CSGE602055 Operating Systems
CSF2600505 Sistem Operasi
Week 02: Security, Protection, Privacy, & C-language

Rahmat M. Samik-Ibrahim (ed.)

University of Indonesia

`https://os.vlsm.org/`
Always check for the latest revision!

REV270 26-Feb-2021

Week	Schedule & Deadline[1])	Topic	OSC10[2])
Week 00	22 Feb - 28 Feb 2021	Overview 1, Virtualization & Scripting	Ch. 1, 2, 18.
Week 01	01 Mar - 07 Mar 2021	Overview 2, Virtualization & Scripting	Ch. 1, 2, 18.
Week 02	08 Mar - 16 Mar 2021	Security, Protection, Privacy, & C-language.	Ch. 16, 17.
Week 03	17 Mar - 23 Mar 2021	File System & FUSE	Ch. 13, 14, 15.
Week 04	24 Mar - 30 Mar 2021	Addressing, Shared Lib, & Pointer	Ch. 9.
Week 05	31 Mar - 06 Apr 2021	Virtual Memory	Ch. 10.
Week 06	07 Apr - 25 Apr 2021	Concurrency: Processes & Threads	Ch. 3, 4.
Week 07	26 Apr - 02 May 2021	Synchronization & Deadlock	Ch. 6, 7, 8.
Week 08	03 May - 09 May 2021	Scheduling + W06/W07	Ch. 5.
Week 09	17 May - 23 May 2021	Storage, Firmware, Bootloader, & Systemd	Ch. 11.
Week 10	24 May - 06 Jun 2021	I/O & Programming	Ch. 12.

---

[1]) The **DEADLINE** of Week 00 is 28 Feb 2021, whereas the **DEADLINE** of Week 01 is 07 Mar 2021, and so on...

[2]) Silberschatz et. al.: **Operating System Concepts**, 10th Edition, 2018.

[3]) This information will be on **EVERY** page two (2) of this course material.

STARTING POINT — `https://os.vlsm.org/`

☐ **Text Book** — Any recent/decent OS book. Eg. (**OSC10**)
Silberschatz et. al.: **Operating System Concepts**, 10th Edition,
2018. See also `http://codex.cs.yale.edu/avi/os-book/OS10/`.

☐ **Resources**

    ☐ **SCELE OS211** —
`https://scele.cs.ui.ac.id/course/view.php?id=3134`.
The enrollment key is **XXX**.

    ☐ **Download Slides and Demos from GitHub.com**
`https://github.com/UI-FASILKOM-OS/SistemOperasi/`:
os00.pdf (W00), os01.pdf (W01), os02.pdf (W02), os03.pdf (W03),
os04.pdf (W04), os05.pdf (W05), os06.pdf (W06), os07.pdf (W07),
os08.pdf (W08), os09.pdf (W09), os10.pdf (W10).

    ☐ **Problems** — `https://rms46.vlsm.org/2/`:
195.pdf (W00), 196.pdf (W01), 197.pdf (W02), 198.pdf (W03),
199.pdf (W04), 200.pdf (W05), 201.pdf (W06), 202.pdf (W07),
203.pdf (W08), 204.pdf (W09), 205.pdf (W10).

    ☐ **LFS** — `http://www.linuxfromscratch.org/lfs/view/stable/`

    ☐ **OSP4DISS** — `https://osp4diss.vlsm.org/`

    ☐ **DOIT** — `https://doit.vlsm.org/001.html`

Agenda

- Overview of system security
- Policy/mechanism separation
- Security methods and devices
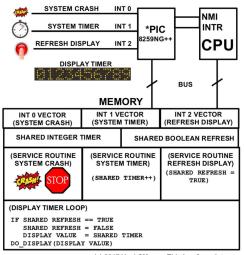- Protection, access control, and authentication
- Backups

---

[1]Source: ACM IEEE CS Curricula 2013

- Articulate the need for protection and security in an OS (cross-reference IAS/Security Architecture and Systems Administration/Investigating Operating Systems Security for various systems). [Assessment]
- Summarize the features and limitations of an operating system used to provide protection and security [Familiarity]
- Explain the mechanisms available in an OS to control access to resources [Familiarity]
- Carry out simple system administration tasks according to a security policy, for example creating accounts, setting permissions, applying patches, and arranging for regular backups [Usage]

---

[1]Source: ACM IEEE CS Curricula 2013

Figure: How to protect and secure this design?

The Security Problem

- **OSC10**:
    - **Security** is a measure of confidence that the integrity of a system and its data will be preserved.
    - **Protection** is the set of mechanisms that control the access of processes and users to the resources defined by a computer system.
- Secure System, Intruders, Threat, Attack.
- Security Violation Categories: Breach of (confidentiality, integrity, availability), theft of service, DOS.
- Security Violation Methods: Masquerading, Replay attack, Human-in-the-middle attack, Session hijacking, Privilege escalation.
- Security Measure Levels: Physical, Network, Operating System, Application.
- Program, System, and Network Threats
    - Social Engineering: Phishing.
    - Security Hole: Code Review.
    - Principle of least privilege.

The Security Problem (cont)

- Threats: Malware, Trojan Horse, Spyware, Ransomware, Trap (back) Door, Logic Bomb, Code-injection Attack, Overflow, Script Kiddie.
- Viruses: Virus Dropper, Virus Signature, Keystroke Logger.
- Worm, Sniffing, Spoofing, Port Scanning, DOS (Denial of Service).
- Cryptography: (Symmetric and Asymmetric) Encryption, Public/Private Key Pairs, Key Distribution, Digital Certificate.
- User Authentication:
    - Password: One Time Password, Two-Factor Authentication,
    - Biometrics.
- Implementing Security Defenses: Policy, Assesment, Prevention, Detection, Protection, Auditing.
- Linux Security
- gnupg & sha1sum

Protection

- Principle of Least Privilege
- Domain Structure and Access Matrix
- ACL: Access Control List
    - Domain = set of Access-rights (eg. **user-id**).
    - Access-right = <object-name, rights-set> (eg. object: file).

	File1	File2	File3	Printer
User1	Read		Read	
User2				Print
User3		Read	Execute	Print
User4	R/W		R/W	Print

- Access-right Plus Domain (Users) as Objects

	F1	F2	F3	Printer	U1	U2	U3	U4
U1	R		R			SW		
U2				Print			SW	SW
U3		R	EXEC	Print				
U4	R/W		R/W	Print	SW			

Copy Rights

- Start

	File1	File2	File3
User1	Exec		Write*
User2	Exec	Read*	Exec
User3	Exec		

- User3: Read access to File2 (by User2)

	File1	File2	File3
User1	Exec		Write*
User2	Exec	Read*	Exec
User3	Exec	**Read**	

- Owner Rights

	File1	File2	File3
User1	O & E		W
User2		O & R* & W*	O & R* & W
User3		W	W

Privacy (Wikipedia)

- Privacy can mean different things in different contexts; different people, cultures, and nations have different expectations about how much privacy a person is entitled to or what constitutes an invasion of privacy.
- Considering all discussions as one of these concepts
  - Right to be let alone (such as one's own home).
  - Limited access (no information collection).
  - Control over information (in the era of big data).
  - States of privacy: solitude, intimacy, anonymity, and reserve.
  - Secrecy: does not apply for any already publicly disclosed.
  - Personhood and autonomy.
  - Self-identity and personal growth.

Beginner's Guide to Internet Safety & Privacy

- **URL:** `https://choosetoencrypt.com/privacy/complete-beginners-guide-to-internet-safety-privacy/`
- Who Are You Protecting Yourself From?
    - Governments
    - ISPs
    - (H)Crackers
    - Trackers
    - Advertisers/Malwertisers
- Which Information Should You Keep Private?
    - Metadata
    - Personal Information
    - Passwords
    - Financial Data
    - Medical Records
    - History
    - Communication

- Reference: (Any C Language Tutorial)

Week 02: Summary

- Reference: (OSC10-ch16 OSC10-ch17 demo-w02)
- Goals of Protection
- Domain and Access Matrix
- ACL: Access Control List
- The Security Problem
- Threats: Trojan Horse, Trap Door, Overflow, Viruses, Worms, Port Scanning, DOS (Denial of Service).
- Cryptography: (Symmetric and Asymmetric) Encryption,
- User Authentication: Password, Biometrics.
- Implementing Security Defenses: Policy, Assesment, Prevention, Detection, Protection, Auditing.
- Privacy.

- ☐ Week 02: Assignment (**os02.pdf**). (Eg. **cbkadal**).
    1. Read: (OSC10 chapter 16 + chapter 17)
    2. Generate a GnuPG Key Pair https://osp4diss.vlsm.org/CBKadal2.html.
    3. Import the operatingsystems@vlsm.org **Public Key** from https://osp4diss.vlsm.org/ETC/ospubkey.txt.
    4. Export **YOUR PUBLIC KEY** to be displayed as https://cbkadal.github.io/os211/TXT/mypubkey.txt.
    5. Visit https://os.vlsm.org/GitHubPages/. Review and pick at least 3 out of your 10 closest neighbors. Place the result into https://cbkadal.github.io/os211/TXT/myrank.txt.
    6. Update your **TOP 10 List** of Week 02 (https://cbkadal.github.io/os211/W02/). Please be more creative!
    7. Write a simple and useful bash script (https://cbkadal.github.io/os211/TXT/myscript.sh).
    8. Update https://cbkadal.github.io/os211/TXT/mylog.txt.
    9. Make SHA256SUM and sign it (detached, armor) as SHA256SUM.asc.
- ☐ This page is https://os.vlsm.org/Slides/check02.pdf.

The End

- ☐ This is the end of the presentation.
- ☒ This is the end of the presentation.
- This is the end of the presentation.