Trustworthy Computing

CSE443 - Spring 2012
Introduction to Computer and Network Security
Professor Jaeger

www.cse.psu.edu/~tjaeger/cse443-s12/
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
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?
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?
Building Trust

• To build trust in software
  – What do we need to know about it?

• What if we had hardware to measure this?
  – What would it need to do?
  – How would we build systems differently?
Trustworthy Computing

- Microsoft Palladium (NGSCB)
Example of FUD

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

• Components
  – Secure I/O
  – Memory Curtaining
  – Sealed Storage
  – Remote Attestation

• Requires hardware support
Trusted Platform Module

• 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 Component Architecture

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

- I/O
  - Random Number Generator
  - SHA-1 Engine
  - Key Generation
  - RSA Engine
  - Opt-In
  - Exec Engine
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] \cdot value)
- The only way to place a PCR into a state is to extend it a certain number of times with specific values
Secure vs. Authenticated Boot

• 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*
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 sealed 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
Sealed 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
Remote Attestation

- 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.
Linux IMA

- Measure all software and static configuration files
Using TPM

• Many claim TPM will aid DRM

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

• Trusted Computing is a \textit{double-edged sword}
  – so is cryptography
False Claims

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

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

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

• What is the correct OS state?
  – How do you verify this state in a heterogeneous environment?
  – Do security updates keep me from functioning?

• Privacy of software system
  – Must they know the state of my machine?

• How do we take benefit of the TPM and Trusted Computing?