

Trusted Computing

May 2, 2006

mnair@cs.sunysb.edu

We design a system to deliver content from a movie server over the internet. Figure 1 shows the schematic structure of such a system. The security goals of a such a system are:

1. Client must pay for download.
2. Can view only for 3 days.
3. Cannot share the movies.
4. Must watch all the advertisements.
5. Integrity of the movie (No Censorship).

In current systems with the root privileges, you can perform any action that you want; thus you can obtain the binary. The twist is that you donot trust the owner/root. We look at three solutions to this problem:

- Closed Platforms
- Trusted Computing Platforms
- Terra - Trusted Virtual Machine Monitor

Closed Platforms

A closed platform is usually a system with limited computing capability. It caters to only a small, specific function. The characteristic feature(closed) of these systems is that their structure and design is known only to the system designers. Examples of such computing devices include cellphones and DVD players. Cellphones are difficult to program. The designer donot intend it to be used for any purpose other than the one it is expressly programmed for in the factory. All DVDs are encrypted with a key. There exists a chip

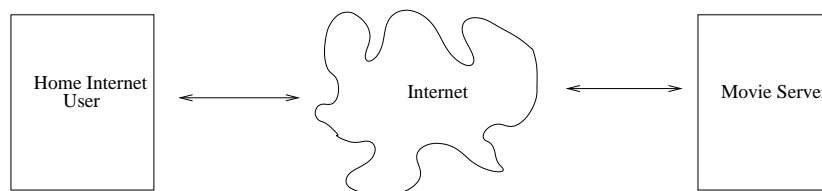


Figure 1: Schematic Design of Internet Movie Distribution Scheme

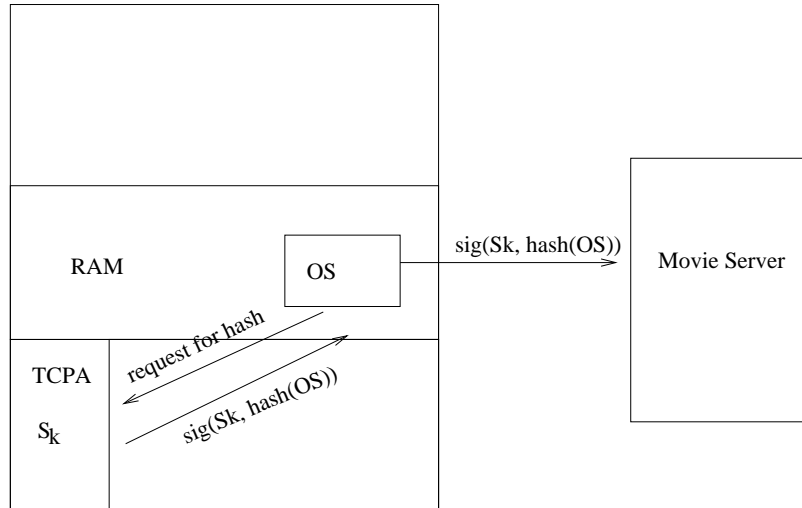


Figure 2: Design of Trusted Computing Platforms

for cryptography in the player which has the secret key. When a company designs a DVD player it is contractually bound to design it in a manner that does not compromise this secret key.

With closed platform we get very good security. Unfortunately we get it at the expense of flexibility and extensibility.

Trusted Computing Platform(TCP)

This comes under various names, TCPA(Trusted Computing Platform Alliance), Palladium, NGSCB(Next Generation Secure Computing Base). We want a small piece of tamper resistant hardware, which even an attacker(?) with a high-level of access cannot modify. What we require is *remote attestation*, i.e. we want to be able to securely identify the software running on a remote computer. If we trust this software then we can derive trust relations with other software running on the system and thus we will be able to achieve our goal.

We will thus require a hash of the operating system running on the system. However a system could lie about its hash – a wayward system could compute the hash from an image of another OS which exists on disk and send it. Thus we will require the hash to be signed by a piece of hardware we trust; the

trusted computing platform(TCP). TCPs should be tamper resistant and should sign only the currently running OS. A possible design for TCPs are elucidated in figure 2.

TCP proves to the remote party that the currently running client is "WinXP". Then the server trust WinXP to enforce the security policy. Thus the client enforces the security policy. This is the essence of remote attestation.

Criticisms

- **OS Fingerprinting** - Establishes accurately the OS running on the client side.
- **Vendor Locking** - Inability to change h/w or s/w vendors.
- **OS Inflexibility** - Ability to use only trusted operating systems.

Terra

The idea is to run a trusted Virtual Machine Monitor under the operating system. A Virtual machine(VM) is a number of different identical execution environments coexisting on a single computer, each of which exactly emulates the host computer. A Virtual Machine Monitor is that which manages these virtual machines. The structure of Terra is shown in figure 3.

Virtualization is a well studied technology. It is possible to get good performance and strong isolation (security) from VMMs. Here too we have a TCP which signs the TVMM images. TVMM in turn signs VM images. TVMM stores the signature of each VM securely on disk. If the signature of the currently running VM is that which is stored on disk, then the TVMM is able to verify that the VM has not been tampered with and thus can be trusted.

Trust is managed in the following manner:

1. TCPA to verify TVMM.
2. TVMM to verify the Virtual Machines and the disk images.

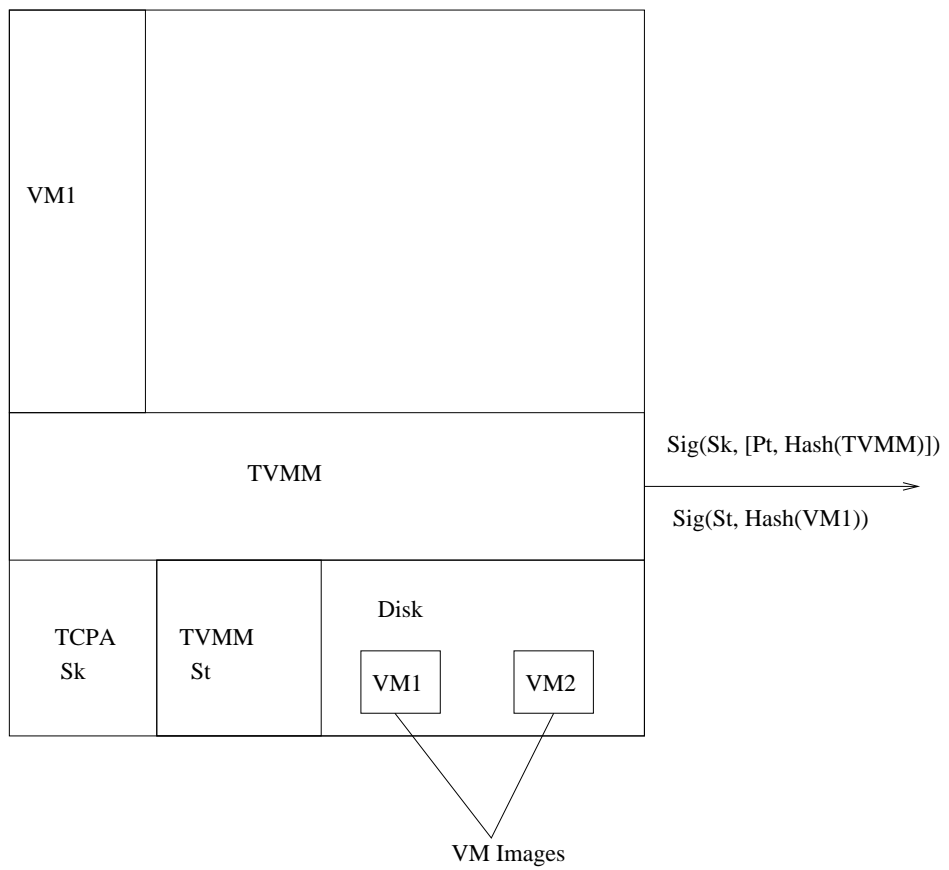


Figure 3: Design of Terra