Hochschule Konstanz
Fakultät Informatik

Introduction to IT Security

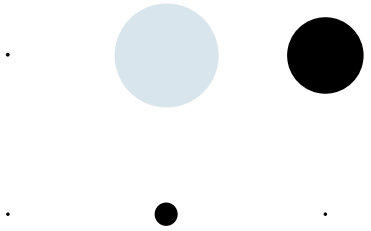
WIN+AIN

Hanno Langweg

04a Secure Operating Environments - OS Hardening

Secure Operating Environments

- Security of operating systems
- Trusted Computing
- Access control
- Malware



Hochschule Konstanz
Fakultät Informatik

Operating System Security

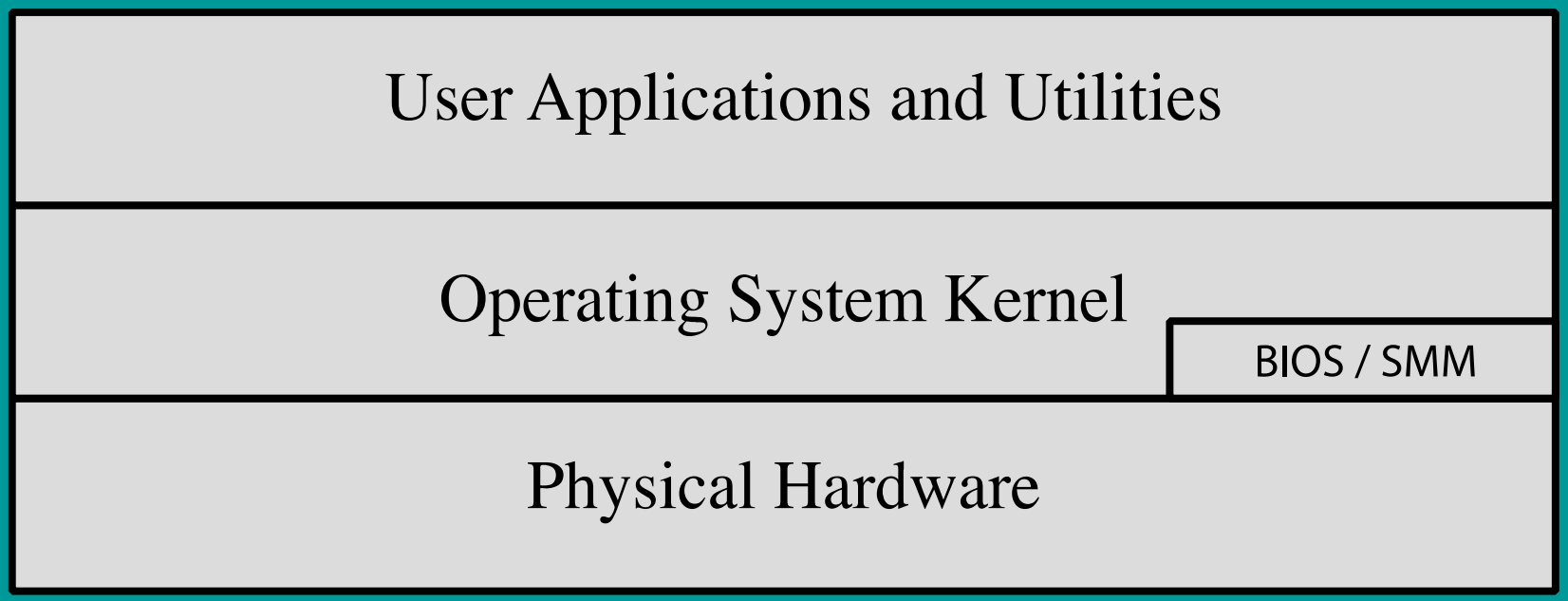


Figure 12.1 Operating System Security Layers

IT baseline protection

- IT-Grundschutz ("baseline protection") developed by German Federal Information Security Agency BSI (Bundesamt für Sicherheit in der Informationstechnik)
- Modules for secure IT operation
  - OPS: IT operations
  - SYS: IT systems
- Over 85% of targeted cyber intrusions investigated by Australian Signals Directorate (ASD) in 2009 could have been prevented; top four strategies:
  - White-list **approved applications**
  - **Patch** third-party applications and OS vulnerabilities
  - **Restrict** administrative privileges
  - Create a defense-in-depth system

Operating Systems Hardening

- Secure base OS
  - Install and patch OS
  - Harden and configure OS by:
    - Removing unnecessary services, applications, protocols
    - Configuring users, groups, and permissions
    - Configuring resource controls
- Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)
- Test security of basic OS to ensure that steps taken adequately address its security needs

Remove Unnecessary Services, Applications, Protocols

- Fewer software packages available to run ➔ less risk
- System planning process should identify what is required for a given system
- Default configuration might not be secure:
  - Default configuration set to maximize ease of use and functionality rather than security
  - Additional packages can later be installed if required

Configure users, groups, and permissions

- Not all users need same access to all data and resources on a system
- Elevated privileges should be restricted to those users that require them, and only when needed to perform task
- System planning process should consider:
  - Categories of users on the system
  - Privileges they have
  - Types of information they can access
  - How and where access control configuration is set
- Remove/disable/secure default accounts included as part of installation

Configure Resource Controls, Install Additional Security Controls

- Once users and groups are defined, appropriate permissions can be set on data and resources
- Many security hardening guides provide lists of recommended changes to default access control configuration
- Further security possible by additional security tools:
  - Anti-virus software
  - Host-based firewalls
  - IDS (intrusion detection) or IPS (intr. prevention) software
  - Application white-listing

IT baseline protection example excerpt

– B 3.102 Servers under Unix

Threat scenarios

The following typical threats to the IT-Grundschutz of a Unix server are assumed to exist:

Organisational shortcomings

- G 2.15 *Loss of confidentiality of sensitive data in the UNIX system*

Human error

- G 3.10 *Incorrect export of file systems under UNIX*
- G 3.11 *Improper configuration of sendmail*

Technincal failure

- G 4.11 *Lack of authentication possibilities between NIS server and NIS client*
- G 4.12 *Lack of authentication possibilities between X server and X client*

Deliberate acts

- G 5.41 *Misuse of a UNIX system with the help of UCCP*
- G 5.89 *Hijacking of network connections*

IT baseline protection example excerpt

The bundle of safeguards for servers running the Unix operating system is presented in the following.

Planning and design

- M 2.33 (Z) *Division of administrator roles under Unix*
- M 4.13 (A) *Careful allocation of identifiers*
- M 4.18 (A) *Administrative and technical means to control access to the system-monitor and single-user mode*
- M 5.16 (B) *Survey of network services*
- M 5.34 (Z) *Use of one-time passwords*
- M 5.64 (Z) *Secure Shell*
- M 5.83 (Z) *Secure connection of an external network with Linux FreeS/WAN*

Implementation

- M 4.9 (A) *Use of the security mechanisms of X Windows*
- M 4.14 (A) *Mandatory password protection under Unix*
- M 4.19 (A) *Restrictive allocation of attributes for Unix system files and directories*
- M 4.20 (B) *Restrictive allocation of attributes for Unix user files and directories*
- M 4.21 (A) *Preventing unauthorised acquisition of administrator rights*
- M 4.22 (Z) *Prevention of loss of confid[illegible] of sensitive data in the Unix system*
- M 4.23 (B) *Secure invocation of execu*
- M 4.105 (A) *Initial measures after a Un*
- M 4.106 (A) *Activation of system loggir*
- M 5.17 (A) *Use of the NFS security mechanisms*
- M 5.18 (A) *Use of the NIS security mechanisms*
- M 5.19 (A) *Use of the sendmail security mechanisms*
- M 5.20 (A) *Use of the security mechanisms of rlogin, rsh, and rcp*
- M 5.21 (A) *Secure use of the telnet, ftp, tftp, and rexec*
- M 5.35 (A) *Use of the security mechanisms of UUCP*
- M 5.72 (A) *Deactivation of unnecessary network services*

Operation

- M 4.25 (A) *Use of logging in Unix systems*
- M 4.26 (C) *Regular security checks of Unix systems*

Contingency planning

- M 6.31 (A) *Procedural patterns following a loss of system integrity*