

# 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!

REV190 07-Feb-2019

# Operating Systems 2019-1

A (Rm 3114) [Tu/Th 10-12] — B (Rm 3114) [Tu/Th 13-15] — C (Rm 3114)

[Tu/Th 16-18] — D (Rm 2401) [Tu/Th 10-12] — E (Rm 2306) [Tu/Th 13-15]

| Week     | Schedule             | Topic  | OSC10                                  |
|----------|----------------------|--|--|
| Week 00  | 07 Feb - 13 Feb 2019 | Overview 1, Virtualization & Scripting         | Ch. 1, 2, 18.                          |
| Week 01  | 14 Feb - 20 Feb 2019 | Overview 2, Virtualization & Scripting         | Ch. 1, 2, 18.                          |
| Week 02  | 21 Feb - 27 Feb 2019 | Security, Protection, Privacy,<br>& C-language | Ch. 16, 17                             |
| Week 03  | 28 Feb - 06 Mar 2019 | File System & FUSE                             | Ch. 13, 14, 15                         |
| Week 04  | 12 Mar - 18 Mar 2019 | Addressing, Shared Lib, & Pointer              | Ch. 9                                  |
| Week 05  | 19 Mar - 25 Mar 2019 | Virtual Memory                                 | Ch. 10                                 |
| Mid-Term | 23-30 Mar 2019 (tba) | MidTerm (UTS)                                  |  |
| Week 06  | 02 Apr - 08 Apr 2019 | Concurrency: Processes & Threads               | Ch. 3, 4                               |
| Week 07  | 09 Apr - 15 Apr 2019 | Synchronization & Deadlock                     | Ch. 6, 7, 8                            |
| Week 08  | 16 Apr - 22 Apr 2019 | Scheduling                                     | Ch. 5                                  |
| Week 09  | 23 Apr - 29 Apr 2019 | Storage, BIOS, Loader, & Systemd               | Ch. 11                                 |
| Week 10  | 30 Apr - 06 May 2019 | I/O & Programming                              | Ch. 12                                 |
| Reserved | 07 May - 17 May 2019 |  |  |
| Final    | 18-25 May 2019 (tba) | Final (UAS)                                    | This schedule is<br>subject to change. |
| Extra    | 27 Jun 2019          | Extra assignment confirmation                  |  |

# The Weekly Check List

- ☐ **Resources:** <https://os.vlsm.org/>
  - ☐ **(THIS) Slides** — <https://github.com/UI-FASILKOM-OS/SistemOperasi/tree/master/pdf/>
  - ☐ **Demos** — <https://github.com/UI-FASILKOM-OS/SistemOperasi/tree/master/demos/>
  - ☐ **Extra** — [BADAK.cs.ui.ac.id:///extra/](http://BADAK.cs.ui.ac.id:///extra/)
  - ☐ **Problems** — <https://rms46.vlsm.org/2/>:  
195.pdf (Week 00), 196.pdf (Week 01), 197.pdf (Week 02),  
198.pdf (Week 03), 199.pdf (Week 04), 200.pdf (Week 05),  
201.pdf (Week 06), 202.pdf (Week 07), 203.pdf (Week 08),  
204.pdf (Week 09), 205.pdf (Week 10).
- ☐ **Text Book:** any recent/decent OS book. Eg. (**OSC10**) Silberschatz et. al.: **Operating System Concepts**, 10<sup>th</sup> Edition, 2018.
- ☐ Encode your **QRC** with size upto 7cm x 7cm (ca. 400x400 pixels):  
"OS191 CLASS ID SSO-ACCOUNT Your-Full-Name"
- ☐ Write your Memo (with QRC) **every week**.
- ☐ Login to badak.cs.ui.ac.id via kawung.cs.ui.ac.id for at least **10 minutes** every week. Copy the weekly demo files to your own home directory.  
Eg. (Week00): `cp -r /extra/Week00/W00-demos/ W00-demos/`

# Agenda

- 1 Start
- 2 Jadwal
- 3 Schedule
- 4 Agenda
- 5 Week 02
- 6 Week 02: Protection, Security, Privacy, & C-language
- 7 The Security Problem
- 8 Protection
- 9 Privacy
- 10 C Language
- 11 Week 02: Summary
- 12 Week 02: Check List
- 13 The End

# Week 02 Security & Protection: Topics<sup>1</sup>

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

---

<sup>1</sup>Source: ACM IEEE CS Curricula 2013

# Week 02 Security & Protection: Learning Outcomes<sup>1</sup>

- 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]

---

<sup>1</sup>Source: ACM IEEE CS Curricula 2013

# Week 02: Protection, Security, Privacy, & C-language



(c) 2017 VauLSMorg – This is a free picture

Figure: How to protect and secure this design?

# The Security Problem

- Program, System, and Network Threats
  - Security Hole: Code Review
  - Principle of least privilege
- 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, Application, Operating System, Network.
- 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).



# The Security Problem (cont)

- 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  | <b>Read</b> |        |

- Owner Rights

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

- 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.

- 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.

- ☐ **How to improve this document?**

# The End

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