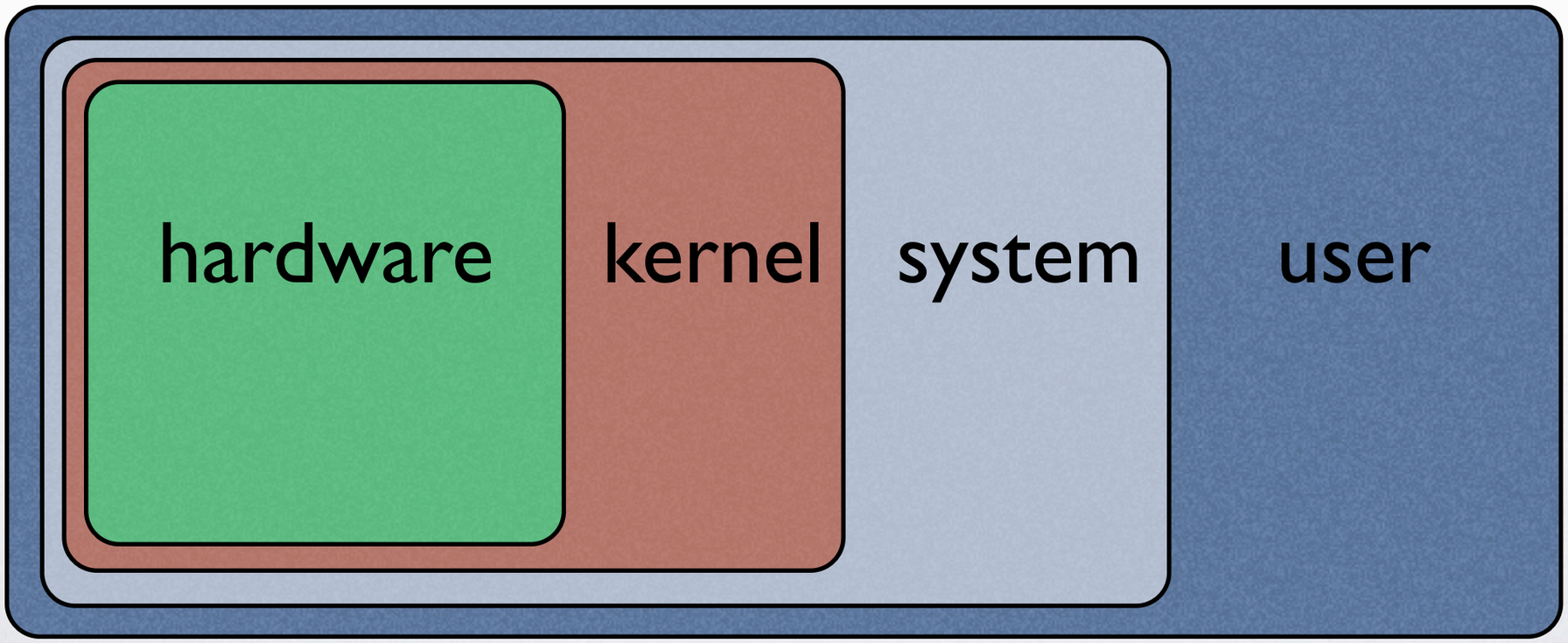



Trusted Computing and O/S Security

Aggelos Kiayias

O/S Security

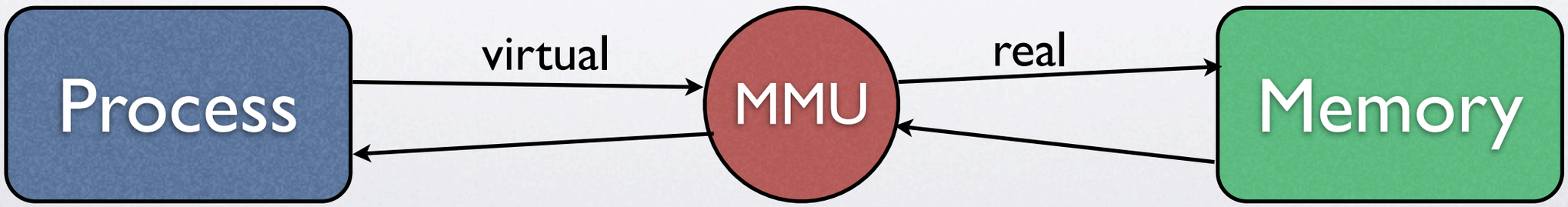
- Fundamental concept for O/S Security: **separation.**



Each layer may try to verify the outer layer

Address Translation

- Run a program in its own "address space"
- Program thinks its running in a continuous memory chunk.
- In fact this chunk is virtual and translated into real memory addresses by a memory management unit.



Protected Mode

- What processes should be capable of writing translation tables, affecting the MMU etc?

- Hardware controlled protected mode operation: full memory access privileges, etc.

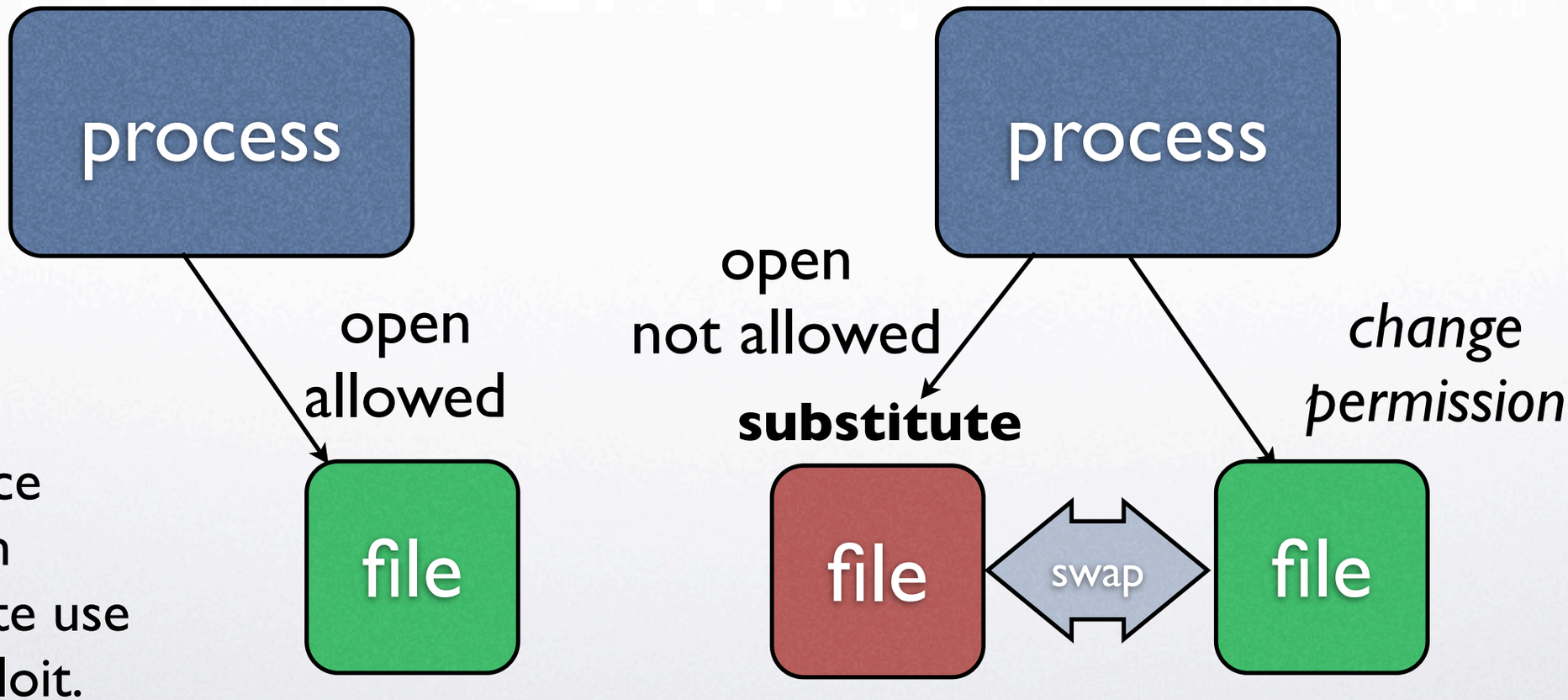
- Kernel may run in non-protected mode, where user applications in protected mode.

CPU-sharing

- Each process needs CPU time in parallel.
- User processes may pass control to Kernel processes and vice-versa.
- What kinds of Kernel functions is a user process allowed to use?
- What arguments is it allowed to pass?

TOCTOU

- Time of check - time of use vulnerabilities.



arms race between legitimate use and exploit.

Example

```
if (access(filename, W_OK) == 0){
 if ((fd = open(filename, O_WRONLY)) == NULL){
 perror(filename);
 return(0);
 }
/* now write to the file */
}
```

Suppose that the above is root uid

access - determine accessibility of a file

SYNOPSIS

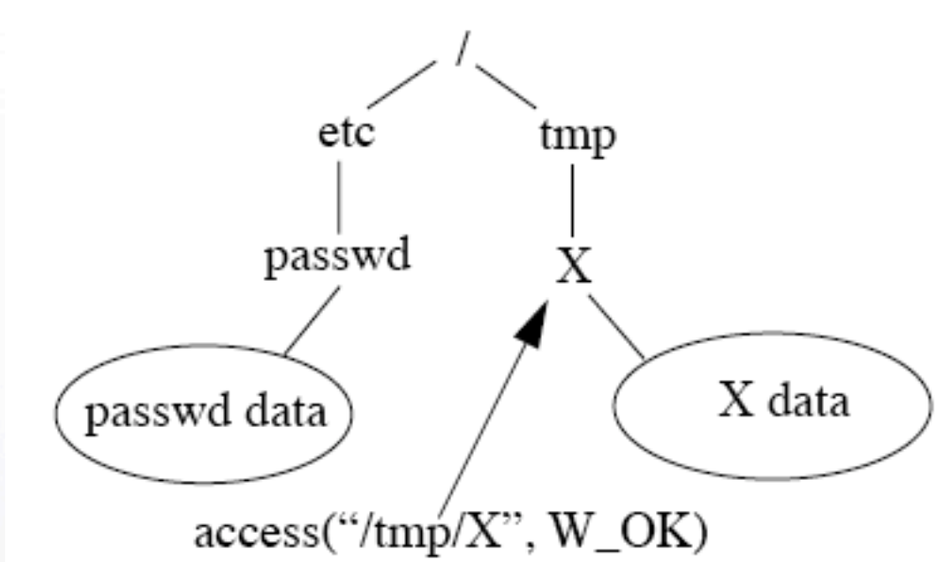
```
#include <unistd.h>

int access(const char *path, int amode);
```

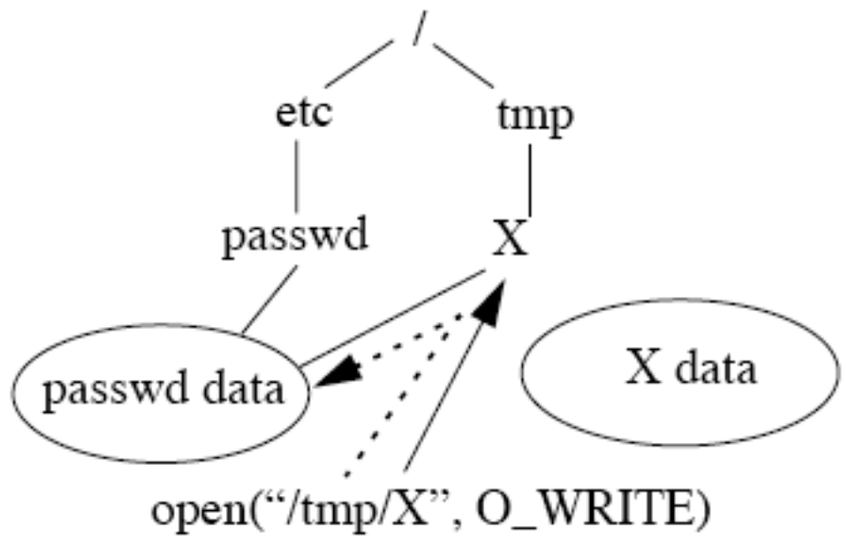
DESCRIPTION

The *access*() function shall check the file named by the pathname pointed to by the *path* argument for accessibility according to the bit pattern contained in *amode*, using the real user ID in place of the effective user ID and the real group ID in place of the effective group ID.

The value of *amode* is either the bitwise-inclusive OR of the access permissions to be checked (R_OK, W_OK, X_OK) or the existence test (F_OK).

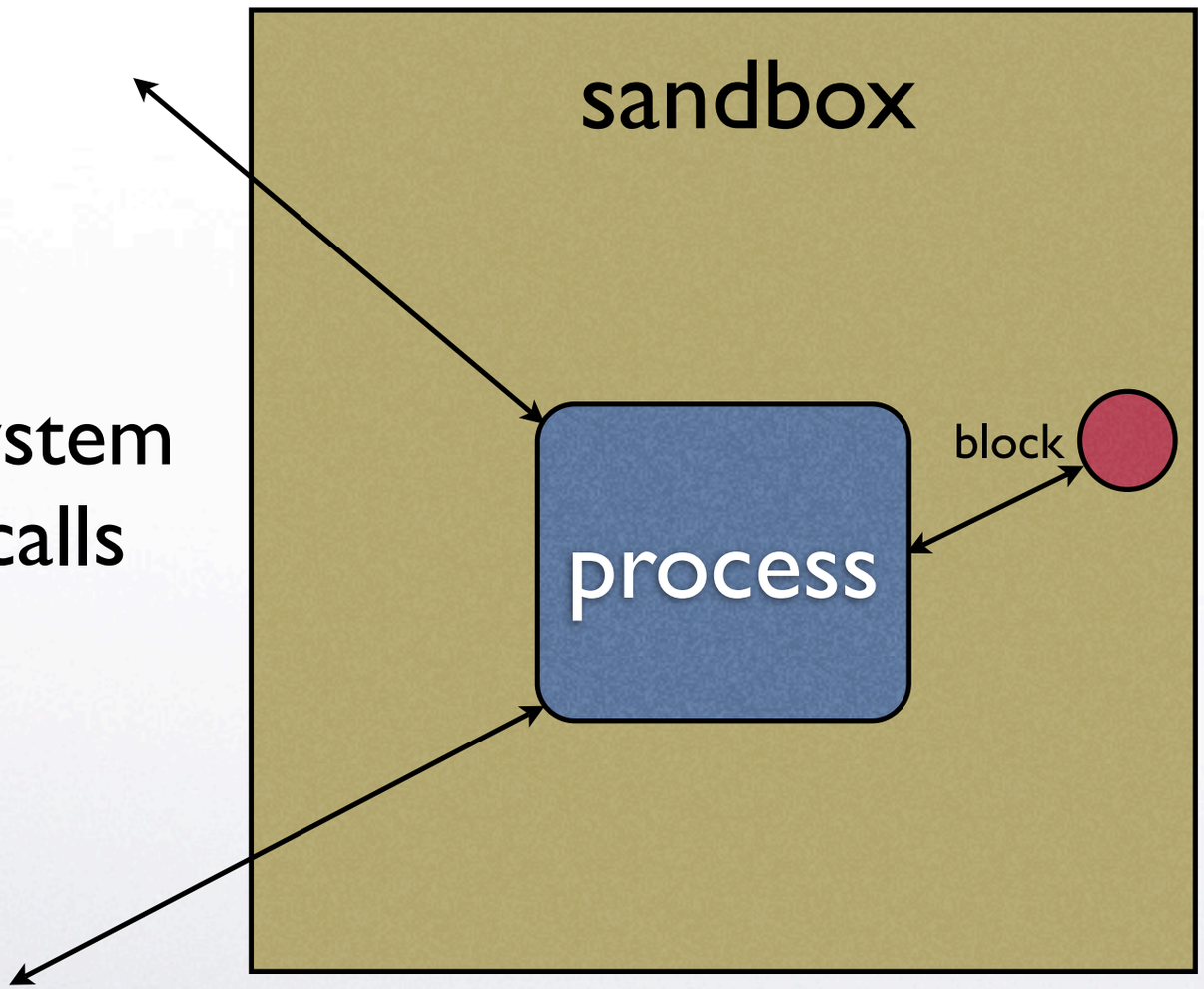
TOCTOU attack





From M. Bishop, M. Dilger, Checking for Race Conditions in File Accesses, Computing Systems 9 (2) pp. 131–152 (Spring 1996).

Sandboxing



Isolation of process from system

System call Interposition

Sandbox Policy?

May result in TOCTOU arms race vulnerability

Sandboxing, II

- systrace : free sandboxing tool for linux and freebsd. http://www.systrace.org/
- supports writing a policies that regulate the system calls (e.g., to network and disk) an application is allowed to perform.

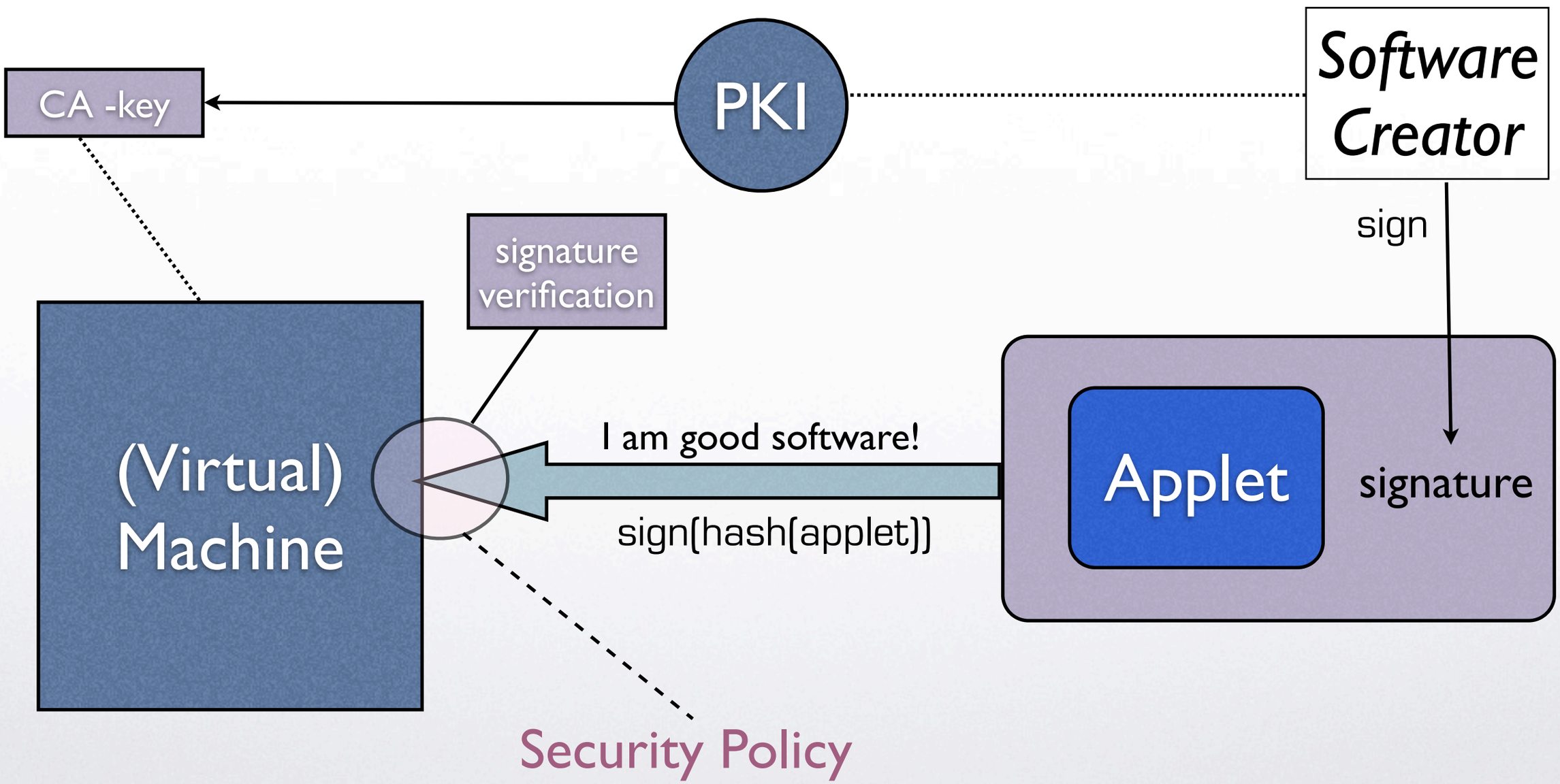
Virtual Machines

- Give the application its own machine ... a *virtual machine*.
- CPU and all physical devices are simulated.
- You can simulate devices you may not have!
- Performance cost.
- Example : VMware. Parallels. QEMU.

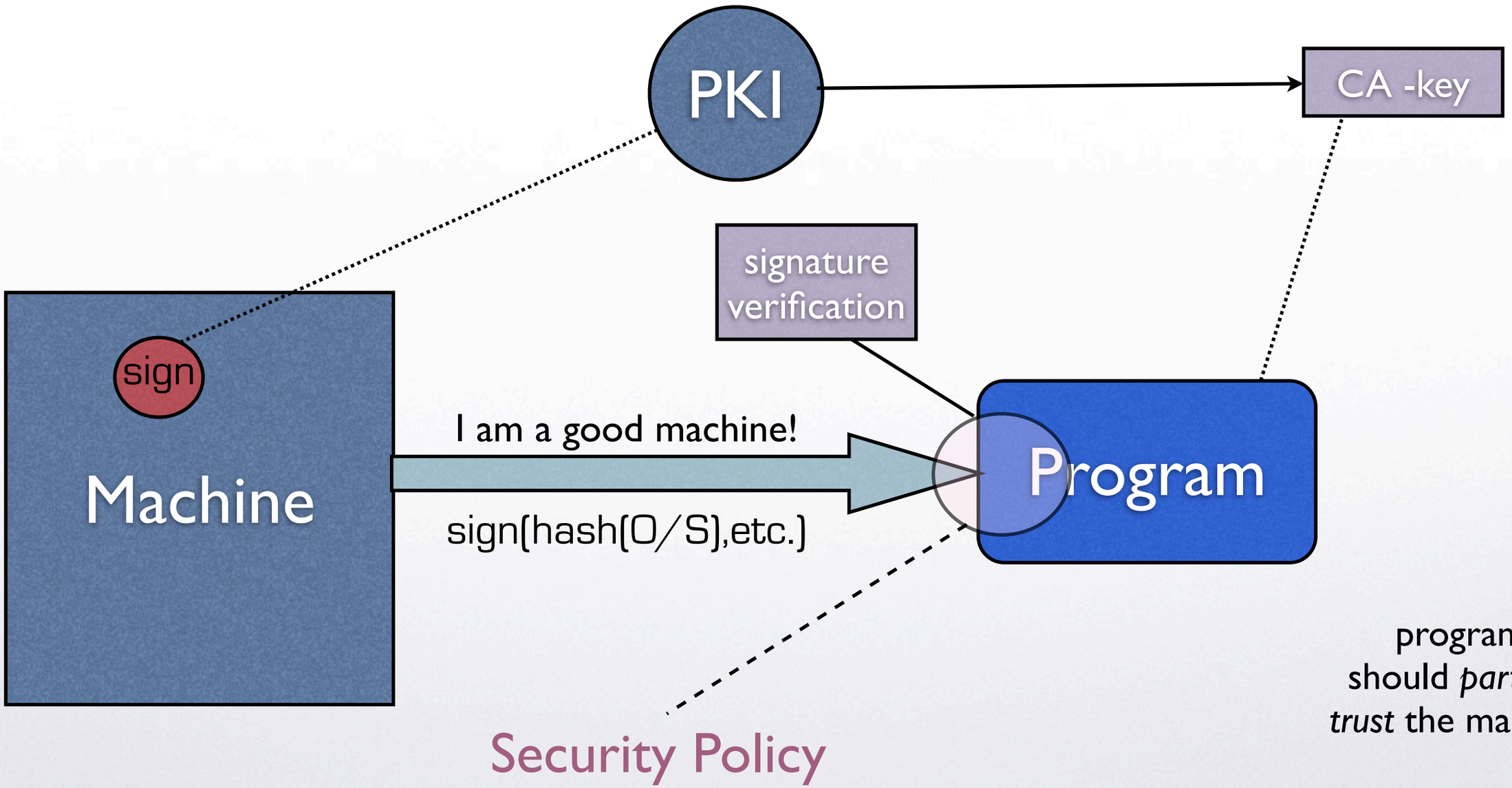
Interpreted Languages

- The Java Virtual Machine.
- SecurityManager class can be used by an applet to probe privileges inside its sandbox.
- Typical settings include restricted Internet access (deny everything except connection to the same server the applet came from), denying of most local resources such as disk read/writes, print jobs, clipboard, system libraries, exit JVM, etc.

Trusting the Software



Attestation



Trusted Computing

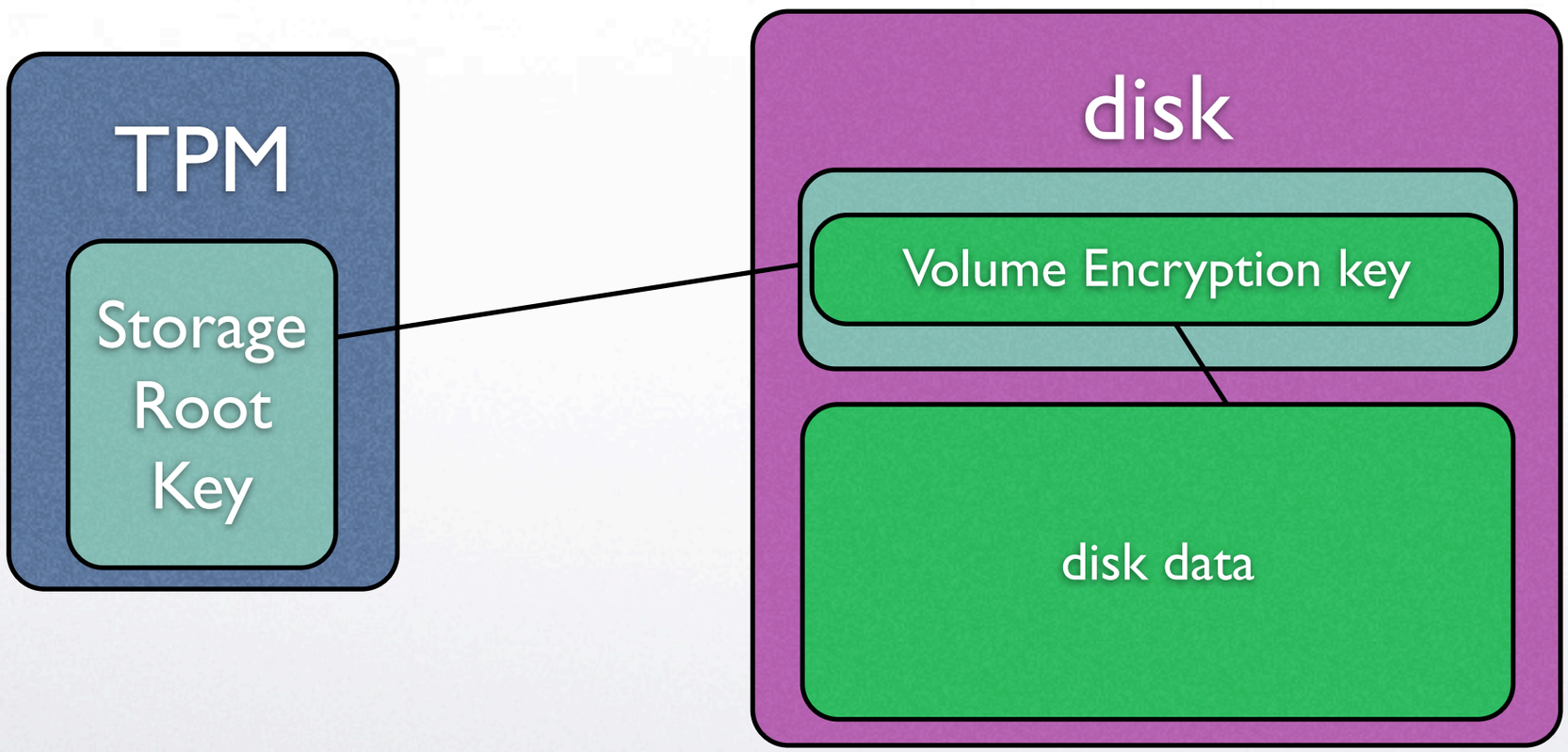
- Employ a *trusted platform module* (TPM) to facilitate remote attestation, stronger process isolation, secure I/O and other security features.
- How does it look?

Microsoft NGSCB

- Next Generation Secure Computing Base (used to be part of upcoming Windows codename *Longhorn* - now Vista; current status : upcoming).
- Strong Process Isolation. *Memory can only be accessed by application that it belongs.*
- Sealed Storage. *Data are stored in encrypted with a key derived from application/O/S info. Other apps or modified O/S's (e.g., compromised cannot read them)*
- Secure path to and from the user. *I/O streams between devices and applications are encrypted.*
- Attestation. *System attests to programs and remote systems that is uncompromised.*

http://www.microsoft.com/technet/archive/security/news/ngscb.mspx?mfr=true

Bitlocker (MS Vista)



In order to activate TPM several alternatives exist:
1) do nothing
2) use a PIN
3) use a strong key stored in a USB flash drive

also possible to setup a recovery key

The very first integration of TPM and Windows O/S (more to come...)

Trusted Computing Group

- Formerly: Trusted Computing Platform Alliance (Intel, Microsoft, HP, Compaq, IBM). Founded '99.
- It is a: "not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices"

https://www.trustedcomputinggroup.org/home

Possible TPM functions

- Cryptographic key management and operation: storage of RSA, DH, AES and other secret key data that allow the TPM to sign and encrypt data. Keys can be unique per TPM and initialized at activation time.
- protected non-volatile memory.
- protected counters
- Random number generation.
- Monitor Boot Process.

Platform Configuration Registers

- PCR contains a hash-chain :
  Hash(...., Hash(OSLoader, Hash(BIOS)) ...)
- PCRs are maintained by TPM and can be used to
  - (1) demonstrate the software running in the system.
  - (2) implement access control bound to a certain software configuration.
  - (3) detect tampering of the local machine.

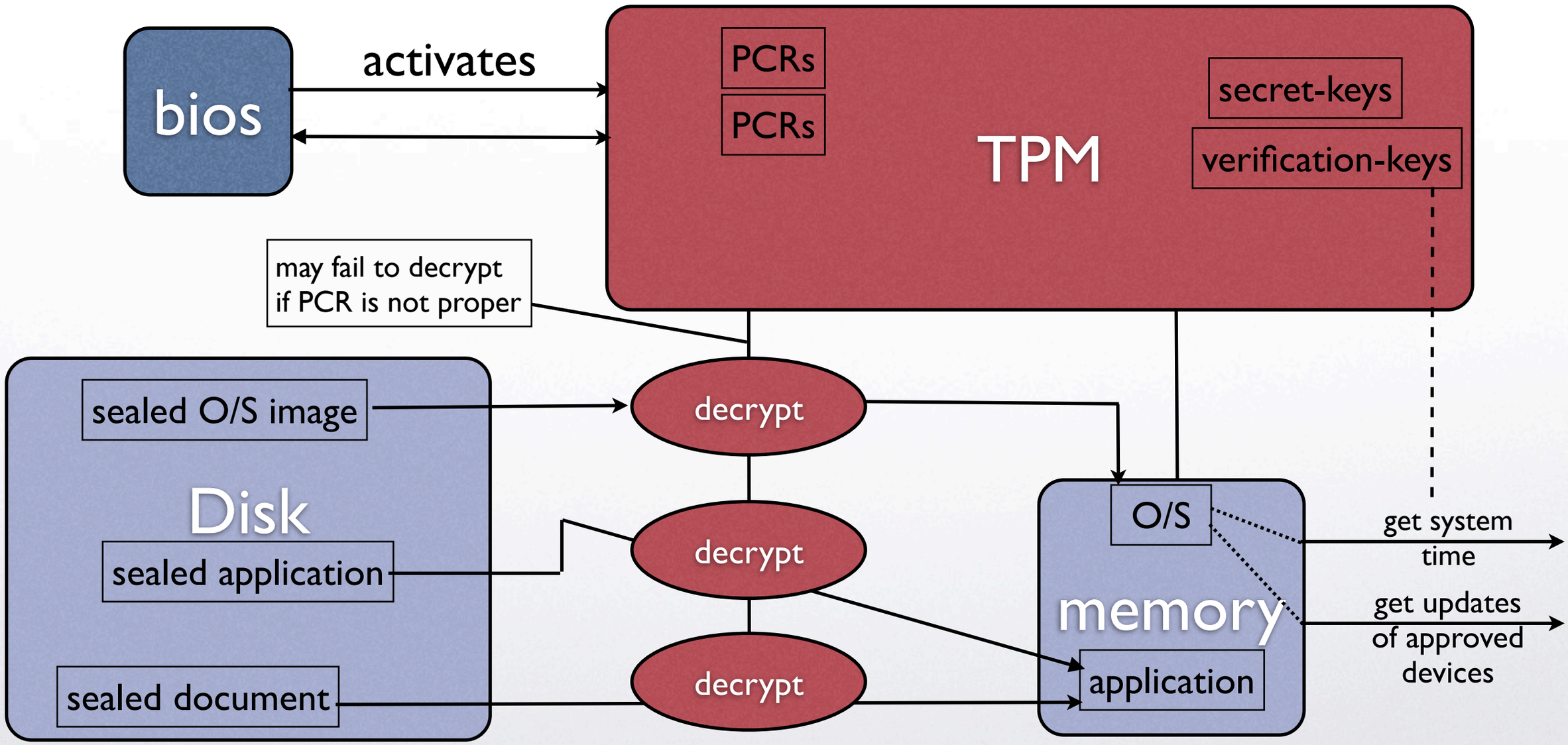
PCR Access Control

- User can ask TPM to **seal** any data based on a PCR register.
- Subsequently data will only be accessible if the PCR register is the same:
  - e.g., if a certain file is sealed and then you change your boot loader the sealed file would not be decryptable in your new configuration.

Remote attestation

- Have TPM create a signature on the PCR.
- Remote source (assuming that TPM is untampered) can use the TPM public-key to verify signature.
- After attestation remote source can make a SSL tunnel with local application for data exchange.
- issue: remote source must be able to recognize all valid PCR states.

Trusted Computing System



TC Potential

- Only trusted applications load, only appropriate documents are displayed (at the right times etc.).
- Licensing enforcing (hardware devices, software, media, music, movies).
- A compromised application will cease to operate properly (e.g., unable to open files).
- A compromised system will be unable to be fully functional.

TC and open source

- TC software (O/S or applications) may be released as open source.
- Still, this does not mean that it can be installed or read files in a TC system.
- HP is preparing a TC Linux system.

Issues

- Current state (what if programs/ O/S is altered at run-time?)
- What if bad code is sealed?
- What about privacy of users?

TC and Copyright Protection

- A match in heaven.
- A TC system allows any type of licensing (e.g., making media/documents unreadable, unplayable and impossible to save/print or modify). TPM counters can enforce time/# of use policies.
- It would require that the user is denied "root" (no hooks to the TPM).

XBOX

- XBOX = 733 MHz Pentium III, 64MB, USB, 10GB Hard Drive, DVD. O/S based on Windows 2000.
- Employed some TC techniques (CPU starts on a ROM not a flash BIOS, ROM loader verifies a second bootloader who eventually verifies windows kernel).
- Every game is signed by an RSA signature and the console verifies.

http://events.ccc.de/congress/2005/fahrplan/attachments/591-paper_xbox.pdf

why the fuss?

Threat	*Effect*	*Reason*
Linux	Xbox as a computer	Xbox sold at loss
Homebrew	media player, browser	software monopoly
Copied Games	piracy	obvious
Unlicensed Games	anyone can make games	missing royalties

table extracted from :

http://events.ccc.de/congress/2005/fahrplan/attachments/674-slides_xbox.pdf

Hacking XBOX

- Eventually hacked and linux installed (illegal under the DMCA). The software modification takes advantage of game saving feature and vulnerabilities. (gamesave buffer overflow *Mechassault, 007 Agent Under Fire, Splinter cell*).

- Games are running in Kernel mode!

- Loading a hacked save-game from USB storage you can (1) take over and boot linux, (2) modify XBOX dashboard.

- XBOX 360 significant efforts underway (as of 2009 - hardware mod is needed for linux to run); MS can respond to vulnerabilities with online patches.