Trusted Computing – Special Aspects and Challenges

Prof. Dr.-Ing. Ahmad-Reza Sadeghi
Chair for System Security
Horst-Görtz-Institute for IT-Security
Ruhr-University Bochum, Germany

http://www.trust.rub.de
Organizational Issues

- **Lecture**
  - Mondays 10.15 am – 11.45 am in IC 1/161

- **Exercises**
  - Theoretical part (homework)
  - Practical part (in the Lab for Operating System Security and Trusted Computing, IC 4/31)
  - 7 Exercises of two hours, starting in the middle of Mai

- **Tutors**
  - Hans Lühr, Biljana Cubaleska (contact data on www.trust.rub.de)

- **Exam**
  - Oral examination (75 % of the mark)
  - Exercises (25 % of the mark)
Recommended Literature

- D. Challenger, K. Yoder, et al.
  “A Practical Guide to Trusted Computing”
  IBM Press, 2008

- Thomas Müller
  “Trusted Computing Systeme – Konzepte und Anforderungen”
  Springer Verlag, 2008

- Lecture Website:
  http://www.ei.rub.de/studierende/lehrveranstaltungen/231/
  - Lecture slides
  - Exercises
  - Other references
  - All announcements
Roadmap of this Lecture

- Introduction to trusted computing
- Trusted Platform Module (TCG)
- Selected TCG Functionalities
  - Authenticated boot, binding and sealing, attestation, trusted network connect
- Trusted virtualization
- Some research concepts and challenges
  - IBM Integrity Measurement Architecture, property-based attestation, trusted channels, virtual TPM, TPM compliance, trusted virtual domains
Chapter 1: Introduction to Trusted Computing

Prof. Dr.-Ing. Ahmad-Reza Sadeghi
Chair for System Security
Horst-Görtz-Institute for IT-Security
Ruhr-University Bochum, Germany

http://www.trust.rub.de
Roadmap of Chapter 1

Introduction to Trusted Computing

- **Motivation**
- **Notion of trust**
- **Towards trustworthy computing platforms**
- **Trusted Computing Group (TCG) approach to trusted computing**
- **Basic TCG concepts**
The Big Picture

- Trustworthiness in distributed IT systems
  - Different parties with potentially conflicting requirements involved
  - Cryptographic methods are of limited help
- How to define „trustworthiness“?
- How to determine/verify it?
- How could common computing platforms support such functionality?
  - Even a secure OS cannot verify own integrity
- The role of Trusted Computing
  - Enable the reasoning about the “trustworthiness” of own and other’s IT system
Demand for TC and Application Domains

- **Demand for Trusted Computing**
  - Improve security of existing IT Systems (malware, phishing, etc.)
  - Increasing threats for IT systems
  - Inflexibility of traditional secure systems (reference monitors)
  - Improve existing IT infrastructures (e.g., VPN)
  - Enable new applications with sophisticated (security) requirements

- **Application domains**
  - Monitoring and verifying integrity of IT systems
  - Controlling access to and usage of services and resources (online services, shared hardware, sensitive data)
Possible Use-Cases

- **E-Services**
  - Government (e.g., e-Voting integrity)
  - Health (e.g., confidentiality of sensitive medical records)
  - Commerce (e.g., enforceability of digital signatures)
- **Online banking**
- **Grid computing**
- **Digital/enterprise rights management**
- **Secure supply chains**
- **Mobile computing**
Roadmap of Chapter 1

Introduction to Trusted Computing

- Motivation
- Notion of trust
- Towards trustworthy computing platforms
- Trusted Computing Group (TCG) approach to trusted computing
- Basic TCG concepts
Issues and Vocabulary

- **Trust**
  - Complicated notion studied and debated in different areas (social sciences, philosophy, psychology, computer science,...)
  - Notion relating to belief in honesty, truthfulness, competence, reliability etc. of the trusted entity
  - Social Trust - belief in the safety or goodness of something because of reputation, association, recommendation, perceived benefit

- **Meanings (an attempt)**
  - Secure: system or component will not fail with respect to protection goals
  - Trusted: system or component whose failure can break the (security) policy (Trusted Computing base (TCB))
  - Trustworthy: the degree to which the behavior of the component or system is demonstrably compliant with its stated functionality

- **Trusted Computing Group (TCG) defines a system as trusted**
  - “[...] if it always behaves in the expected manner for the intended purpose.”
Basic Idea for Trusted Platform

- Trusted components in hardware and software
- Provides a variety of functions that must be trusted
  - in particular a set of cryptographic and security functions
- Creates a foundation of trust for software
- Provides hardware protection for sensitive data
  - e.g., keys, counters, etc.
- Desired goals
  - Trusted Computing Base (TCB) should be minimized
  - Compatibility to commodity systems
Objectives

- **Multilateral security**
  - Considers different and possibly conflicting security requirements of different parties and strives to balance these requirements
  - Refers to (classical) security goal (e.g., confidentiality, integrity and availability)
  - Typical conflict occurs between the wish for privacy and the interest in cooperation

- **Problems**
  - Insufficient protection in SW and HW of existing computing platforms
    - Malicious code (viruses, Trojan horses, ...)
    - DMA (Direct Memory Access)
    - No secure storage
  - Main reasons
    - High complexity and poor fault isolation of operating systems
    - Lack of functional and protection mechanisms in hardware
    - Security unawareness of users or security measures still not useable enough
Roadmap of Chapter 1

Introduction to Trusted Computing

- Motivation
- Notion of trust
- Towards trustworthy computing platforms
- Trusted Computing Group (TCG) approach to trusted computing
- Basic TCG concepts
Primary Goals

- Improve security of computing platforms
- Reuse existing modules
  - e.g., GUI, common OS
- Applicable for different OS
  - No monopoly, space for innovation (small and mid-sized companies)
- Open architecture
  - Use open standards and open source components
  - Trustworthiness/costs/reliability/compatibility
- Efficient portability
- Allow realization of new applications/business models
  - Providing multilateral security needed for underlying applications
    (based on various sets of assumptions and trust relations)
  - Avoiding potential misuse of trusted computing functionalities
Desired Primitives

1. Metric for code configuration
   - I/O behavior of a machine based on an initial state
   - e.g., represented by the hash value of the binary code
     - Problematic when functionality depends on other codes not included in hashing (e.g., shared or dynamically linked libraries)
   - Sometimes the notion of code identity is used [EnLaMaWi2003]

2. Integrity verification (Attestation)
   - Allows a computing platform to export verifiable information about its properties (e.g., identity and initial state)
   - Comes from the requirement of assuring the executing image and environment of an application located on a remote computing platform
Desired Primitives (cntd.)

3. Secure storage
   - to persist data securely between executions using traditional untrusted storage like hard drives
   - To encrypt data and assured to be the only capable of decrypting it

4. Strong process isolation
   - Assured (memory space) separation between processes
   - Prevents a process from reading or modifying another process’s memory

5. Secure I/O
   - Allows application to assure the end-points of input and output operations
   - A user can be assured to securely interact with the intended application
Need for Secure Hardware and Software

- **Hardware**
  - Even a secure operating system cannot verify its own integrity (another party is needed)
  - Secure storage
  - DMA control
    - Isolation of security-critical programs
  - Hardware-based random numbers
    - Fundamental to cryptography

- **Software (operating systems)**
  - Hardening, e.g., SE Linux [LoSm2001]
    - Still too complex and large TCB (Trusted Computing Base)
  - Complete new design
    - e.g., Trusted Mach, EROS (Extremely Reliable Operating System) [TrustedMach1991, Shap1999]
    - Compatibility problem, less market acceptance
  - Secure Virtual Machine Monitors (e.g., [Gold74, Sailer et al 2005])
    - Allow reuse of legacy software
Introduction to Trusted Computing

- Motivation
- Notion of trust
- Towards trustworthy computing platforms
- Trusted Computing Group (TCG) approach to trusted computing
- Basic TCG concepts
Trusted Computing Group (TCG)

- Consortium of IT-Enterprises (since April 2003)
  - Today more than 120 members [TCG]
    - www.trustedcomputing.org/about/members/
- Focus on development of hardware-enabled trusted computing and security technology across multiple platforms and devices
- Evolved from Trusted Computing Platform Alliance (TCPA)
  - Formed by Hewlett-Packard (HP), Compaq (today part of HP), IBM, Intel and Microsoft in January 1999
- Has published various specifications
TCG Work Groups I

- Trusted Platform Module (TPM) Work Group
  - Specifies Trusted Platform Module (TPM)

- TCG Software Stack (TSS) Work Group
  - Specifies hardware and operating system independent interfaces for using TPM features

- Trusted Network Connect (TNC) Work Group
  - Standards ensuring multi-vendor interoperability that enable network operators to enforce security policies for endpoint integrity for network connections

- Infrastructure Work Group (IWG)
  - Adoption and integration of TCG concepts into Internet and enterprise infrastructure technologies
TCG Work Groups II

- **PC Client Work Group**
  - Specifies functionality, interfaces, and security and privacy requirements for PC clients using TCG components
  - Has advisory role for TPM and other TCG work groups

- **Server Work Group**
  - Specifies integration of TCG technology into server systems

- **Mobile Phone Work Group**
  - Adoption of TCG concepts for mobile devices
  - Addresses specific features of mobile devices like connectivity and limited capability
TCG Work Groups III

- Storage System Work Group
  - Standards for security services on dedicated storage systems with removable media drives, flash storage and multiple storage device systems including dedicated storage controller interfaces
  - E.g., ATA, Serial ATA, SCSI, FibreChannel, USB storage, FireWire (IEEE 1394) and Network Attached Storage (NAS)
TCG Main Specification

- Trusted Platform Module (TPM) [TPM2002, TPM2003, TPM2007]
  - Provides a set of immutable cryptographic and security functions

- Trusted Software Stack (TSS) [TSS2003, TSS2007]
  - Issues low-level TPM requests and receives low-level TPM responses on behalf of higher-level applications
Roadmap of Chapter 1

Introduction to Trusted Computing

- Motivation
- Notion of trust
- Towards trustworthy computing platforms
- Trusted Computing Group (TCG) approach to trusted computing

- Basic TCG concepts
  - Chain of trust
  - Integrity measurements
  - Abstract model of TCG concept
Chain of Trust for Measurements

- Goal is to gain trust in entity $E_n$
- Operational standpoint: $E_0$ launches $E_1$, $E_1$ launches $E_2$, ...
- To trust $E_n$ one must trust $E_{n-1}$
- $E_0$, $E_1$ to $E_n$ creates a “chain of trust”
- “Transitive trust”
  - Trust is transitive from $E_0$ to $E_1$ to $E_2$ ...
  - It does not invert: trusting $E_0$ does NOT imply that one must trust $E_2$
  - Trusting $E_2$ REQUIRES one to trust $E_0$ and $E_1$
Chain Measurement

- **What does one need to “trust” the chain**
  - The identity of each item in the chain
  - identity = measurement (according to TCG definition)
    - E.g., a hash value of the binary code
  - Generic flow: each member measures its successor before passing the control to it
    - $E_0$ measures $E_1$ before passing control to $E_1$ and so on

- **Who measures $E_0$?**
  - Root of Trust for Measurements (RTM)
    - Must be trusted, no mechanism to measure it
    - To create a chain of trust the first entity must be the RTM
Performing Integrity Measurements

1. RTM measures entity E
2. RTM creates Event Structure in TPM Event Log
   - SML contains the Event Structures for all measurements extended to the SM
   - SM Event Log can be stored on any storage device
     - E.g., hard disk
3. RTM extends value into Registers
4. Execute/pass control to entity E
Abstract Model of TCG Concept

**Trusted Platform P**
- provides integrity of host H

**Host H (untrusted)**
- firmware
- operating system
- applications

**Attestor A**
- trusted component (hard- and software)
- Securely stores $C_H$

**Verifier V**
- local or remote
- can decide whether $C_H$ violates its security requirements
- can “bind/seal” data D to a specific (probably secure) configuration/state of H

**Challenge / Verifier**

**User / Adversary**

**Attest**: Verify system integrity

**Bind/Seal**: Access control depending on system configuration

$C_H$ - initial configuration/state of host H when platform P has been booted

D - data to be revealed only if host H is in the (secure) configuration $C_H$

---

insecure channel

secure channel
Concerns About TCG Approach

- Potential basis for Digital Rights Management (DRM)
- Less freedom
  - Including freedom of choice and user control
- Privacy violation
  - Disclosure of platform identity and configuration
- Confusing language
  - “Trust”, “control”, “opt-in”, ...
- Core specifications unreadable
  - Leads to misunderstanding
- Danger of restricting competition
  - Misuse of sealed storage capabilities, locking out alternative applications and inhibiting interoperation
- Much of the criticism related to Microsoft’s NGSCB
  - Several name changes Palladium, NGSCB, Longhorn, Vista
  - Bad publicity or legal challenges on rights to the names
Legal Requirements on TC/TCG

- **Main actors**
  - German Government Requirements Catalogue on TCG
  - Electronic Frontier Foundation (EFF)
  - European Commission Article 29 (Data Protection Working Party)
  - New Zealand Government’s initiative on TC/DRM technologies

- **Main requirements**
  - Prevent confusion and clarify terms (trust, trusted, trustworthy, thread model)
  - Privacy issues (user, platform,...), application and design of new technologies should be privacy compliant by default
  - Unrestricted user control (e.g., over keys and IT technology)
  - Transparency of certification
  - Option for transferring secrets between different machines
  - Functional separation of TPM and CPU/chipsets
  - Product discrimination
  - TC/DRM should not adversely affect security of government-held information
Next Chapter:

Chapter 2:

**Trusted Platform Module (TPM) - Main TCG Specification**