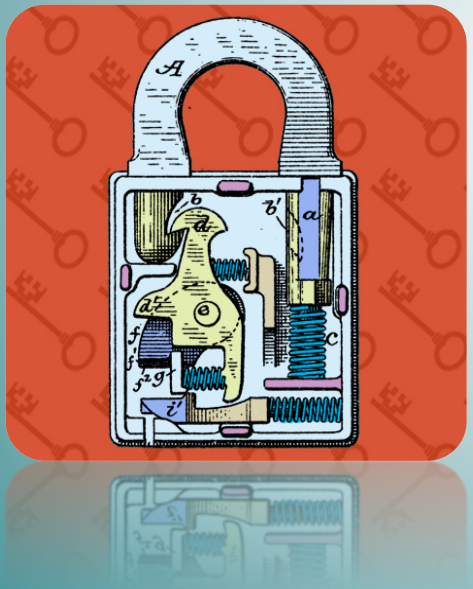
Garantía y Seguridad en Sistemas y Redes

Tema 11. Operating System Security



Esteban Stafford

Departamento de Ingeniería Informática y Electrónica

Contents

Motivation

- Top 35 Mitigation Strategies (DSD Australia)
- First four could prevent 70% of analised attacks (2009)
  - Patch operating systems and applications using auto-update
  - Patch third party applications
  - Restrict admin privileges to users who need them
  - White-list approved applications

System Security Planning

- Thinking before doing!
- Cost of planning is less than retro-fitting
- Planning check list:
  - Identify purpose of system, info stored, applications, services, and security requirements.
  - Categorize users.Their privileges and info they should have access to.
  - Decide authentication methods.
  - How does the system access the information, local and remote.
  - Who are the administrators of the system. How, from where?
  - Aditional security measures. Host FW, anti-virus, logging...

Initial Setup

- Installation process is very vulnerable. Perform in a protected area.
- Ensure OS media and additional drivers are malware-free.
- Restrict internet access.
- Install minimum system.
- Protect boot process. (BIOS)
- Consider crypto FS.
- Configure auto-update. (With pre-validation)

Strip Unnecessary Stuff

- Any software may contain vulnerabilities.
- Make sure ONLY needed applications/services are installed.
- Better not to install than install and disable or remove.

Users, Groups and Auth.

- Not all users do the same.
- Taylor permisions to suit the need of the different user groups.
- Special users only access elevated privileges when needed.
- Configure authentcation methods.
- Enforce password complexity, lengthe ageing.
- Local vs remote centralized authentication/authorization.
- Disable login in default accounts. Change default passwords.

Install Additional Security

- Install IDS, anti-virus, host firewall.
- Consider white-listing applications.
- Install logging
- Configure filesystem backup and archiving.

Test System Security

- Run automated auditing tools.
- Repeat periodicly during system lifetime.