} + \Delta t_{Sign} + \delta t$
- Atmel TPM: $\Delta t_{Sign} = 100$ ms (1024) and 500 ms (2048)



Advantages

- Local time measurement
  - No non-deterministic network latency
  - Resolution is limited $\Rightarrow \Delta t_{cksum} \nearrow$
- Unique platform identification
  - Link hardware configuration to TPM signing key
  - Prevents proxy attack
- Basic TPM support
  - Only device driver
  - No adapted bootloader
  - No adapted operating system
- Immune to TPM reset attack
  - $TSN_1 \neq TSN_2$

Outline

1 Remote attestation
- Motivation
- Trusted computing platforms
- Legacy platforms

2 Legacy OS with TPM
- TPM time stamping
- Improved Pioneer Protocol
- Trusted bootloader

3 Conclusions

Configuration identification

Hardware upgrade

- Adversary can speed up *cksum*()
- Replace CPU or RAM

- TCG chain of trust until bootloader
  1. Bootloader records CPUID in TPM
  2. Bootloader benchmarks *cksum*() and stores $\Delta t_{expected}$ in TPM
- TCG attestation to report hardware configuration
- Hardware upgrade detected

Conclusions

- Trusted computing support limited
- Secure operating system required to offer application level attestation
- Pure software based attestation for legacy platform has shortcomings
- Bridge the gap by using TPM time stamping and trusted bootloader