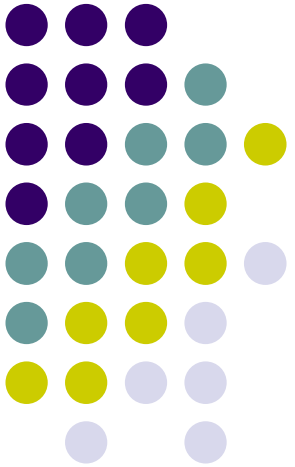
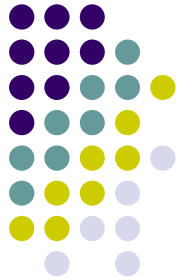
Trusted Computing, Trusted Platform Module

PA018
Vašek Matyáš



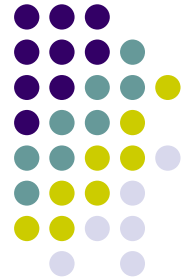
First 20 slides courtesy of Dieter Gollmann

History



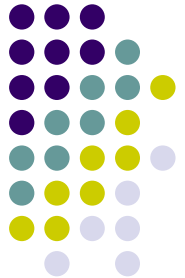
- The term “trusted” computing has been used for a long time in computer security.
- Trusted Computing Base (TCB) defined in the Orange Book (TCSEC,1985).
- Orange Book evaluation classes for higher assurance levels (B1 – B3, A1) require support for label-based multi-level security (MLS).

TCB (1985)



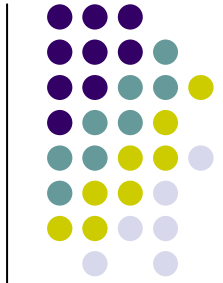
The totality of protection mechanisms within a computer system - including hardware, firmware, and software - the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of the TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

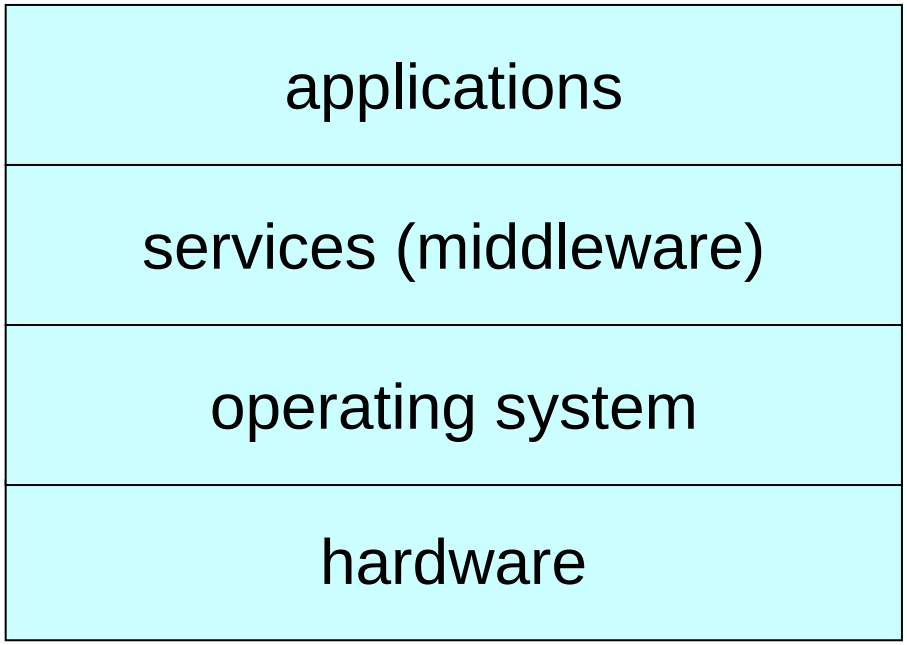
Trusted Computing



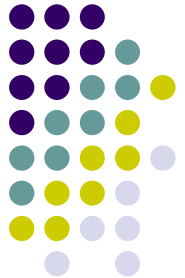
- Every security relevant component is part of the TCB!
- A component is trusted if it can hurt you!
- Distinguish “trusted” from “trustworthy” systems.
- Orange Book: High assurance systems had to support multi-level security.
- “Trusted Unix”, “Trusted Solaris”, “Trusted Oracle”, etc. are products supporting MLS.

Placing security controls





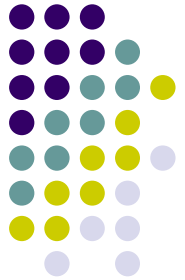
Hardware/Software Co-Design



- Advantage of placing controls at the hardware layer:
  - Performance: Efficient support for frequent O/S operations
  - Assurance: More difficult to circumvent than controls at higher layers
- Incentive for hardware designers to adapt microprocessors to typical use by O/S.
- Incentive for O/S writers to use features provided by microprocessors.

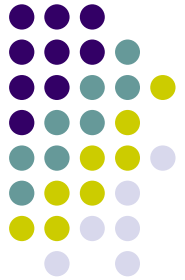
- Remark (Bill Caelli): Some of the security features of the Intel 80286 processor were dropped from the 80386 because they were not used by MS-DOS.

TCPA (1999)



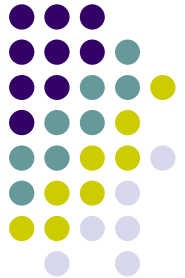
- Trusted Computing Platform Alliance (TCPA)
- Founder members: Compaq, Hewlett-Packard, IBM, Intel, Microsoft
- Goal: Make the Web safer for surfers, using open-source hardware and software.
- 200 members by April 2003, then disbanded and reformed as the Trusted Computing Group (TCG), retaining the TCPA documents and specifications.

TCG (2003)



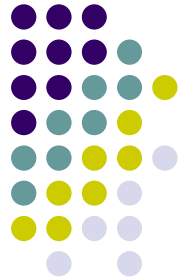
- Trusted Computing Group
- Not-for-profit industry-standards organization aiming to enhancing the security of the computing environment in disparate computer platforms.
- Formed in Spring 2003.
- Carries on from work in the TCPA.
- Puts “roots of trust” into computer platforms.
- https://www.trustedcomputinggroup.org/home

Roots of Trust



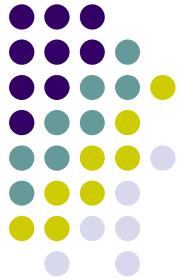
- Root of Trust: "A component that must always behave in the expected manner, because its misbehavior cannot be detected."
  - I.e., a trusted component in the traditional sense.
- "The complete set of Roots of Trust has at least the minimum set of functions to enable a description of the platform characteristics that affect the trustworthiness of the platform."
  - Leap from trusted components to trustworthiness of platforms.

Roots of Trust



- Root of Trust for Measurement (RTM): "A computing engine capable of making inherently reliable integrity measurements."
  - Despite the grandiose name, this is essentially just an implementation of a hash function.
- "This is the root of the chain of transitive trust."
  - Marketing jargon for: To make a statement about the state of the system, you first have to check that essential programs and tables have not been tampered with.

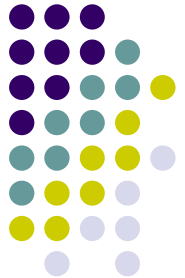
Integrity Measurements



- "Integrity measurement is the process of obtaining metrics of platform characteristics that affect the integrity (trustworthiness) of a platform,
  - Marketing jargon for: Compute hash (digest) of security critical resources.

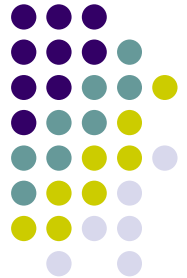
  storing those metrics, and putting digests of those metrics in Platform Configuration Registers (PCRs)."
  - Marketing jargon for: Store those hash values in protected registers.

Roots of Trust



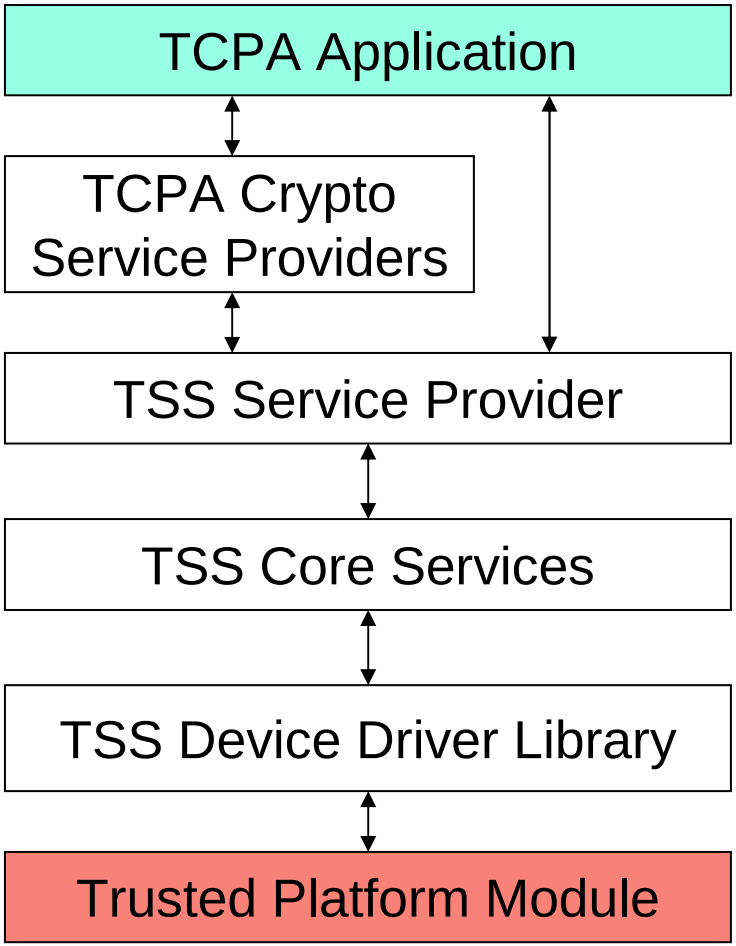
- Root of Trust for Storage (RTS): Computing engine capable of maintaining an accurate summary of values of integrity digests and the sequence of digests.
  - Useful component for implementing secure boot.
- Root of Trust for Reporting (RTR): Computing engine capable of reliably reporting information held by the RTS.
  - On a TPM, the RTR is the endorsement key.

Trusted Computing Platforms

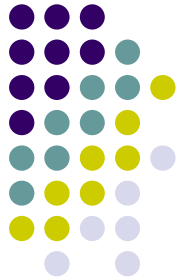


- “Trustworthy” TCB for a PC.
- Note how the meaning of “trusted” has changed in the past two decades.
- Different goals a TCP might support:
  - Process isolation: Classic goal of O/S security, stop processes from interfering with other processes.
  - Attestation: Prove to some other device which software you are running.
  - Sticky policies: Policies that stick to data and cannot be removed by users, e.g. by copying a file.

TCG Software Stack (TSS)



Trusted Platform Modules

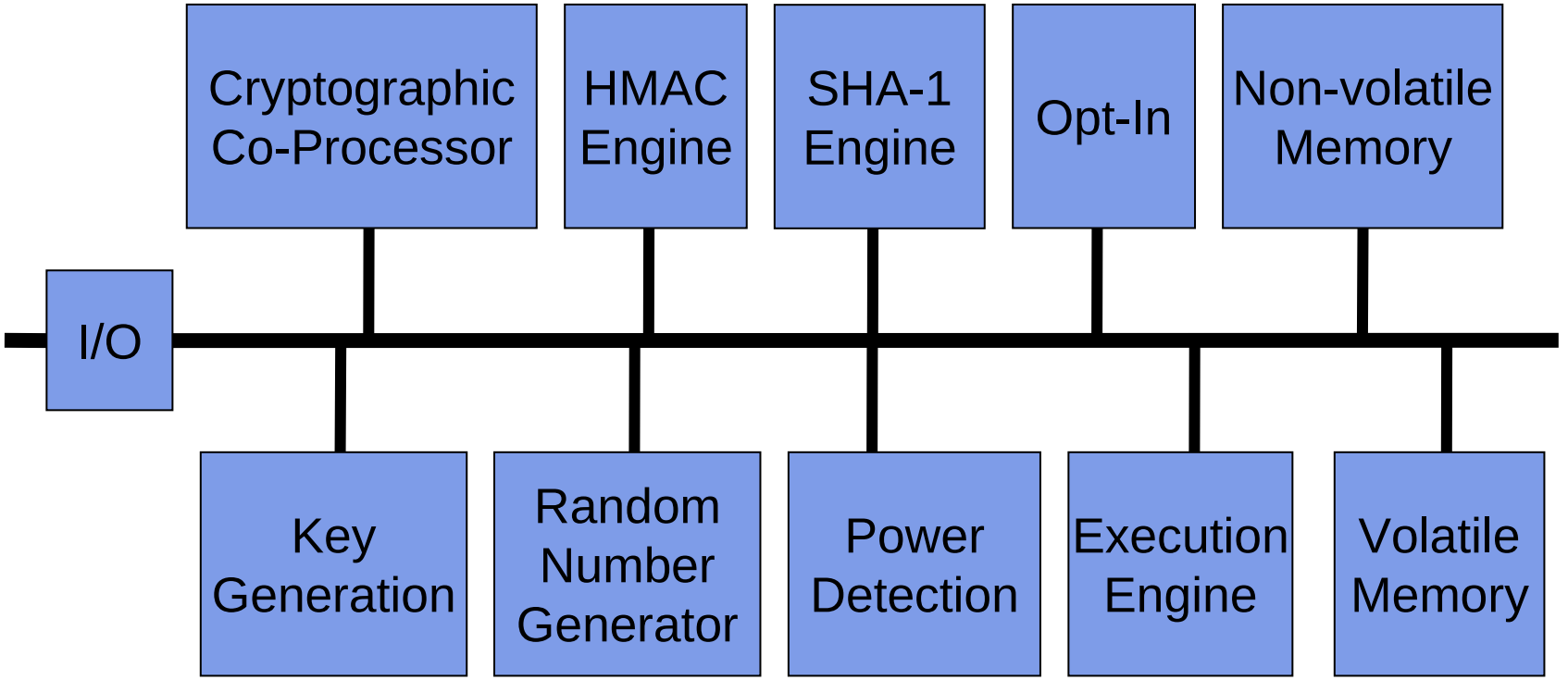


- “The TPM can be thought of as a smart card that is embedded on the system board and acts as a smart card for the machine.”

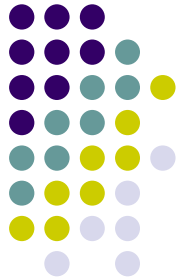
  [“Securing network-based client computing”, Dell white paper 12/2004]

- Smart card = IC on a plastic card
- TPM = smart card without the plastic !?
- TPM = security coprocessor.

Trusted Platform Module

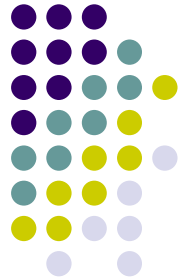


Product: Infineon TPM



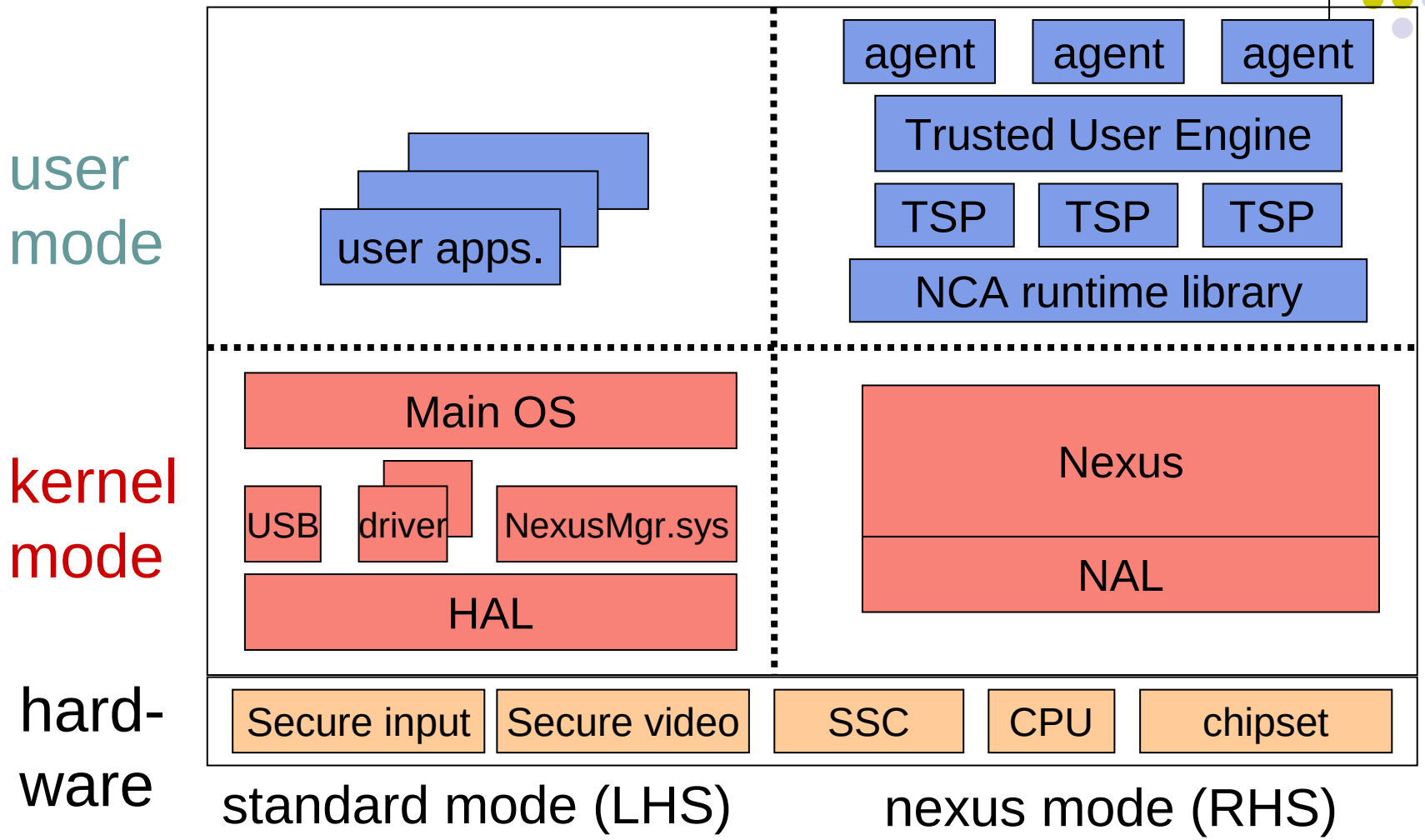
- Secure Controller
- Protected Storage (EEPROM)
- Asymmetric Key Generation (RSA, up to 2048-bit keys)
- Hardware-RSA-Accelerator
- Hardware Hash Accelerator (SHA-1, MD-5)
- True Random Number Generator
- Low Pin Count (LPC) Interface
- Embedded Secure Operating System
- TCG Software Stack (TSS) compliant to spec. 1.1b
- TPM Cryptographic Service Provider (CSP)
- Based on the TCG Main Specification version 1.1b

NGSCB – Palladium (MS)

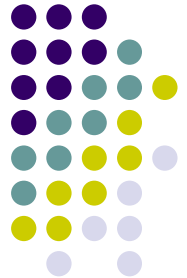


- Next Generation Secure Computing Base.
- Design constraint: Do not break existing Windows applications.
- First proposal: Left-hand-side – right-hand-side design:
  - LHS: Windows and Windows applications (unchanged).
  - RHS: Nexus operating system provides trusted services.
- Status in 2004: In the long term vision, the Nexus is somewhat akin to a hypervisor.

NGSCB (Palladium, “old”)

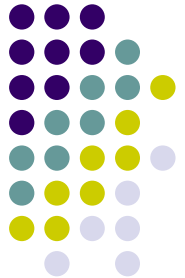


Trusted Computing in Vista



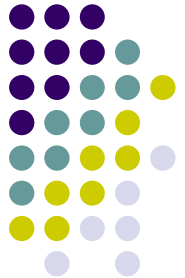
- Secure Startup announced for Vista (Longhorn, April 2005)
- Threat: stolen laptops that contain sensitive business data
  - 591,000 laptops stolen in the U.S. in 2001.
- Countermeasure: Encrypt all data on disk; keep key in TPM; encryption/decryption key derived from system configuration.
- Changes to the BIOS change decryption key.
- No protection once user is active.

Secure Startup



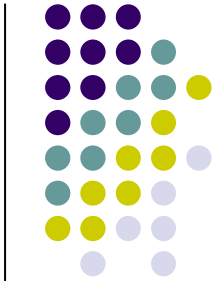
- Encrypts entire Windows partition, including page files, temp files, hibernation files, and crash dump files.
- Protects third-party Windows applications.
- Simplifies PC recycling, speeds up data deletion: Data on encrypted volume rendered useless by deleting the TPM key store.
- *Provisions for key recovery required.*
- Difference to EFS (encrypted file system): EFS encrypts on a per-user basis, keys on hard disk.

Dieter Gollman's Conclusions



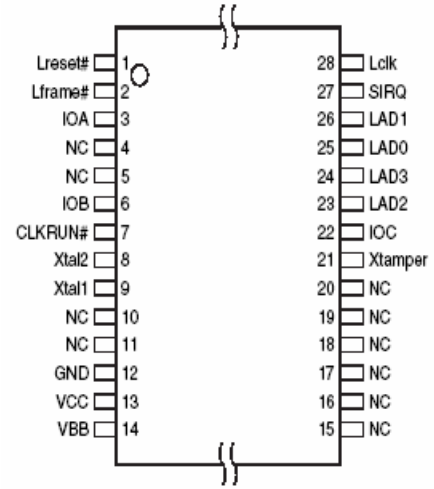
- Evolution: PC as a stand-alone device had lost the ability to defend itself.
- Return to the past:
  - Redeployment of "old" ideas (process isolation, type enforcement).
- Strong (and surprising) emphasis on cryptography, with some novel applications:
  - Attestation: lost its killer application (DRM).
  - Sticky policies.
- Supports applications where policies are not set by the owner of a device but restrict the owner.
- Fertile area of speculation: Some high-level specifications are available (keep changing), but only a few products.

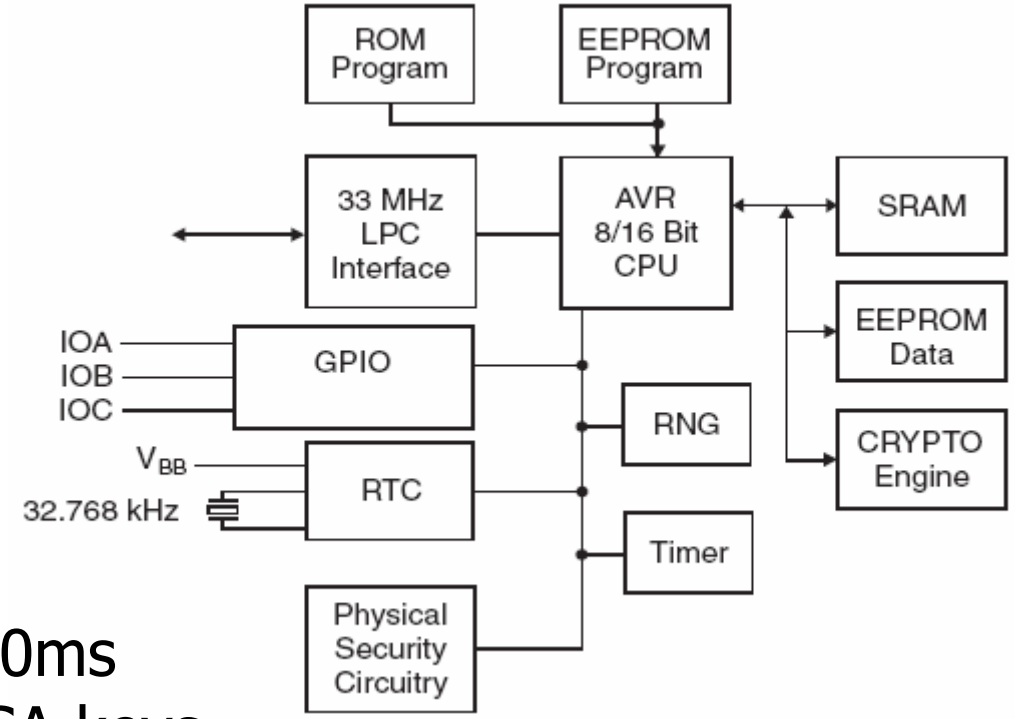
Smarcards vs HSM



		čipové karty		HSM		
0	otevření krytu	>=0	minuty	2,3	hod – měs.	
1	preparace čipu	>=1	hodiny	>=3	dny	
2	rekonstrukce čipu	>=1.5	dny	>=3	měsíce	
3	testování čipu	>=1.5	dny	>=3	týdny – měs	
4	čtení paměti	>=2	dny	>=3	min – týdny	
5	UV záření	>=1.5	dny	>=3	>= týdny	
6	ozáření CMOS tranz.	>=1.5	dny	>=3	>= týdny	
7	mikrovlnné radiace	–	dny	>=3	>= týdny	
8	chybová analýza	>=1.5	dny	>=3	>= dny	
9	výkonová analýza	>=1.5	dny	>=3	>= dny	
10	časové útoky	>=1.5	dny	>=3	>= dny	
11	diferenciální EM anal.	>=1.5	dny	>=3	>= týdny	
12	datové remanence	>=1.5	dny	>=3	>= dny	
13	reverse engineering	>=1	dny/týdny	>=1	měsíce	

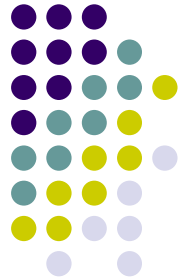
TPM: Atmel AT97SC3201





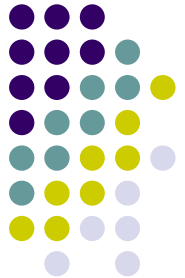
- RSA sign – 2048b in 500ms
- Internal EEPROM for RSA keys
- Design „secure HW and FW“
- Secure clock
- Internal TRNG
- Tamper detection

TCPA – Trusted Computing Platform Alliance



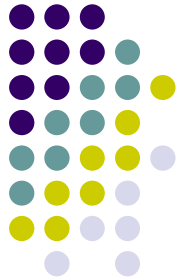
- TPM – specialized or flash
- BIOS
- Software with integrity metrics
- Computer booting procedure:
  - BIOS calls TPM, which verifies in turn BIOS correctness, the the BIOS verifies integrity of the loader and OS kernel

Trusted Platform Module



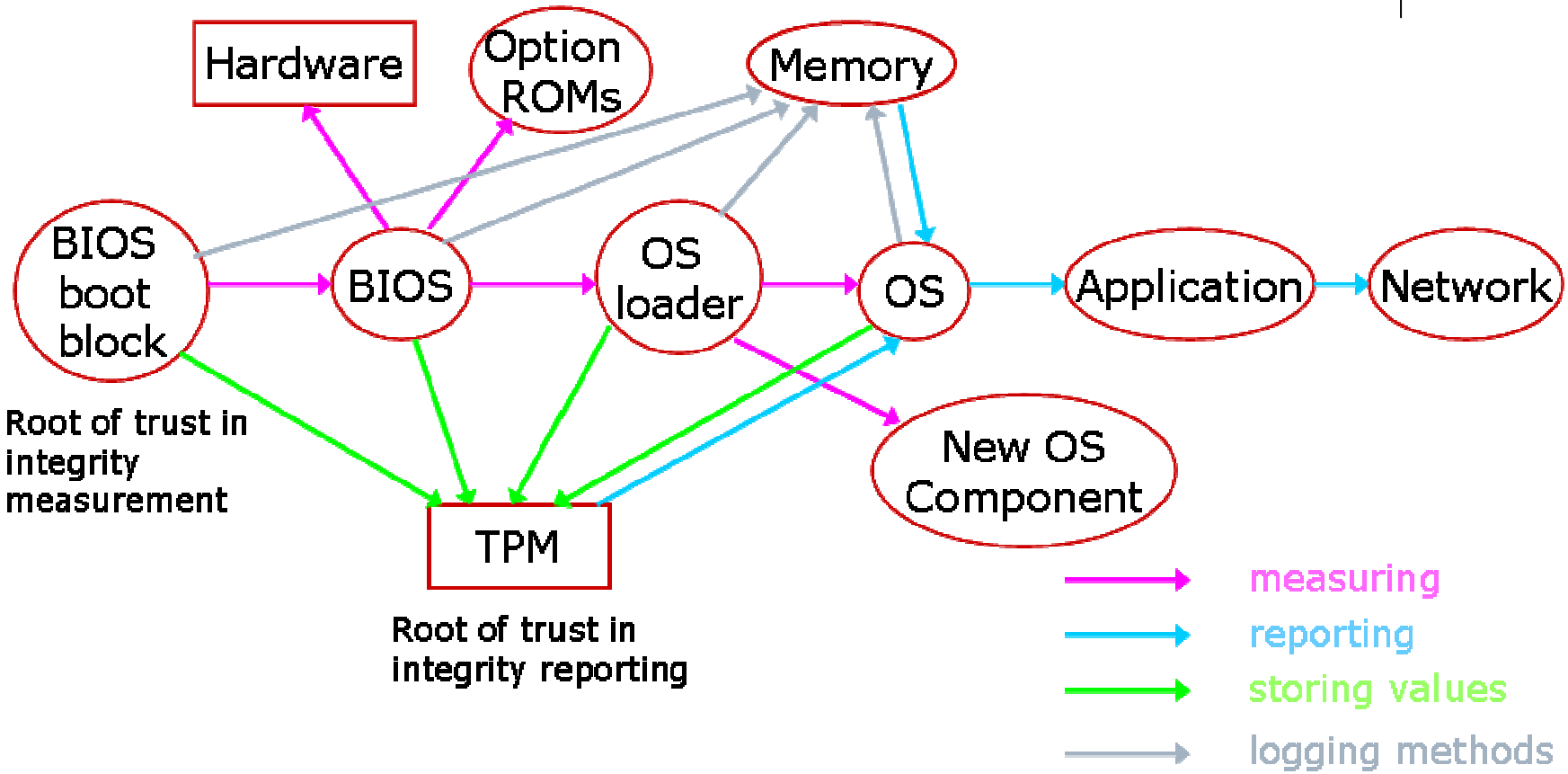
- Specification and manufacturers
- v1.1b, v1.2
  - Wider support of protocols, finer access control, concept of location
  - Atmel, Infineon, Broadcom, Sinosun, STMicroelectronics, Winbond
- Components, API, basic functions
  - Logical structure of TPM
    - RNG, secure memory for keys and data, RSA Engine
  - Basic functions TPM:
    - protected capabilities;
    - integrity measurement;
    - integrity reporting.

TPM cont'd

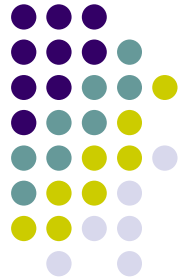


- Parts of TPM:
  - Trust roots – for all functional areas
  - sealed storage, process identification (*CodeID*), trusted paths.
- Applications
  - Data protection (against theft), control of resources,
  - user authentication,
  - virtual cards (soft smartcards),
  - Digital Rights Management (DRM).
- Security risks, enhancements of TPM
  - Flaws discovered (so far)
    - Replay attack against the O*bject-Independent Authorization Protocol*
  - Platform restart counter, work with user smartcards,trusted computed in distributed environments.

Integrity verification



Term project presentations!!!



April 17:

- **Barányi**
- **Benkovský**
- **Červenka**
- **Drašar**
- **Folkman**
- **Gerguri**

April 24:

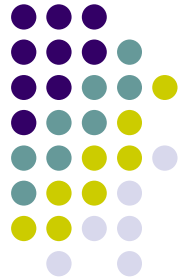
- **Halabica**
- **Henzl**
- **Hubr**
- **Hulán**
- **Kocian**
- **Ondrák**

May 15:

- **Ashurova**
- **Honus**
- **Puškár**
- **Soběslavský**
- **Svoboda**
- **Synak**
- **Štverák**

Reminders: the presentation is worth (up to) 5 points from your course score; it should last at most 15 minutes (time for questions & discussion will be provided); laptop with AcroRead and PowerPoint will be available. ***Rehearse!!!!!***

Course reading – week 4



- Laser-printed PIN Mailer Vulnerability Report
  - Mike Bond, Steven J. Murdoch, and Jolyon Clulow
  - http://www.cl.cam.ac.uk/~mkb23/research/PIN-Mailer.pdf

- Will be used for our discussion next week – think of possible countermeasures!!!