Security II

Gregory Mounie

2012-10-16 mar.

Outline

How Protect physically your hardware

- Chain the box
- Remove if possible, the readers (CDROM, USB, SD) or close them
- Boot order (the hard disk first)
- Add a password to the BIOS (or UEFI)

Basic software protection

- Minimize user right
  - Windows: troyan horse, network disk, virus
  - Unix: admin right, SELinux, Virtualization
- Crypt mobile storage (including laptop hard-disk)
- Passwords
  - keep also hashes safe
- Minimize running services

ACL

`chmod` allows to set up:

1. user access (the proprietary of the file)
2. group access (the group of the proprietary associated to the file)
3. other access (any other people)
4. sticky bit, setuid bit

`getfacl` and `setfacl` allows manipulation at a finest grain and set up default inherited right for new file/directory:

1. the same rights as `chmod`
2. the mask
3. one particular user access
4. one particular group access
5. inheritable previous right with the keyword `default`

ACL example

```
setfacl -m u:Alice:rwx ./TheFile.txt
setfacl -m default:g:Admin:rwx ./Thedirectory
```


Disabing an account

lock `passwd -l username`

unlock `passwd -u username`

sudo

sharing administrator right

```
username ALL=(ALL) ALL
```

quota

activate it in /etc/fstab: usrquota, grpquota soft and hard limits on blocks and on inodes

Ssh pre-history (pre-Big-Internet)

In the old days, it was already possible to work remotely with UNIX and transfer data (rlogin, telnet, rsh, ftp).

- Password are plain text, but store as hashes on the server
  It passes through the network in plain text The hash is computed on the server and compare to its database.
- Other needs
  X11 forwarding

Ssh multiple strategies

Two main possibilities

- Create a secure channel before sending the password (Diffie-Hellman)
- Use a private/public key pair

Diffie-Hellman

Public information: a G group (x), a generator g of the group with an order of n. n is a 1024 bits integer.

1. Alice choose x and send $X = g^x mod n$, (Bob, $Y = g^y mod n$)
2. Alice compute $K = Y^x = g^{xy} mod x$ (Bob compute K too)
3. K is the session key

- Safety of the value of K
  - to compute K, you need x or y in addition to the messages
  - to compute x knowing X require to compute a discrete log. The only known way is to enumerate all values of $g^z mod n$
- Compute g^x
  How to compute g^x quickly ?

Ssh host key

- A key identifies the server
- The client verifies the key of the server at every connection
- The client accept the key at the first connection

Counter-example: NIS+NFSv3

- NIS: password hashes are readable by any user on the network

```
ypcat passwd
```

- NFS: filtering access by IP addresses: Most of the time access is granted to a IP range. Otherwise, spoofing is possible by any computer on the local network.

```
/               master(rw) trusty(rw,no_root_squash)
/projects       proj*.local.domain(rw)
/usr            *.local.domain(ro) @trusted(rw)
/home/joe       pc001(rw,all_squash,anonuid=150,anongid=100)
```

- NFS: NFS use UID of the client to authenticate and compute access right (default option: `sec=sys`)

Why people use NIS+NFSv3 now

It is trivially easy to set up a network (10-20 minutes) !

Secure solutions exist
NFSv4 allows use of Kerberos to mitigate previous problems

Kerberos

3 steps connection to a service:

1. authenticate user with the login server
2. get a ticket usable only with the targeted service
3. connect to the service using the ticket

The secret key of the user/service (K_a and K_b) is know by the associated `Principal` (user/service) and the server. A secret key K_{tgs} is shared also with the Ticket Granting Server `TGS` The keys are stored in a database of the server (the Key Distribution Center `KDC`)

Kerberos messages

To connect A to B:

1. from A to login server : A
2. answer : $Ka(Ks, Ktgs(A, Ks)) $,
3. from A to TGS : $Ktgs(A, Ks), B, Ks(t) $,
4. answer : $Ks(B, Kab)Kb(A, Kab)$
5. from A to B : $Kb(A, Kab), Kab(t)$
6. answer : $Kab(t + 1)$

How to set up Kerberos

The main problem of kerberos settings is the key management.
In addition to setup Kerberos, you need also to setup LDAP (user directory).

emulation versus virtualization versus containment

emulation and simulation simulate a host on another host
virtualization simulate the loneliness on the host
Containment separate the host in separated parts

Emulation

Android SDK
The android SDK for x86 (PC) come with a simulator of the ARM architectures (qemu)

Qemu/Bochs/VmWare

- linux guest on windows host,
- windows guest on linux host,
- linux guest on linux host.

- Hardware dependent emulation
  When the guest use the same (or similar) hardware, the emulation may run natively the non-privileged instructions (kvm)

Virtualization

It simulates the loneliness on the host. It is an old idea (mainframe IBM).
It is very similar to time sharing systems but one step further: Instead of switching between running software in user mode, virtualization switches between simulated hardware (user+system mode).

Definition (Hypervizor)

The intermediate layer between the virtualized hardware and the real one.

- Para-virtualisation (Xen)
  - the hypervizor is a coopération layer betwen (le guest est au courant)

Ring 0, Ring 3, Ring -1

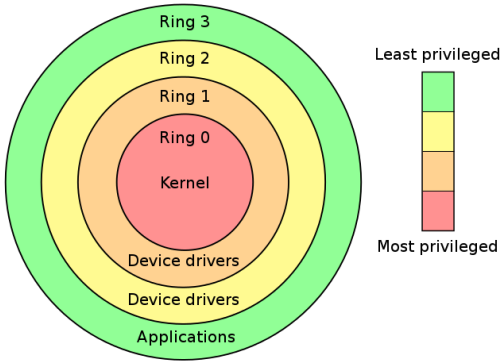

Figure: The classical privileged rings

Ring -1.

Processors with Intel VT-x or AMD-V extensions add a ring -1

Containment

Your default linux provides several helpful mechanisms:

- Chrooting (Schroot):: use only a subset of the file system for your processes
- cgroup:: limit the processor and the memory used by a set of processes
- LXC:: a full virtual environment based on cgroup

SELinux

A set of modules implementing a mandatory access control (MAC)
The idea is to limit the possibilities of an application at a kernel level in a flexible way.