Operating System Security

Francesco Regazzoni

Contents

1 Operating Systems Security

2 Random Number Generators

What is an Operating System?

- Software controlling the overall operation of a multipurpose computer system, including such tasks as memory allocation, input and output distribution, interrupt processing, and job scheduling.
  $www.crucial.com/library/glossary.asp$
- Software that shares a computer system's resources (processor, memory, disk space, network bandwidth, and so on) between users and the application programs they run. Controls access to the system to provide security.
  $www.tldp.org/LDP/Linux - Filesystem - Hierarchy/html/glossary.html$
- Still a Software!

How To Harden the OS?

- Remove all the unnecessary software
- Remove all the unnecessary services
- Change default accounts
- Use the least privilege principle
- Regularly update
- Activate logging

Remove all the unnecessary software

- Be sure that we are running the bare minimum needed
- Example: do not leave office applications in a web server
- Be careful also of “unwanted additions” (software installed for testing that stays there)

Remove all the unnecessary services

- Similarly, be sure that we are running the bare minimum needed
- Could be difficult to identify which services are running
- We can check which ports are open to identify an active service
- For instance: Port 22 SSH, Port 53 DNS, Port 80 HTTP

Change default accounts

- Often you have standard account (administrator and guest, for instance)
- Often have permissive permission
- Often have “standard” password
- Disable these accounts if not needed
- Change all the default passwords

Use the least privilege principle

- Give to programs, users and systems just enough privileges
- Provide privileges when needed and disable after
- Separate accounts

Regularly update

- Vulnerabilities are frequently discovered
- Regular updates allow to mitigate/patch vulnerabilities
- Patch also the critical controlling software

Activate logging

- Accurate log is fundamental (why?)
- Activities carried out with administrative privileges
- Logins of users
- Updates to OS

Handling Sharing vs Protection

- Sharing: wanted (why?)
- Protection: needed but difficult

Basic security OS

- Separation
- Protection
- Access Control
- Logging

Separation

- Processes and Users must be separated
- Physical separation: separated devices
- Temporal separation: executed at different moment of time
- Logical separation: believe to have its machine
- Cryptographic separation: encrypt memory

Memory Protection

- Processes can access memory only within certain boundaries
- Memory section can have a tag to enforce/check accesses

Access Control

- Ensures that all direct accesses to object are authorized
- Protects against accidental and malicious threats by regulating the read, write and execution of data and programs

Requires

- Proper user identification
- Information specifying the access rights is protected form modification

Access Control - Main Components

- Access control policy
- specifies the authorized accesses of a system
- Access control mechanism
- implements and enforces the policy

Covert Channel

- A way to break the insulation indirectly
- Information is transferred in a covert way

Contents

1 Operating Systems Security

2 Random Number Generators

Random Number Generators

- True Random Number Generators
- Pseudo Random Number Generators

True Random Number Generators

- Entropy Source
- “Digitalizer”
- Post Processing

Entropy Source

- Ring Oscillators
- Quantum

Post Processing

- Remove the bias
- von Neumann

Pseudo Random

- Generated from a seed
- Sequences that have the statistical property of a random sequence

How to test randomness

- Apply statistical test
- Make an entropy model of the source

Can we trust the RNG?

- A lot of security depends on the RNG
- Get access to internal states to ensure quality

Questions?

f.regazzoni@uva.nl