Fachhochschule Gelsenkirchen

Trusted Computing
→ Introduction

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Content

- Aim and outcomes of this lecture
- Motivation of Trusted Computing
- Notion of Trust
- Towards Trustworthy Computing Platform
- TCG Approach to Trusted Computing
- Basic TCG Concepts
- Summary

Content

- **Aim and outcomes of this lecture**
- Motivation of Trusted Computing
- Notion of Trust
- Towards Trustworthy Computing Platform
- TCG Approach to Trusted Computing
- Basic TCG Concepts
- Summary

Trusted Computing
→ Aims and outcomes of this lecture

Aims

- To introduce in the topic “Trusted Computing”
- To explore the need and the general idea of Trusted Computing
- To analyze the goals of Trusted Computing
- To assess the concerns of Trusted Computing

At the end of this lecture you will be able to:

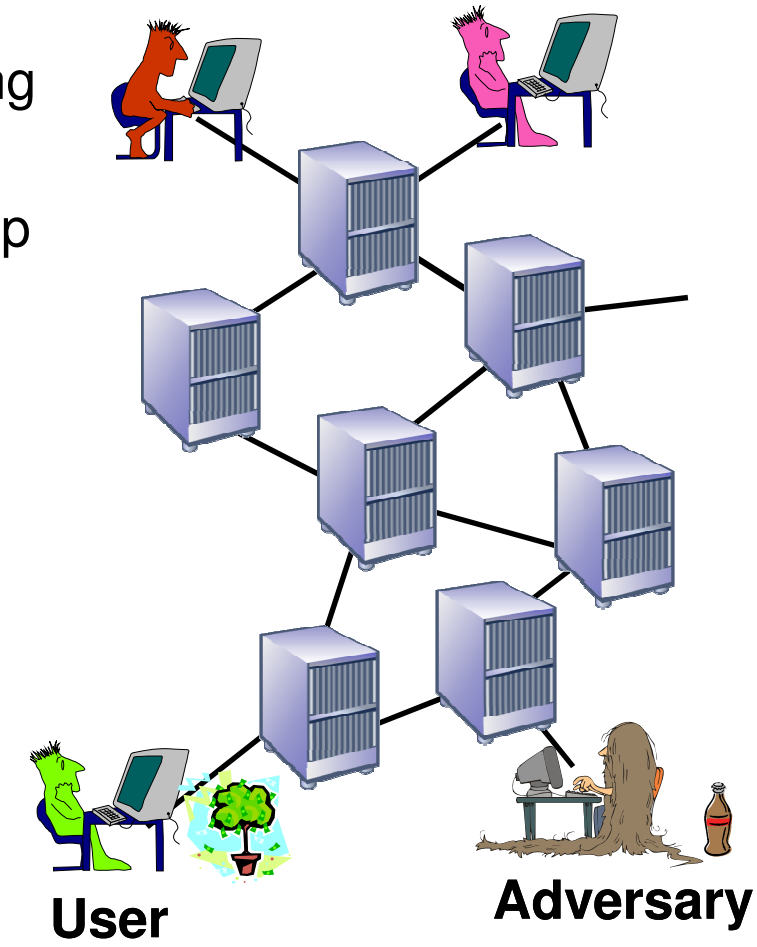
- Understand what the basic idea and the need for Trusted Computing is
- Know something about the approach to Trusted Computing
- Know the Trusted Computing Group (TCG) and what they do
- Understand the need of Trusted Computing

Content

- Aim and outcomes of this lecture
- **Motivation of Trusted Computing**
- Notion of Trust
- Towards Trustworthy Computing Platform
- TCG Approach to Trusted Computing
- Basic TCG Concepts
- Summary

Motivation of Trusted Computing
→ 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 it’s own integrity
- **The role of Trusted Computing**
  - Enable the reasoning about the “trustworthiness” of own and other’s IT system [see also Kuhl2003, KuGe2003]



Motivation of Trusted Computing
→ 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)

Motivation of Trusted Computing
→ Attacks to be resisted

- All software attacks

- Some (but not all) hardware attacks
  - nothing can guarantee that all hardware attacks can be resisted unless the system is physically isolated (in a locked room, surrounded by armed guards)
  - a “smartcard” level of protection is all we can do at a reasonable price

Motivation of Trusted Computing
→ 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

Content

- Aim and outcomes of this lecture
- Motivation of Trusted Computing
- **Notion of Trust**
- Towards Trustworthy Computing Platform
- TCG Approach to Trusted Computing
- Basic TCG Concepts
- Summary

Notion of Trust
→ Issues and Vocabulary

- **Trust** [RoSiBuCa98, Luhm1979, Cole1990, RoSiBuCa98]
  - 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

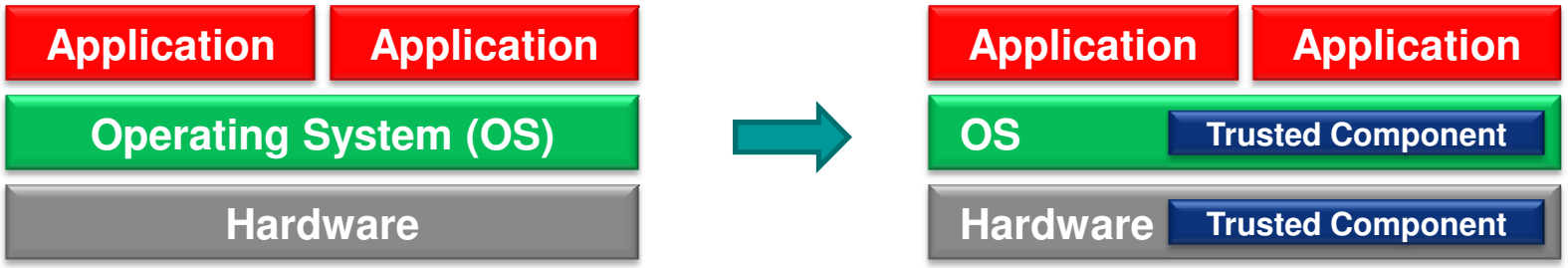
- **Meanings** (an attempt) (see also [BILBNC2005])
  - ***Secure:*** system or component will not fail with respect to protection goals
  - ***Trusted:*** system or component whose failure can break the (security) policy (Trusted Computing Base (TCB))
  - ***Trustworthy:*** the degree to which the behavior 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."

Notion of Trust
→ Basic Idea for Trusted Platform

Trusted components in hardware and software

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



Conventional Platform **Trusted Platform**

Notion of Trust
→ Objectives

- **Multilateral Security** [Rann1994]
  - 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 (security)

- **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

Content

Trustworthy Computing Platforms
→ Primary Goals (1/2)

- **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

Trustworthy Computing Platforms
→ Primary Goals (2/2)

- **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

Trustworthy Computing Platforms
→ Desired Primitives (1/2)

- **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]

- **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

Trustworthy Computing Platforms
→ Desired Primitives (2/2)

- **Secure storage**
  - To persist data securely between executions using traditional untrusted storage like hard drives
  - To encrypt data and assure to be the only capable of decrypting it
- **Strong process isolation**
  - Assured (memory space) separation between processes
  - Prevents a process from reading or modifying another processes' memory
- **Secure I/O**
  - Allows applications to assure the end-points of input and output operations
  - A user can be assured to securely interact with the intended application

Trustworthy Computing Platforms
→ Need for Secure Hardware

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

Trustworthy Computing Platforms
→ Need for Secure Software (OS)

- **Hardening**, e.g., SELinux [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

Content

- Aim and outcomes of this lecture
- Motivation of Trusted Computing
- Notion of Trust
- Towards Trustworthy Computing Platform
- **TCG Approach to Trusted Computing**
- Basic TCG Concepts
- Summary

Trusted Computing Group (TCG)
→ Overview

- Consortium of IT enterprises (since April 2003)
  - Today more than 140 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

Trusted Computing Group (TCG)
→ Membership (1/2)

140 Total Members as of March 24, 2008
8 Promoter, 80 Contributor, 52 Adopter

Promoters
AMD
Hewlett-Packard
IBM
Infineon
Intel Corporation
Lenovo
Microsoft
Sun Microsystems, Inc.

Contributors
American Megatrends, Inc.
Aruba Networks
Atmel
AuthenTec, Inc.
Broadcom Corporation
Certicom Corp.
Citrix Systems, Inc
Decru
Dell, Inc.
DPHI, Inc.
Emulex Design and Manufacturing
Enterasys Networks
Ericsson Mobile Platforms AB
ETRI
Extreme Networks
France Telecom Group
Freescale Semiconductor
Fujitsu Limited
Fujitsu Siemens Computers
Gemalto NV
General Dynamics C4 Systems
Giesecke & Devrient
Green Hills Software
HID Global
Hitachi, Ltd.
Huawei Technologies Co., Ltd.
Identity Engines

Contributors
Infoblox
Insyde Software Corp.
InterDigital Communications, LLC
ITE Tech Inc.
Juniper Networks, Inc.
Lancope, Inc.
Lexar Media, Inc.
Lexmark International
Lockheed Martin
LSI Logic
Marvell Semiconductor, Inc.
Matsushita Electric Industrial
McAfee, Inc.
Mirage Networks
Mobile Armor, inc.
Motorola Inc.
NEC
Neoscale Systems
Nokia
Nokia Siemens Networks GmbH
Nortel
NTRU Cryptosystems, Inc.
NVIDIA
NXP Semiconductors
Oxford Semiconductors
Phoenix
PMC-Sierra
Renesas Technology Corp.
Ricoh Company LTD

Contributors
RSA, The Security Division of EMC
SafeNet, Inc.
Samsung Electronics Co.
SanDisk Corporation
Seagate Technology
SECUDE IT Security GmbH
Sharp Electronics Corporation
Siemens AG
SMSC
Sony Corporation
Spansion LLC
StepNexus, Inc
StillSecure
STMicroelectronics
Symantec
Symbian Ltd
Toshiba Corporation
Trapeze Networks
Unisys
UPEK, Inc.
Utimaco Safeware AG
VMware, Inc.
Vodafone Group Services LTD
Wave Systems
Western Digital

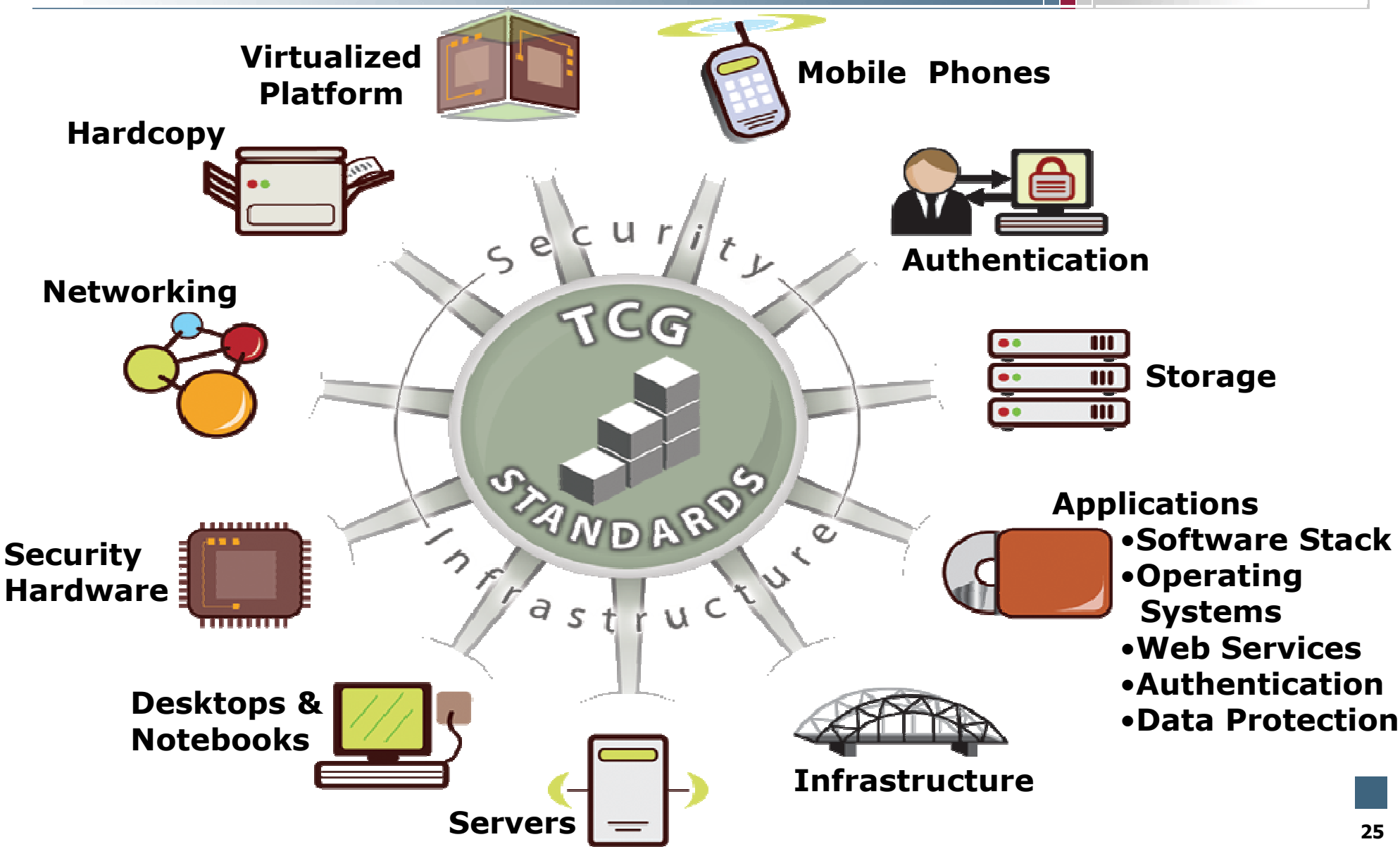
Trusted Computing Group (TCG)
→ Membership (1/2)

140 Total Members as of March 24, 2008
8 Promoter, 80 Contributor, 52 Adopter

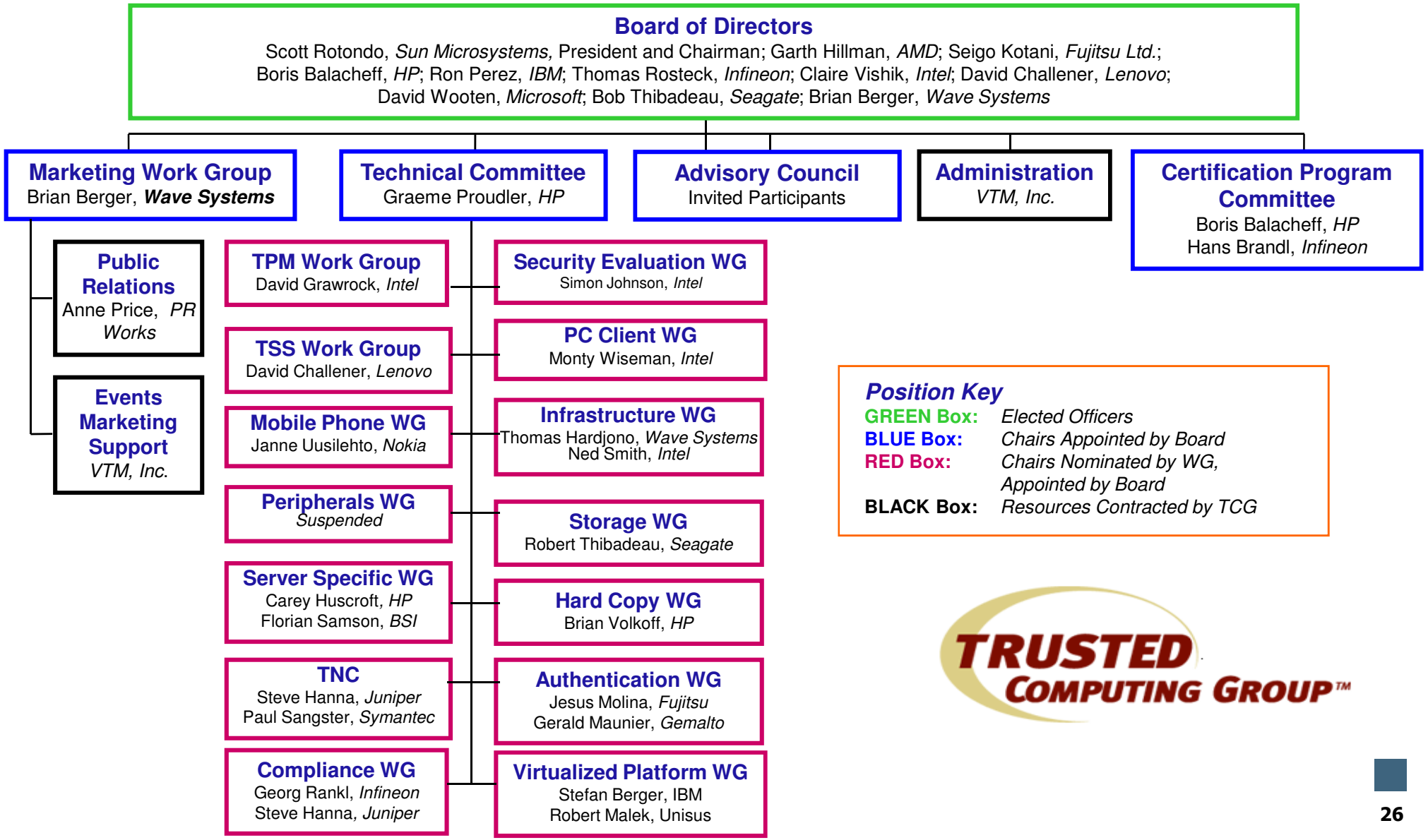
Adopters
Apani Networks
AUCONET GmbH
Avenda Systems
Bioscrypt Inc.
Bit9, Inc.
BlueCat Networks
BlueRidge Networks
BlueRISC, Inc.
Bradford Networks
ConSentry Networks
CMS Products
CPR Tools, Inc.
Cranite Systems, Inc.
Credant Technologies
Cryptomathic Ltd.
CryptoMill Technologies
Dartmouth College
FireScope Inc.
ForeScout Technologies
Hangzahou Synochip Technology Co. Ltd.
High Density Devices
ICT Economic Impact, Ltd.
IDEX ASA
Insight International Corp
Intellasys

Adopters
Link-A-Media Devices
Lockdown Networks
Mazu Networks
MoSys, Inc.
Nanjing Byosoft, Ltd
nSolutions, Inc.
O2 Micro
PatchLink Corporation
Penza Research Electrotechnical Institute
Q1 Labs
SafeBoot
Safend LTD.
Shavlik Technologies
SignaCert, Inc.
Sirrix AG Security Technologies
SkyRecon Systems
Softex, Inc.
Stonewood Electronics
TELUS
Thales Communication
The Boeing Company
Trust Digital
UNETsystem
Valicore Technologies, Inc.
ViaSat, Inc.
Vormetric, Inc.
Winbond Electronics Corporation

Trusted Computing Group (TCG)
→ The "BIG" Picture



TCG Organization



Position Key

GREEN Box:	*Elected Officers*
BLUE Box:	*Chairs Appointed by Board*
RED Box:	*Chairs Nominated by WG, Appointed by Board*
BLACK Box:	*Resources Contracted by TCG*

Specifications Published
→ Partial List

- **TPM Work Group**
  - TPM Specification Version 1.2 Rev 94
- **PC Client Work Group**
  - PC Client Specific TPM Interface Specification (TIS) Version 1.2
  - PC Client Specific Implementation Specification for Conventional Bios Version 1.2
  - TCG EFI Protocol Specification
  - TCG EFI Platform Specification
- **Server Work Group**
  - Generic Server Specification Version 1.0
  - TCG Itanium Architecture Based Server Specification Version 1.0
- **TSS Work Group**
  - Software Stack Specification Version 1.2
  - Software Stack1.2 Headers Errata 1
  - Software Stack Specification Version 1.1
  - Software Stack Specification Header File
- **TNC Subgroup**
  - TCG TNC Architecture Version 1.1
  - TCG TNC IF-IMC Specification Version 1.1
  - TCG TNC IF-IMV Specification Version 1.1
  - TCG TNC IF-PEP: Protocol Bindings for RADIUS Version 1.0
  - TCG TNC IF-Protocol Bindings for Tunneled EAP Methods Version 1.0
  - TCG TNC IF-TNCCS Specification Version 1.0
- **Infrastructure Work Group**
  - IWG Credentials Profile Spec
- **Mobile Phone Work Group**
  - TCG Mobile Reference Architecture Version 1.0
  - TCG Mobile Trusted Module Specification Version 1.0
- **Storage Work Group**
  - Storage Architecture Core Specification 0.9

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

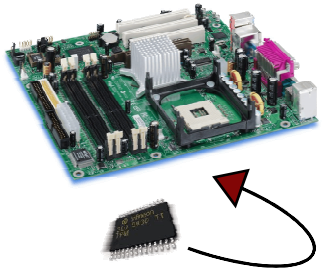
Trusted Computing Group (TCP)
→ Motivation and Idea

- ***Fundamental motivation***
  - Develop **open specifications** for trustworthy IT systems (servers, PCs, embedded systems, etc.)
  - Improve the security of distributed applications at a **reasonable economic cost**
  - Avoid any extensive changes to existing hardware or software

- ***Main Idea***
  - Manipulation-proof hardware component (securer than software) **→ "improvement" against software-based attacks.**
  - Security of the system is reduced to the security of a security module
  - The integrity and authenticity of an IT system can be reliably tested, even from a distance

Trusted Computing Group
→ Main Functions (1/2)

- ***Trusted Platform Modules (TPM)***
  - Reliable random generator (secure cryptographic keys)
  - Cryptographic functions: signature (RSA), hash function (SHA-1)
  - Creation of different cryptographic keys
  - **Platform Configuration Register (PCR) for storing the system configuration**.



TPM

- ***Secure Storage***
  - Creation of secure cryptographic keys
  - Storage of these keys in the hardware module

- ***Sealing***
  - Cryptographic keys can be binded to the IT system and/or a specific software configuration.
    - → Provide protection against manipulations of the operating system

Trusted Computing Group
→ Main Functions (2/2)

- ***(Remote) Attestation***
  - Analyse the current configuration of the IT system
  - Detecting manipulated IT systems (distributed systems, Web Services, …)
  - Communication only with trustworthy IT systems
- ***Access Control***
  - Implementation of access rules in a network with unknown IT systems (TNC)
- ***Trusted Boot***
  - System configuration can be checked (smartcard, USB stick, mobile phone)
- ***Installed TPMs***
  - 60 million by the end of 2006
  - 130 million by the end of 2007
  - 200 million by the end of 2008

TPM

Content

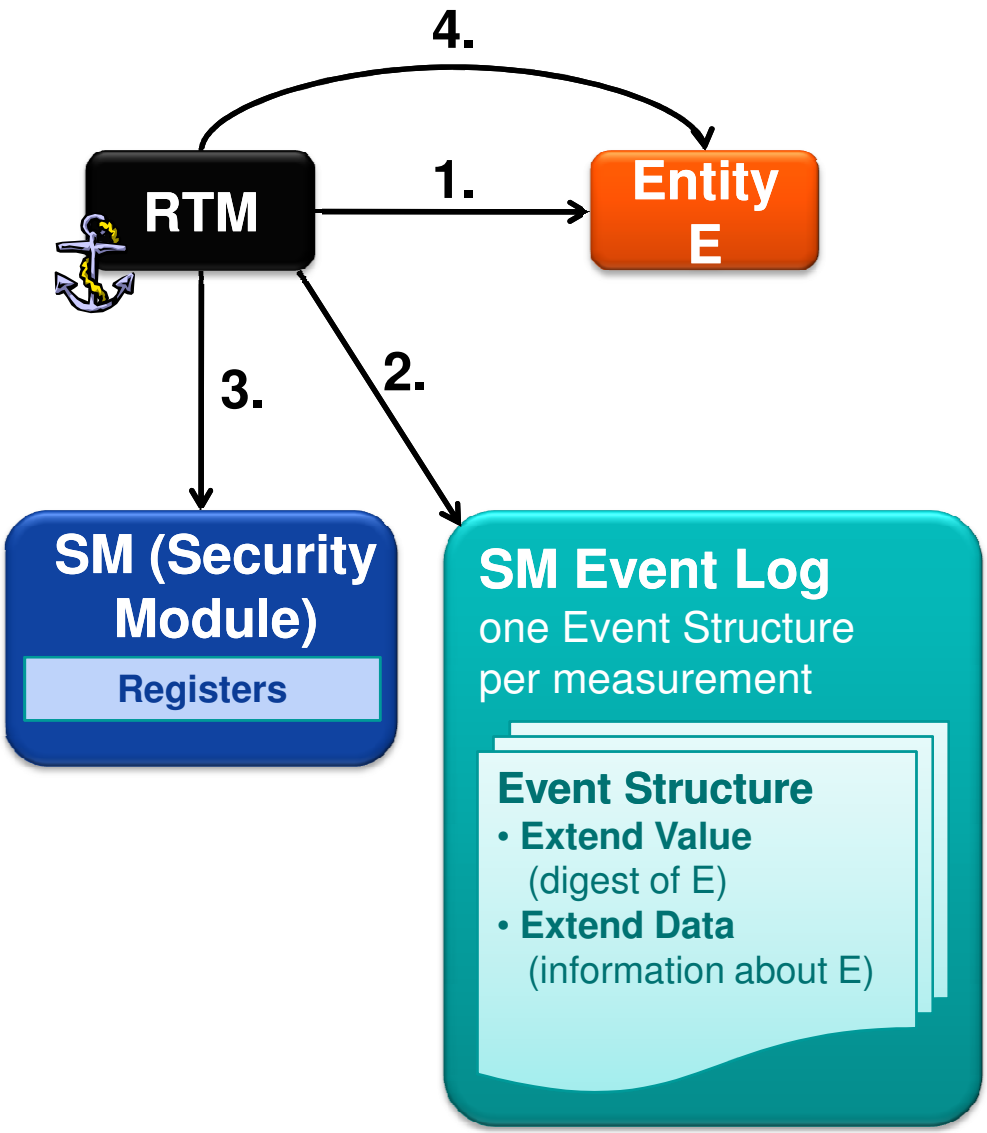
Basic TCG Concepts
→ Chain of Trust for Measurements

- 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

Basic TCG Concepts
→ Chain Measurement

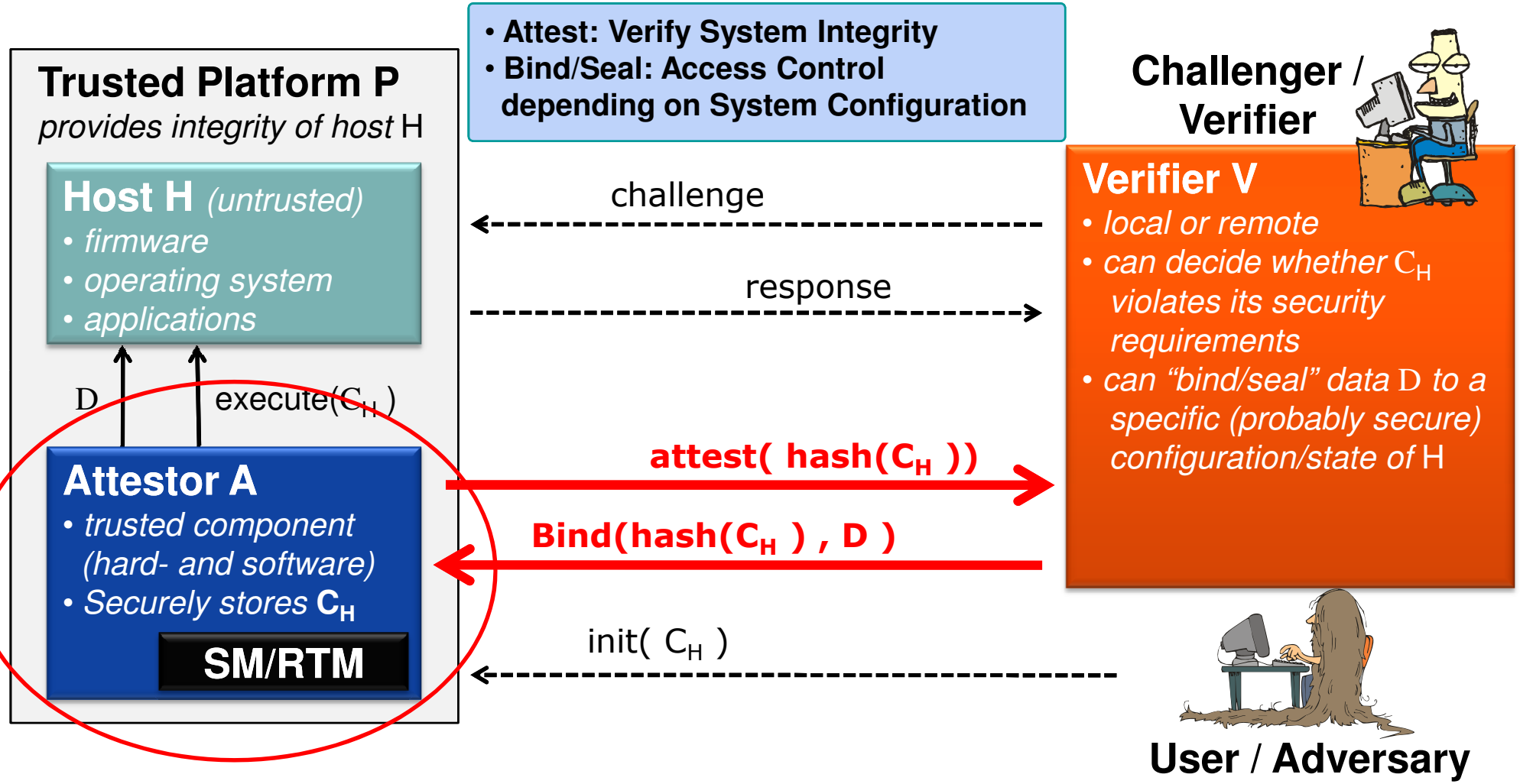
- **What does one need to "trust" the chain**
  - The identity of each item in the chain
  - identity = measurement (according to TCG definition)
    - e.g., a hash value of the binary code
  - ***Generic flow:*** each member measures its successor before passing the control to it
    - E_0 measures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

Basic TCG Concepts
→ 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

Basic TCG Concepts
→ Abstract Model of TCG



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

Basic TCG Concepts
→ TPM Supervises its Platform

- **Software can be affected** by other software
- Trusted components required to perform **integrity measurements**
- Minimal set of components that must be trusted:
  Root of Trust for Measurement (RTM)
  - Basic computing engine
    - CPU, system memory, chipset
  - CRTM (Core RTM, e.g., part of system BIOS)
  - TPM (Platform Configuration Registers, PCR)

Basic TCG Concepts
→ 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

Basic TCG Concepts
→ Concerns About TCG Approach

- **Danger of restricting competition**
  - Misuse of sealed storage capabilities, locking out alternative applications and inhibiting interoperation
    [Scho2003, Ande2002, Ande2003, Cour2002]

- **Much of the criticism related to Microsoft's NGSCB**
  - Several name changes Palladium, NGSCB, Longhorn, Vista
    [Microsoft2003a, Microsoft2003b, Microsoft2003c, Vista2006]
  - Bad publicity or legal challenges on rights to the names
    [Lemo2003, Bech2003]

Legal Requirements on TC/TCG
→ Main actors

- German Government Requirements Catalogue on TCG [GG2003]
- Electronic Frontier Foundation (EFF) [Scho2003]
- European Commission Article 29 (Data Protection Working Party) [EC2004]
- New Zealand Government's initiative on TC/DRM technologies [NZG2006]

Legal Requirements on TC/TCG
→ 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

Content

- Aim and outcomes of this lecture
- Motivation of Trusted Computing
- Notion of Trust
- Towards Trustworthy Computing Platform
- TCG Approach to Trusted Computing
- Basic TCG Concepts
- **Summary**

Trusted Computing
→ Summary

- We have to improve the security and we have to increase the threads.
- Trusted Computing seems to be a good approach to reach these targets.
- TCG is a consortium consisting of the most imported IT companies and these companies support specifications which can help to realize the trusted computing idea.

Fachhochschule Gelsenkirchen

Trusted Computing
→ Introduction

Thank you for your attention!
Questions?

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Trusted Computing
→ Literature

- [1] **Prof-. Dr.-Ing. Ahmad Reza Sadeghi**
  http://www.trust.rub.de/home/
- [2] N. Pohlmann, A.-R. Sadeghi, C. Stüble: "European Multilateral Secure Computing Base", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 09/2004
- [3] N. Pohlmann, H. Reimer: „Trusted Computing – eine Einführung", in "Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen", Hrsg.: N. Pohlmann, H. Reimer; Vieweg-Verlag, Wiesbaden 2008
- [4] M. Linnemann, N. Pohlmann: "An Airbag for the Operating System – A Pipedream?", ENISA Quarterly Vol. 3, No. 3, July-Sept 2007

Links:

Institute for Internet Security:
http://www.internet-sicherheit.de/forschung/aktuelle-projekte/trusted-computing/