CSE543 - Computer and Network Security

Module: Trusted Computing

Professor Trent Jaeger
What is Trust?
What is Trust?

- dictionary.com
  - Firm reliance on the integrity, ability, or character of a person or thing.
What is Trust?

- dictionary.com
  - Firm reliance on the integrity, ability, or character of a person or thing.

- What do you trust?
  - Trust Exercise
What is Trust?

- dictionary.com
  - Firm reliance on the integrity, ability, or character of a person or thing.

- What do you trust?
  - Trust Exercise

- Do we trust our computers?
Trust

• “a system that you are forced to trust because you have no choice” -- US DoD
Trust

• “a system that you are forced to trust because you have no choice” -- US DoD

• “A ‘trusted’ computer does not mean a computer is trustworthy” -- B. Schneier
Trusted Computing Base

- Trusted Computing Base (TCB)
  - Hardware, Firmware, Operating System, etc
- There is always a level at which we must rely on trust
- How can we shrink the TCB?
Trustworthy Computing

- Microsoft Palladium (NGSCB)
Example of FUD

- Trusted Computing: An Animated Short -
  http://www.lafkon.net/tc/
Trusted Computing

• Components (according to Wikipedia)
  ‣ Secure I/O
  ‣ Memory Curtaining
  ‣ Sealed Storage
  ‣ Remote Attestation

• Requires hardware support
The Trusted Platform Module (TPM) provides hardware support for **sealed storage** and **remote attestation**

What else can it do?

- www.trustedcomputinggroup.org
Where are the TPMs?
TPM Components

- Non-Volatile Storage
- Platform Configuration Register (PCR)
- Attestation Identity Key (AIK)
- Program Code

- Random Number Generator
- SHA-1 Engine
- Key Generation
- RSA Engine
- Opt-In
- Exec Engine

I/O
TPM Discrete Components

• Input/Output (I/O)
  ‣ Allows the TPM to communicate with the rest of the system
• Non-Volatile Storage
  ‣ Stores long term keys for the TPM
• Platform Configuration Registers (PCRs)
  ‣ Provide state storage
• Attestation Identity Keys (AIKs)
  ‣ Public/Private keys used for remote attestation
• Program Code
  ‣ Firmware for measuring platform devices
• Random Number Generator (RNG)
  ‣ Used for key generation, nonce creation, etc
TPM Discrete Components

- **SHA-1 Engine**
  - Used for computing signatures, creating key Blobs, etc

- **RSA Key Generation**
  - Creates signing keys, storage keys, etc. (2048 bit)

- **RSA Engine**
  - Provides RSA functions for signing, encryption/decryption

- **Opt-In**
  - Allows the TPM to be disabled

- **Execution Engine**
  - Executes Program Code, performing TPM initialization and measurement taking
Tracking State

• Platform Configuration Registers (PCRs) maintain state values.
  
• A PCR can only be modified through the Extend operation
  
  ‣ Extend(PCR[i], value) :
    • PCR[i] = SHA1(PCR[i] · value)

• The only way to place a PCR into a state is to extend it a certain number of times with specific values

Measurement Flow
(Transitive Trust)

Application Code

OS Code

OS Loader Code

BIOS Self Measurement
Secure vs. Authenticated

• Secure boot stops execution if measurements are not correct

• Authenticated boot measures each boot state and lets remote systems determine if it is correct

• The Trusted Computing Group architecture uses authenticated boot
Protected Storage

• The TPM has limited storage capacity
  ‣ Key pairs are commonly stored on the system, but are encrypted by a storage key

• Users can protect data by allowing the TPM to control access to the symmetric key

• Access to keys can be sealed to a particular PCR state
Public/Private Keys

• Endorsement Key (EK)
  ‣ Only one EK pair for the lifetime of the TPM
  ‣ Usually set by manufacturer
  ‣ Private portion never leaves the TPM

• Storage Root Key (SRK)
  ‣ Created as part of creating a new platform owner
  ‣ Used for protected storage
  ‣ Manages other keys, e.g., storage keys
  ‣ Private portion never leaves the TPM

• Attestation Identity Keys (AIKs)
  ‣ Used for remote attestation
  ‣ The TPM may have multiple AIKs
Using TCG

- Justify System Integrity
- Attestation Approaches
  - Trusted Platform on Demand (TPoD)
    - IBM Research Tokyo
  - Linux Integrity Measurement Architecture
    - Sailer et al. (USENIX Security 2004)
  - BIND: A Fine-grained Attestation Service for Secure Distributed Systems
    - Shi et al. (IEEE S&P 2005)
- Network Authentication
  - Trusted Network Connect (TNC)
    - www.trustedcomputinggroup.org
Integrity Measurement

- IPsec and SSL provide secure communication
  ‣ But with whom am I talking?

Secure Channel

On-Demand / Grid
Secure Domains
B2B Application
Thin-Client

Monday, December 10, 12
Integrity Measurement

TCG-based Integrity Measurement Architecture

Defined by Grub (IBM Tokyo Research Lab)

Defined by TCG (Platform specific)

Platform Configuration Registers 0-23

Execution Flow

Measurement Flow

Application code

OS code

OS Loader code

CRTM code

TBB + Roots of Trust

0-7

4-7

>= 8
Basic Idea

**Measurement**

- SHA1(Boot Process)
- SHA1(Kernel)
- SHA1(Kernel Modules)
- SHA1(Program)
- SHA1(Libraries)
- SHA1(Configurations)
- SHA1(Structured data)

**System-Representation**

- Signed TPM Aggregate

**System Properties**

- ext. Information (CERT, ...)

**Attested System**

- Data
- Program
- Config data
- Boot-Process
- Kernel
- Kernel module

**Analysis**

- Known Fingerprints
Measurement List

- /bin/bash
- Execution path:
  - Execve(*file)
  - SHA1
- Integrity Value
- Measurement List (Kernel-held)
- Memory Map
- Schedule

Linux Security Module

Traditional execution path
Some Details

- Kernel Measures
  - Executables, Libraries, Modules
- At
  - Load time only
- Applications May Measure Also
  - Critical input

Issues Addressed:
- Prevents writing on actively measured files
  - Cannot open for write while file is open
- Non-deterministic loading
  - Need measurement list
Key Distribution

• Before remote attestation can occur, the challenger must have either knowledge of the public portion of an AIK, or a CA’s public key

• Old standards required the Privacy CA to know the TPM’s Public Endorsement Key (PUBEK)

• Direct Anonymous Attestation (DAA), added to the latest specifications, uses a zero-knowledge proof to ensure the TPM is real
Using TCG

• Many claim TCG will aid DRM

• How might one use the TPM for DRM?
  ‣ Discuss

• Trusted Computing is a double-edged sword
  ‣ so is cryptography
False Claims

• Having a TPM will keep me from using opensource software
  ‣ No, the TCG architecture only specifies authenticated boot. This simply records each step, but does not, and cannot, stop the use of opensource operating systems, e.g. Linux

• TPM, Palladium/NGSCB, and DRM are all the same
  ‣ No, the TPM is only one of the components required for NGSCB to function

• Loss of Internet Anonymity
  ‣ The addition of DAA allows Privacy CAs to function with zero-knowledge proofs

• Others?