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

Rahmat M. Samik-Ibrahim

University of Indonesia

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

REV176 26-Dec-2018

# Operating Systems 2018-2 (Room 3114)
# R/M (Tu/Th 13-15) | I (Tu/Th 15-17)

| Week | Schedule | Topic | OSC10 |
|---|---|---|---|
| Week 00 | 04 Sep - 12 Sep 2018 | Overview 1, Virtualization & Scripting | Ch. 1, 2, 18. |
| Week 01 | 13 Sep - 19 Sep 2018 | Overview 2, Virtualization & Scripting | Ch. 1, 2, 18. |
| Week 02 | 20 Sep - 26 Sep 2018 | Security, Protection, Privacy, & C-language | Ch. 16, 17 |
| Week 03 | 27 Sep - 03 Oct 2018 | File System & FUSE | Ch. 13, 14, 15 |
| Week 04 | 04 Oct - 10 Oct 2018 | Addressing, Shared Lib, & Pointer | Ch. 9 |
| Week 05 | 11 Oct - 17 Oct 2018 | Virtual Memory | Ch. 10 |
| Reserved | 18 Oct - 19 Oct 2018 | | |
| Mid-Term | 24 Oct 2018 | MidTerm (UTS): 09:00 - 11:30 | |
| Week 06 | 30 Oct - 05 Nov 2018 | Concurency: Processes & Threads | Ch. 3, 4 |
| Week 07 | 06 Nov - 12 Nov 2018 | Synchronization & Deadlock | Ch. 6, 7, 8 |
| Week 08 | 13 Nov - 21 Nov 2018 | Scheduling | Ch. 5 |
| Week 09 | 22 Nov - 28 Nov 2018 | Storage, BIOS, Loader, & Systemd | Ch. 11 |
| Week 10 | 29 Nov - 05 Dec 2018 | I/O & Programming | Ch. 12 |
| Reserved | 06 Dec - 14 Dec 2018 | | |
| Final | 19 Dec 2018 | Final (UAS): 09:00 - 11:00 | This schedule is |
| Extra | 4 Jan 2019 | Extra assignment confirmation | subject to change. |

# 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/`
  - **Problems** — `rms46.vlsm.org/2/195.pdf`, `196.pdf`, ..., `205.pdf`
- **Text Book**: any recent/decent OS book. Eg. (**OSC10**) Silberschatz et. al.: **Operating System Concepts**, $10^{th}$ Edition, 2018.
- Encode your **QRC** with size upto 7cm x 7cm (ca. 400x400 pixels): **"OS182 CLASS ID SSO-ACCOUNT Your-Full-Name"**
- For **Week 00**, send your **embedded** QRC **before the** $2^{nd}$ **lecture**
  `mailto:operatingsystems@vlsm.org`
  With Subject: `OS182 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

# Week 02 Security & Protection: Topics[1]

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

[1] Source: ACM IEEE CS Curricula 2013

# Week 02 Security & Protection: Learning Outcomes[1]

- 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

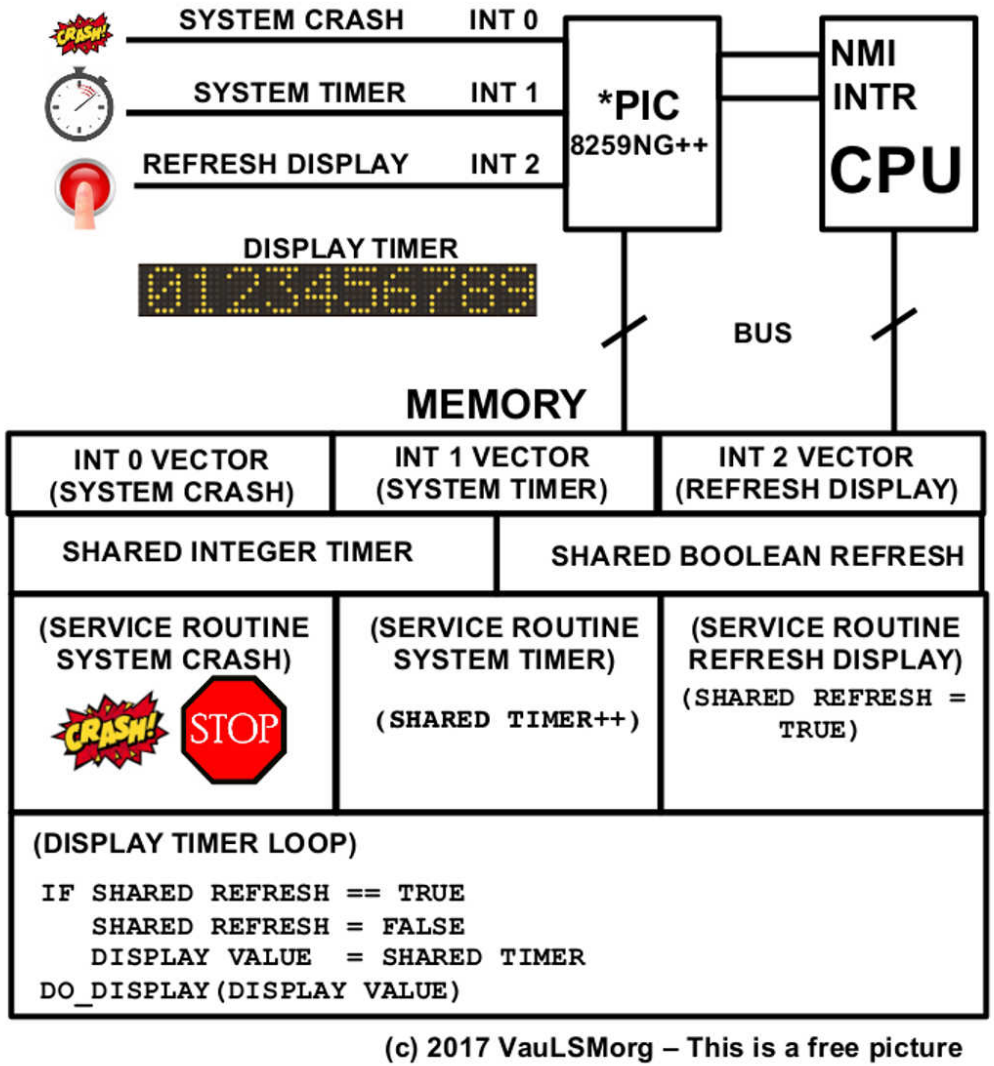


Figure: How to protect and secure this design?

# The Security Problem

- 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 | **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.

# C Language

- 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: Check List

- [ ] **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.