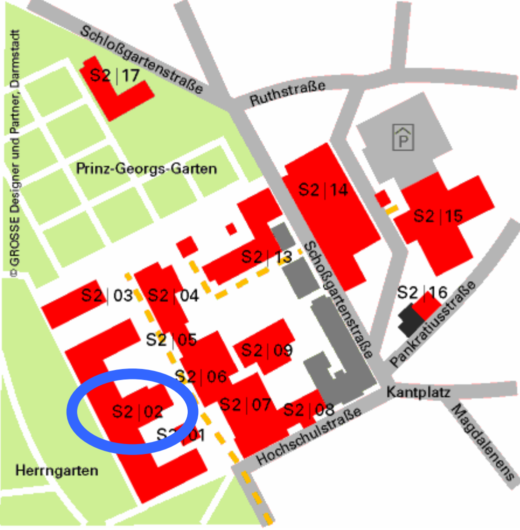
Trusted Computing: Introduction & Applications

Formalia
Lecture 1: TC History & Intro

Dr. Andreas U. Schmidt

Fraunhofer Institute for Secure Information Technology SIT,
Darmstadt, Germany

Formalia



- Venue
  - S2l02,Stadtmitte-Nord,
    Robert-Piloty-Gebäude,
    Hochschulstraße 10, 64289Darmstadt
  - Room E202
- Lecture Dates – in each case 16:00-17:30 MEST

Wed. 23.05.07	Wed. 30.05.07	Wed. 06.06.07	Mon. 11.06.07 Wed. 13.06.07
Wed. 20.06.07	Mon. 02.07.07 Wed. 04.07.07	Mon. 09.07.07 Wed. 11.07.07	Wed. 18.07.07

- Written Exam: Wed. 24.07.07
- Contact
  - Dr. Andreas U. Schmidt
    Fraunhofer SIT
    Rheinstraße 75
    64295 Darmstadt
    Tel. 06151 869 60227
    andreas.schmidt@sit.fraunhofer.de
- Slides: On www.sec.informatik.tu-darmstadt.de and andreas.schmidt.novalyst.de shortly after lecture

Contents 1/3

- TC Introduction & History
  - From TCPA to TCG; Motivations of the Industry and their evolution; The European view; TCG major players; TC related R&D
- TPM Architecture
  - Key Hierarchy and "Take Ownership"; TPM Lifecycle
- Trusted Boot
  - The PCR concept; Information in the Boot Log
- Trusted OS
  - TOS is an old concept; Trusted system architectures; Turaya; EMSCB; TC open source tools
- Remote Attestation
  - Trust Credentials; "Transitive trust"; AIK concepts and implementation issues; The trusted third party PCA

Contents 2/3

- Direct Anonymous Attestation
  - A steep approach to zero-knowledge proofs; The Idemix system; DAA in TC; Implementation and performance issues
- The MTM
  - Requirements of the mobile world; MTM core architecture; Trusted Engines; RIM certificates; Comparison with SIM/MegaSIM
- TCG Infrastructure standards
  - The infrastructure standard suite and how it brings TC "to life"
- TCG special standards
  - Virtualisation; Generalised Authentication; User Authentication (AWG); Major current TCG Activities
- "Traditional" mobile TC applications
  - The TCG's MTM use cases; content protection and DRM; device and software updates, ...
- Ticket systems employing AIKs
  - From AIKs to ticket identifiers; Ticket acquisition and redemption mechanisms; Trusted ticket service access architectures

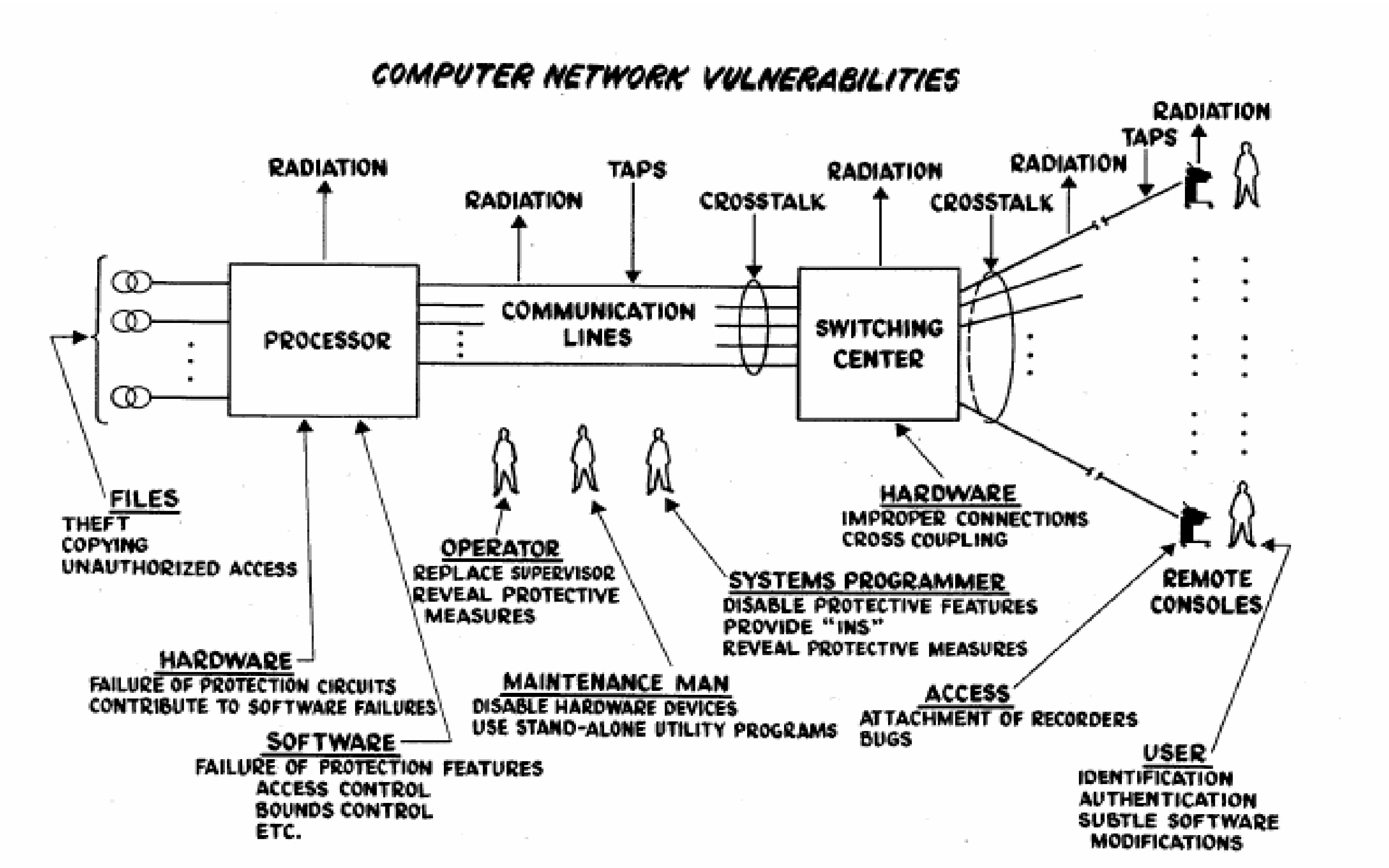
Contents 3/3

- The virtual SIM
  - GSM network access basics; putting GSM credentials into the MTM; three models for MTM based mobile network access; deployment and enrolment
- A bunch of mobile applications
  - Securing content in push services; trusted clock synchronisation; anonymous mobile devices; accessory bonding; forward pricing in rating systems; electronic signatures
- Towards a unified TC Application Infrastructure
  - A little bit of marketing for my EU FP7 project

Threats

- Computers and users are under attack
- What are we doing against it:
  - Installing patches
  - Update AntiVirus-Software
  - Upgrade firewall
  - Run Anti-Spyware software
  - Install Windows Defender
  - Install patches again
  - Check for updates
  - Download patches
  - ... and hope and pray...
- But why don't build secure software?
- People don't (seem to) care. Security is bothering and makes using computers more cumbersome.
- Writing secure software needs educated programmers – are they?
- Trusted Computing promises to help by breaking the cycle – by doing things differently. Does it help?

Vulnerabilities are long known



Pre-History

- Multics System in late 1960s.
  - Trusted path, isolation.
- Paper on Digital Distributed System Security Architecture by Gasser, Goldstein, Kauffman, and Lampson.
  - Described early need for remote attestation and how accomplished.
- 1970 DoD task force (http://seclab.cs.ucdavis.edu/projects/history/papers/ware70.pdf)
  - Focused on main frames with timesharing
- Main Recommendation:
  - ***User isolation***
    - each user program must be isolated from every other user program
  - ***Supervisor protection***
    - The supervisor must have protection from every user program. create user mode and supervisor mode
  - ***Assurance against unanticipated conditions***
    - Handle unexpected events in a well defined manner
  - ***Language processors and utilities***
    - High level languages should use
    - libraries of evaluated utility routines
  - ***Supervisor program***
    - Run as much of the supervisor as you can in user mode. Clean up after sensitive data is in use. Orderly startup and shutdown. Certified ability to control access to files
- Bell-La Padula

Identified research requirements for trusted computers

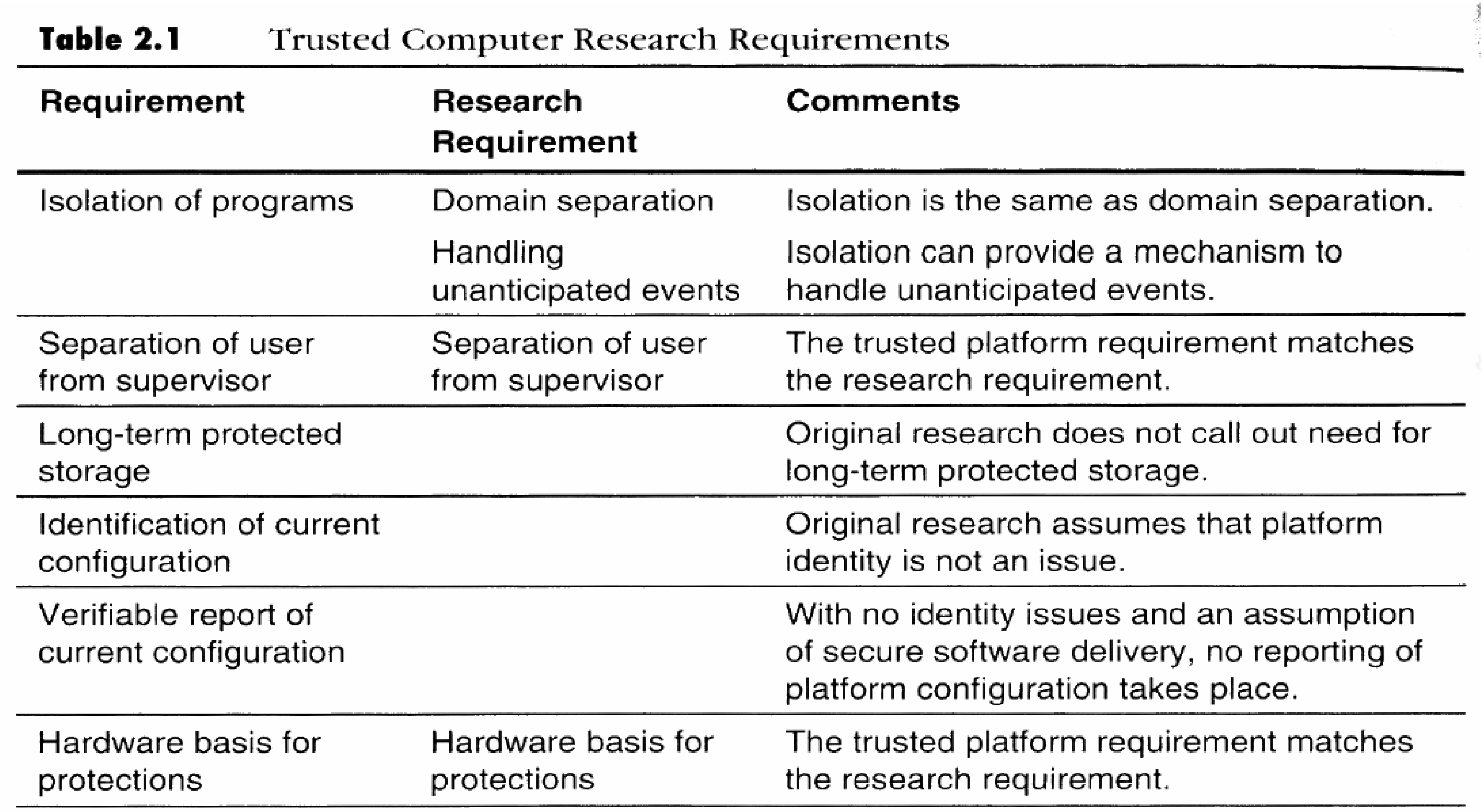


Table 2.1 Trusted Computer Research Requirements

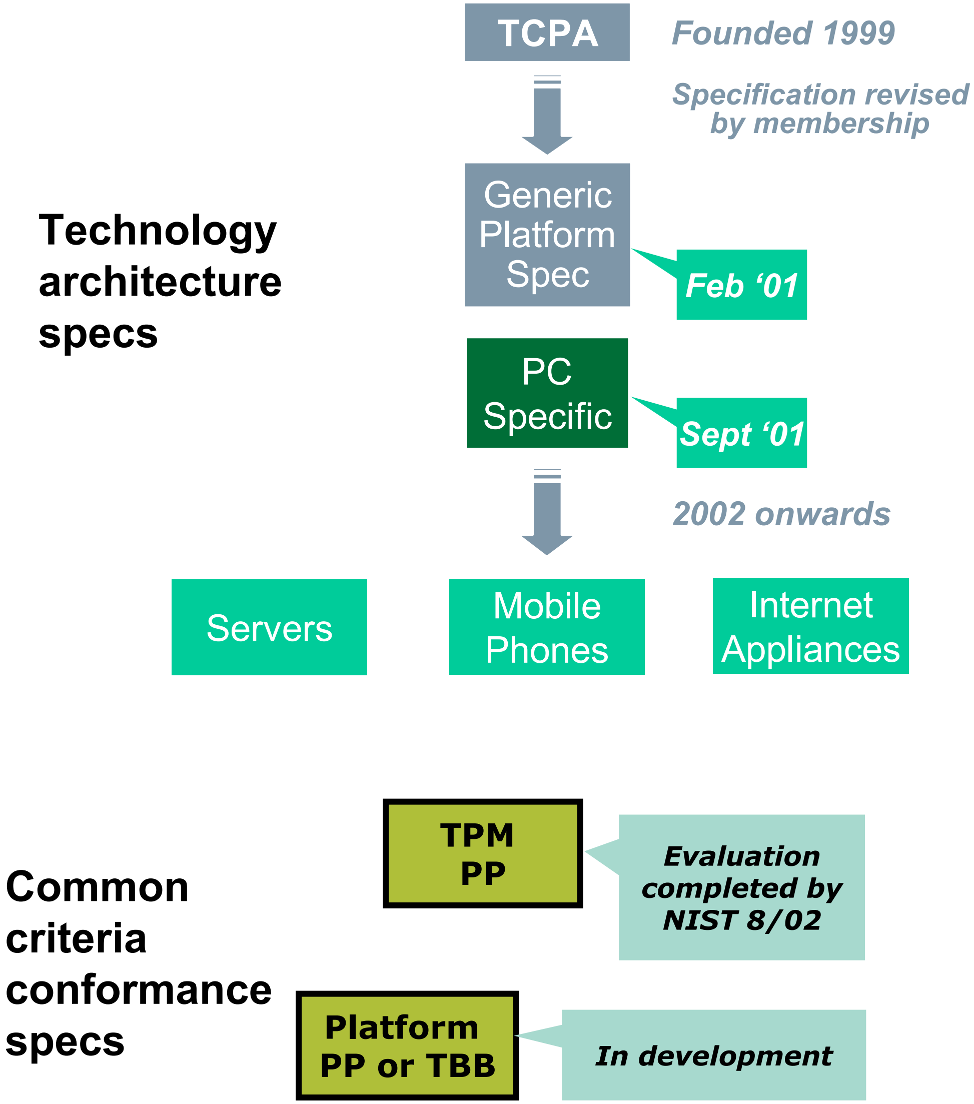
Requirement	Research Requirement	Comments
Isolation of programs	Domain separation	Isolation is the same as domain separation.
	Handling unanticipated events	Isolation can provide a mechanism to handle unanticipated events.
Separation of user from supervisor	Separation of user from supervisor	The trusted platform requirement matches the research requirement.
Long-term protected storage		Original research does not call out need for long-term protected storage.
Identification of current configuration		Original research assumes that platform identity is not an issue.
Verifiable report of current configuration		With no identity issues and an assumption of secure software delivery, no reporting of platform configuration takes place.
Hardware basis for protections	Hardware basis for protections	The trusted platform requirement matches the research requirement.

History: TCPA

- Established in spring 1999
- Promoters were:
  - Compaq, IBM, Intel, HP and Microsoft
- Membership peaked with over 170 companies
- Aim: Reduce business risks by enabling trust in the behavior of critical information systems
- Mission: **To maintain the privacy of the platform owner while providing a ubiquitous interoperable mechanism to validate the identity and integrity of a computing platform**
- Process came to a standstill due to statutes' mandating unanimous decisions
- Reformed to TCG in 2003

TCPA specification activities

Everything beyond 2002 went into TCG



Technology architecture specs

TCPA

Founded 1999

Specification revised by membership

Generic Platform Spec

Feb '01

PC Specific

Sept '01

2002 onwards

Servers

Mobile Phones

Internet Appliances

Common criteria conformance specs

TPM PP

Evaluation completed by NIST 8/02

Platform PP or TBB

In development

Public critique

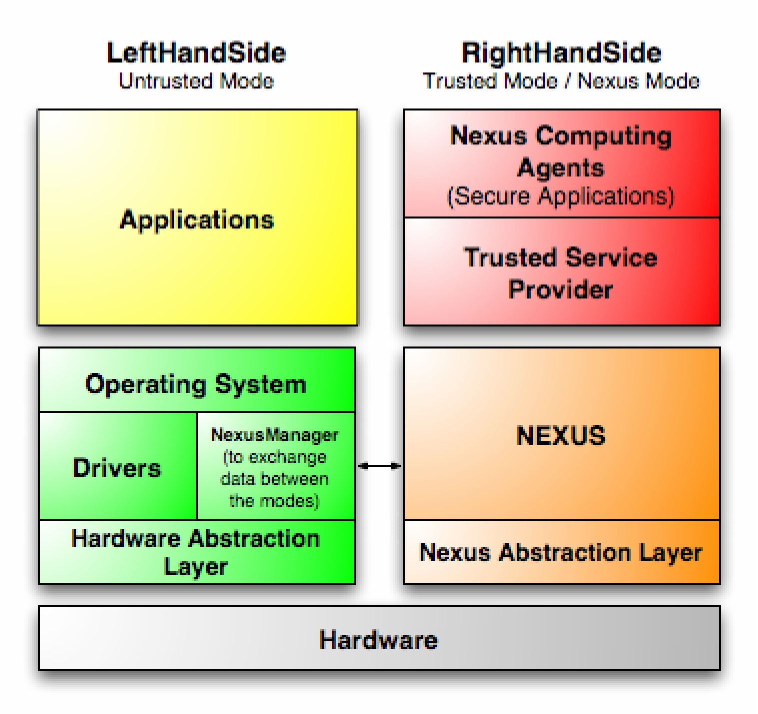
- Prominent exponents: Ross Anderson, Richard Stallman, Lucky Green, Bill Arbaugh, EFF, …
- From DEFCON 10 talk of Lucky Green: Main uses of TC
  - Prevent use of unlicensed software.
  - Digital Rights Management (DRM).
  - Prevent CD ripping and DivX creation.
  - Plug “analog hole.”
  - Enable information flow control.
  - Make PC the core of the home entertainment center, growing overall market.
  - Meet operational needs of law enforcement and intelligence services (FBI, Homeland, NSA, non-U.S. law enforcement).
- Technical objective: Prevent the owner of a computer from obtaining root access.
  - Enforce three levels of access privileges:
    - Privileged access[TCPA members only].
    - Underprivileged access [platform owner].
    - Unprivileged access [non-TCPA applications].
- To succeed where previous efforts have failed:
  - Processor ID (Intel, 1995-1998).
  - Encrypted CPU instruction sets (Intel, 1995-TCPA Phase II).
  - International Cryptography Framework (HP, 1996).
  - Smartcards on motherboard (IBM, ~2003).
- The legal lever: **DMCA**

Some links for the discussion

- https://www.cypherpunks.to/TCPA_DEFCON_10.pdf
- http://www.newsforge.com/business/02/10/21/1449250.shtml?tid=19
- http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html
- http://www.wowarea.com/dyn/vae.php/k_20051030204950
- http://researchweb.watson.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf
- http://www.againsttcpa.com/index.shtml (outdated)
- http://www.lafkon.net/tc/
- http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/TrustedComputingConcepts.html

A glimpse at MS‘ NGSCB

- Formerly known as Palladium
- A mechanism for introducing TC in parallel with present-day open systems.
- Two modes run in parallel:
  the trusted mode and the untrusted mode.
- The trusted mode will be the locked-down one.
  The owner need not use the trusted mode,
  but it will be necessary to do so in order to
  access certain kinds of content,
  such as emails and documents whose authors have
  imposed TC restrictions, and TC-managed media file
  It will not be possible to export files from the
  trusted mode to the untrusted mode.



- Not much less in Vista (kernel mode security), see http://www.symantec.com/avcenter/reference/Windows_Vista_Kernel_Mode_Security.pdf :
  - BitLocker – the not too secure TPM-based disk encryption
  - PatchGuard
  - Driver signing
  - Kernel-mode code integrity checks to ensure kernel integrity at runtime – not hardware-based, perhaps not safe
  - Optional support for Secure Bootup using a TPM – up to OS loader
  - Restricted user-mode access to \Device\PhysicalMemory

The TCG

- Formed 2003, now ~200 organisations, among them Fraunhofer SIT as academic liaison member
- Not-for-profit organization,
  - formed to develop, define and promote open, vendor-independent specifications for trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals and devices
  - Efforts to ensure compliance and conformance of TPMs and trusted hardware
- www.trustedcomputinggroup.org
- And by the way: DRM is not on the agenda!

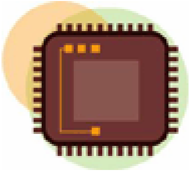
TRUSTED COMPUTING GROUP™

Working Groups

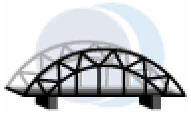
- Mobile
  - provides trust for mobile devices including mobile phones and PDAs

- PC Client
  - provides common functionality, interfaces and a set of security and privacy requirements for PC clients that use TCG components to establish their root of trust

- Trusted Platform Module
  - created the Trusted Platform Module (TPM) specification, version 1.1b and 1.2. The TPM is the root of trust that is the basis of the work of the other TCG work groups.



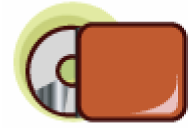
- Infrastructure
  - defines architectural framework, interfaces and metadata necessary to bridge infrastructure gaps



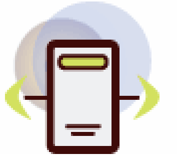
Working Groups

- Hard Copy
  - defining open, vendor-neutral specifications for hardcopy devices that will use TCG components to establish their root of trust.

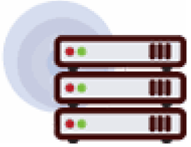
- Software Stack
  - provides a standard set of APIs for application vendors who wish to make use of the TPM.



- Server
  - provides definitions, specifications, guidelines and technical requirements as they pertain to the implementation of TCG technology in servers.



- Storage
  - is building upon existing TCG technologies and focusing on standards for security services on dedicated storage systems.



- Trusted Network Connect
  - focuses on ensuring endpoint compliance with integrity policies at and after network connection.

More Activities

- Conformance and Compliance Activities
- User authentication is an issue
- Details and other subjects are TCG-internal yet

- TPM adoption by hardware vendors, see
  http://www.tonymcfadden.net/tpmvendors_arc.html

TCG Design Principles 1/4

- Security: „TCG-enabled components should achieve controlled access to designated critical protection of secured data and should reliably measure and report a system’s security properties. The reporting mechanism should be fully under the platform owner’s control.”
- Privacy: „TCG-enabled components should be designed and implemented with privacy in mind and adhere to the letter and spirit of all relevant guidelines, laws, and regulations. This includes, but is not limited to, the OECD Guidelines, the Fair Information Practices, and the European Union Data Protection Directive (95/46/EC).” Comprises:
  - Notice: Explicit notice of the collection and retention of personal data should be provided.
  - Choice: Owners should have effective choice and control over the transfer of personal information
  - Purpose Limitation: Personal information collected for one purpose should not be used for another.
  - Control: Private information about the owner should be under the platform owner's control. Private information about the user should be under the user's control.
  - Data Quality: Any stored information should be disposed of in a timely fashion any personal information supplied as a result of TCG-enabled technology should be up-to-date.
  - Access: there must be a way for the individual to review and correct stored data as needed.
  - Proportionality: Personal data collected and transferred must be both relevant and not excessive with respect to the purposes for which it is collected. Private keys should never be disclosed.

TCG Design Principles 2/4

- Interoperability: „Implementations and deployments of TCG specifications should facilitate interoperability. Furthermore, implementations and deployments of TCG specifications should not introduce interoperability obstacles.“
- Portability of Data: „Deployment should support established principles and practices of data ownership.“
  - A catch: User data can be protected (encryption) by the TPM. Two types of hardware assisted protection:
    - Protected storage: Encryption keys (and data protected using these keys) are under control enforced by a TPM
    - Sealed storage: Additional requirement: protected information can only be revealed, if the platform is in a particular software state
    - Problem: Without appropriate safeguards, portability of the data is in danger
  - Migratable keys can be backed up or moved to a different platform (with a different TPM) makes recovery possible
  - Balance of portability with security!

TCG Design Principles 3/4

- Portability of data (ctd.): “Any application that uses TCG technology to bind data to the platform or application should either:
  - a)provide a means to export that data from the TCG security envelope, or
    b)provide appropriate, effective, and timely notice to anyone with a reasonable expectation of access to that data of the absence of data export and the consequences of such an absence.
  - TPM-protected keys should be designated as “nonmigratable” only where there is a clear security requirement for nonmigratability. While for security reasons, nonmigratable data is never migratable (except during data recovery), migratable data should always be accessible to the authorized user.”

TCG Design Principles 4/4

- Controllability: „Each owner should have effective choice and control over the use and operation of the TCG-enabled capabilities that belong to them; their participation must be opt-in. Subsequently any user can reliablydisable the TCG functionality in a way that does not violate the owner's policy."
  - Nobody should be forced to use TCG technology, i.e., no *all or nothing* principle – use what you need
  - Split ownership may complicate this issue – some mandatory functions, some optional
  - Particular principles:
    - Appropriate notice to the user of the entity requiring the security policy.
    - Entity should provide explanation for those aspects of the owners policy that may affect the user (especially e.g. with public-access terminals)
  - TCG-enabled capabilities are opt-in. At any time, a nontechnical user should be able to easily determine the operational state of the TCG-enabled capabilities.
  - Fine grained control of transactions as appropriate per application.
- Ease-of-Use: "The nontechnical user should find the TCG-enabled capabilities comprehensible and usable."
  - Ease of use and security are often viewed as conflicting goals. Some concepts we show later in the lectures indicate the contrary.

Security

- Computer Security
  - Techniques for computing in the presence of adversaries
- Three categories of security goals
  - Confidentiality: preventing unauthorized release of info
  - Integrity: preventing unauthorized modification of info
  - Availability: preventing denial of service attacks
- Protection is about providing all three on a single machine
- Usually considered the responsibility of the OS
- Could also be runtime (e.g., verification in JVM)
- Cryptography
  - Techniques for communicating in the presence of adversaries

Trusted Computing Base (TCB)

- Trusted Computing Base (TCB)
  - Think carefully about what you trust with your data
  - If you type your password on a keyboard, you’re trusting
    - The keyboard manufacturer
    - Your computer manufacturer
    - Your OS
    - The password library
    - The application that is checking the password
    - Your service provider
    - Your bank
  - TCB = set of components (hardware, software, ***people***) that
  - you trust your secrets with
  - Public Web kiosks should not be in your TCB
  - Should your OS? (Think about IE and ActiveX)

Trust involves multiple components

- UNIX program called “login” authenticates users
  - Users enter their account name, password
  - Program checks password against password database (hash values not clear text)
- What could go wrong?
- Why would administrator trust login program?
  - Inspect source code, verify what it does
  - I.e., no ‘backdoors’ that allowed unexpected access
- Is the program safe?
- NO. Trusted computing base includes compiler
  - someone put backdoor in original UNIX login
  - Hacked the C compiler to hide his tracks

Cryptography can bridge TCBs

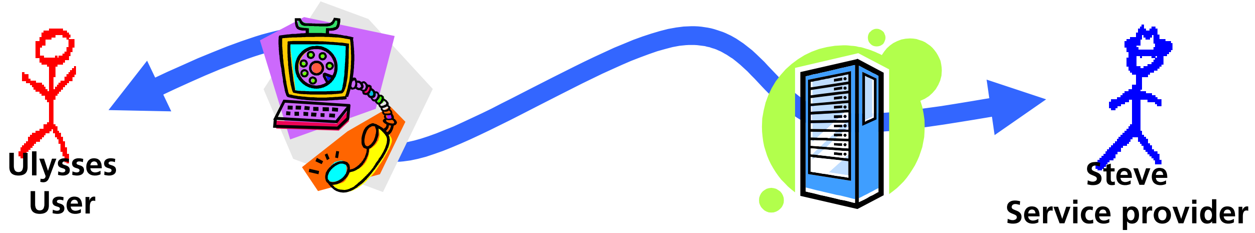
- Enables communication between trusted parties
- Even (especially) in the face of untrusted eavesdroppers
- Allows systems to expand their trusted computing base
- Three main goals:
  - Authentication: verify the identity of the communicating party
    - Distinct from authorization (e.g., ACLs, capabilities)
  - ntegrity: verify the message arrives as sender intended
  - Confidentiality: only recipient can read message
    - This is NOT the same as integrity; can have one without the other.
- Implemented with a wide family of mechanisms
- Rely on some form of "key" or secret; some shared, some not

Trust

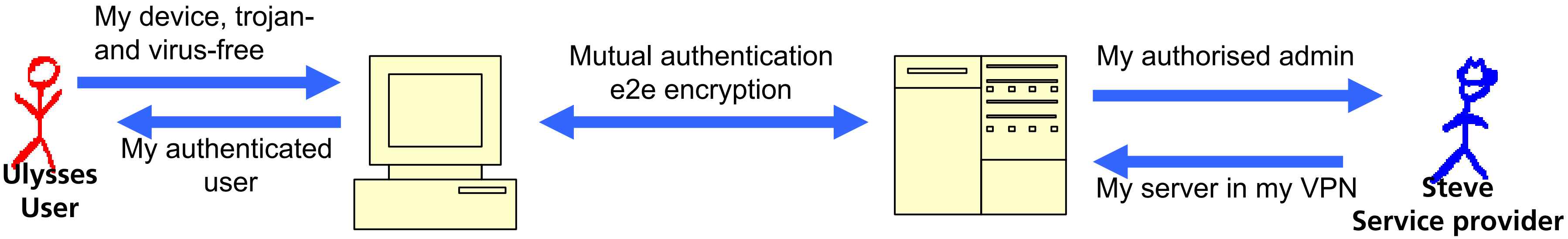
- But what is needed to establish trust?
  - A TCB
  - A trusted platform
  - A trust anchor
  - Means to convey trust

Trust is chained (more often than not)

- How do partners put trust in each other in application scenarios?
- Through technical systems!



- Those need to be trusted as well
- Chains of trust become increasingly long and complex



Transitive trust:
Attest a systems trustworthiness to a third party over multiple hops

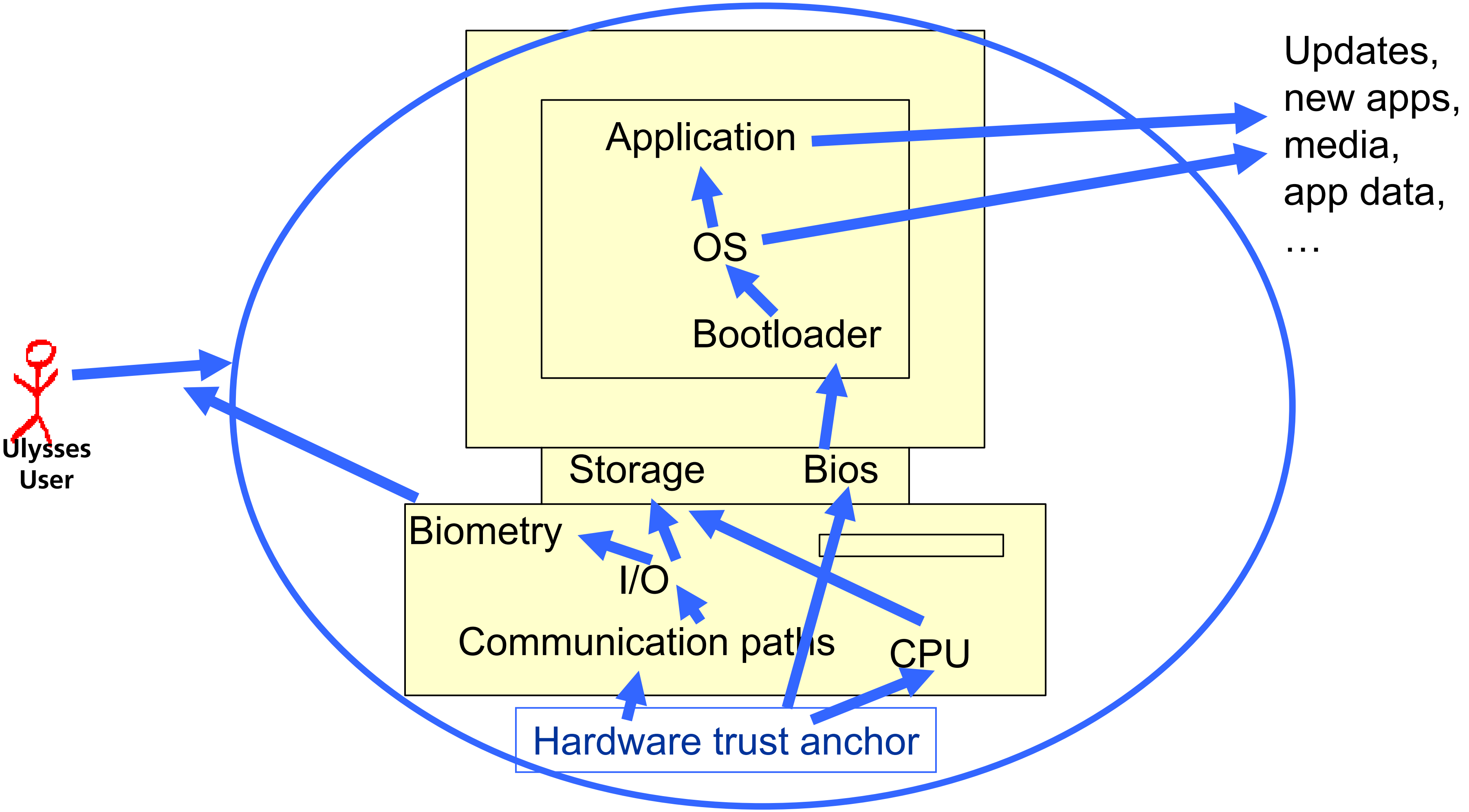
Attestation:
Provide authentic information about a system‘s state to a verifier

Attestation Definition

- American Heritage Dictionary says:
  - "To affirm to be true, correct or genuine"
- For trusted platforms:
  - Cryptographic proof of information regarding the platform
- Information that could be attested to includes:
  - HW on platform
  - BIOS
  - Configuration options
  - And much more

Trusting an open system

- Many components are involved in trust chains in complex, open systems



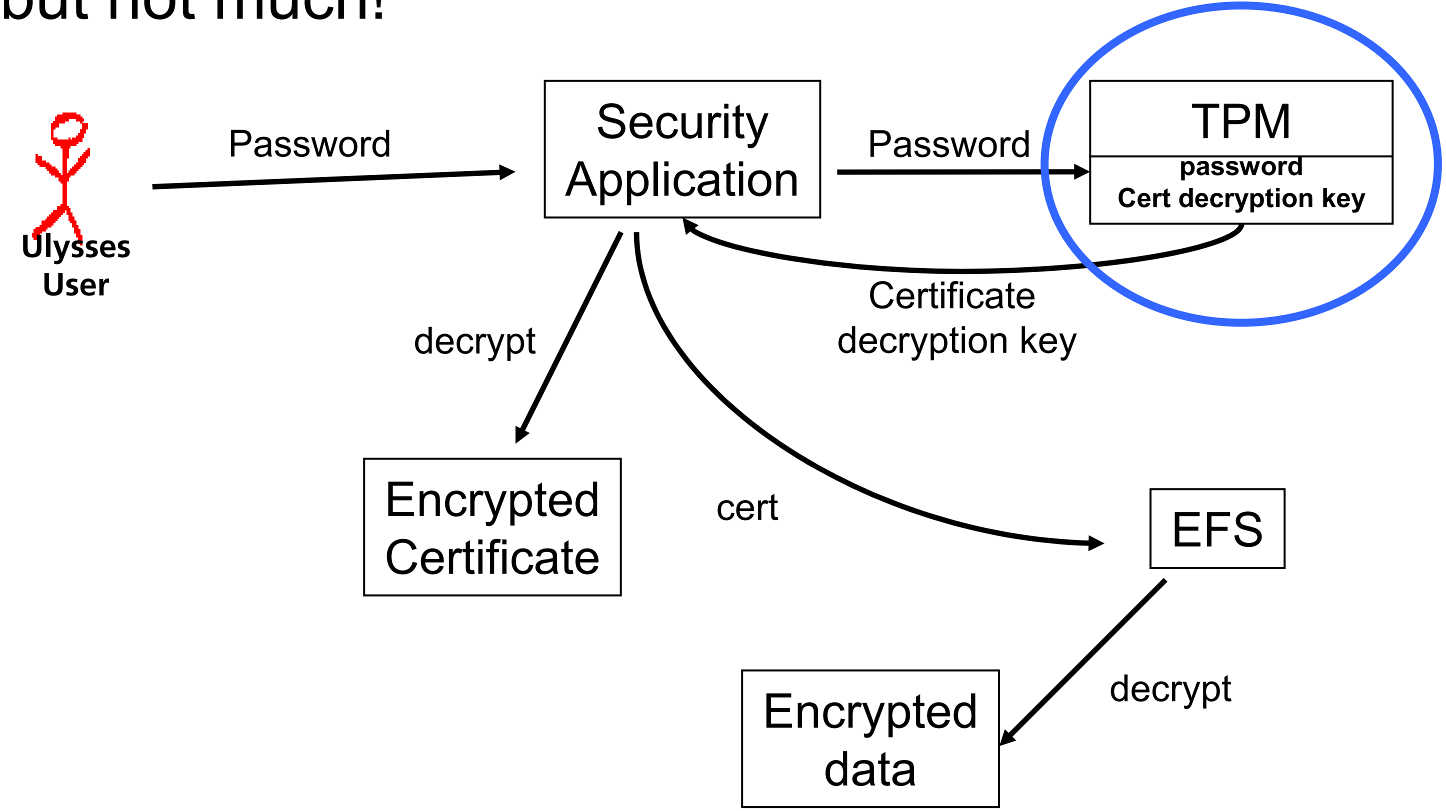
TCG‘s pragmatic definition and assigned task

- Trust
  - An entity can be trusted if it always behaves in the expected manner for the intended purpose

- Trusted Computing
  - Basically a reporting technology to testify the state of a certain system to and optionally its identity to an external verifier

Example: TPM-based disk encryption (present)

- A bit safer (better than BitLocker at least), but not much!



- Many present applications of TC are rudiments, since TPs are not established, TCBs not built

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
  - No, today open implementations of TC functionality exist – L4 Linux, Xen, Trusted Grub, TrouSerS, …
- TCG, Palladium/NGSCB, and DRM are all the same
  - No, the TPM and TCG are 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

My 2 cents on TC

- Many bad uses of TC exist: DRM, blocking free software, impair end-user interests, enforcement of rip-off deals, …
- They become a real danger only through bad legislation like the DMCA (and European/German counterparts) which criminalise customers
- Legal countermeasures exist: Competition Protection and Monopoly law
- In the end all unwanted (commercial) usages of TC are deliberate market distortions!

New threats

- Crime, terrorism spark overreactions
- Will TC be used to enable online-searching of users‘ devices?
- Or prevent it?
- History: Cryptography (export) bans have proven ineffective, since the technology became openly available
- Conclusion: I‘d rather like to see TC open, standardised and widely available from multiple vendors, internationally

New businesses from TC

- New usages of TC may look like the old bad uses, technically
- But can be designed to include fair value propositions to customers
- TC enables new business models
- Golden rule:
  - Offer fair deals and abide by the law
  - Participate, if law gets ugly