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/Slides/os02.pdf
Always check for the latest revision!

REV351 03-Oct-2021

OS212[4]): Operating Systems 2021 - 2

OS A	OS B	OS C	OS INT
Every first day of the Week, **Quiz#1:** (07:40-07:50) and **Quiz#2:** 07:20-07:40			
Monday/Thursday 13:00 — 14:40 14:00 — finish	Monday/Thursday 15:00 — 16:40[1] 16:00 — finish	Monday/Thursday 13:00 — 14:40 13:00 — 14:40	Monday/Wednesday 08:00 — 09:40 09:00 — finish

Week	**Schedule & Deadline[2])**	**Topic**	**OSC10[3])**
Week 00	30 Aug - 05 Sep 2021	Overview 1, Virtualization & Scripting	Ch. 1, 2, 18.
Week 01	06 Sep - 12 Sep 2021	Overview 2, Virtualization & Scripting	Ch. 1, 2, 18.
Week 02	13 Sep - 19 Sep 2021	Security, Protection, Privacy, & C-language.	Ch. 16, 17.
Week 03	20 Sep - 26 Sep 2021	File System & FUSE	Ch. 13, 14, 15.
Week 04	27 Sep - 03 Oct 2021	Addressing, Shared Lib, & Pointer	Ch. 9.
Week 05	04 Oct - 10 Oct 2021	Virtual Memory	Ch. 10.
Week 06	11 Oct - 17 Oct 2021	Concurrency: Processes & Threads	Ch. 3, 4.
Week 07	01 Nov - 07 Nov 2021	Synchronization & Deadlock	Ch. 6, 7, 8.
Week 08	08 Nov - 14 Nov 2021	Scheduling + W06/W07	Ch. 5.
Week 09	15 Nov - 21 Nov 2021	Storage, Firmware, Bootloader, & Systemd	Ch. 11.
Week 10	22 Nov - 28 Nov 2021	I/O & Programming	Ch. 12.

[1]) **OS B:** Week00-Week05 (RMS); Week06-Week10 (MAM).

[2]) The **DEADLINE** of Week 00 is 05 Sep 2021, whereas the **DEADLINE** of Week 01 is 12 Sep 2021, and so on...

[3]) Silberschatz et. al.: **Operating System Concepts**, 10^{th} Edition, 2018.

[4]) 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**, 10^{th} Edition, 2018. See also https://www.os-book.com/OS10/.
- **Resources**
  - **SCELE OS212** — https://scele.cs.ui.ac.id/course/view.php?id=3268. 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** 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

Week 02 Security & Protection: Topics[1]

- Overview of system security
- Cyber Security Introduction
- Policy/mechanism separation
- Security methods and devices
- Protection, access control, and authentication
- Backups
- Safety and Privacy
- Threads
- Cryptography: (Symmetric and Asymmetric) Encryption,
- C Language

[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

Cyber Security Introduction

Visit:

- https://youtu.be/rcDO8km6R6c
- https://youtu.be/CivG_2UqKMg (culture part).
  - Point of Cybersecurity
  - Good Administration
  - Zero Trust Environment
  - Succesful Security Attack
  - Potential Security Threats
  - Security Problems
  - Disaster Recovery
  - Employee Security Policy
  - Culture

Protection & Security Design

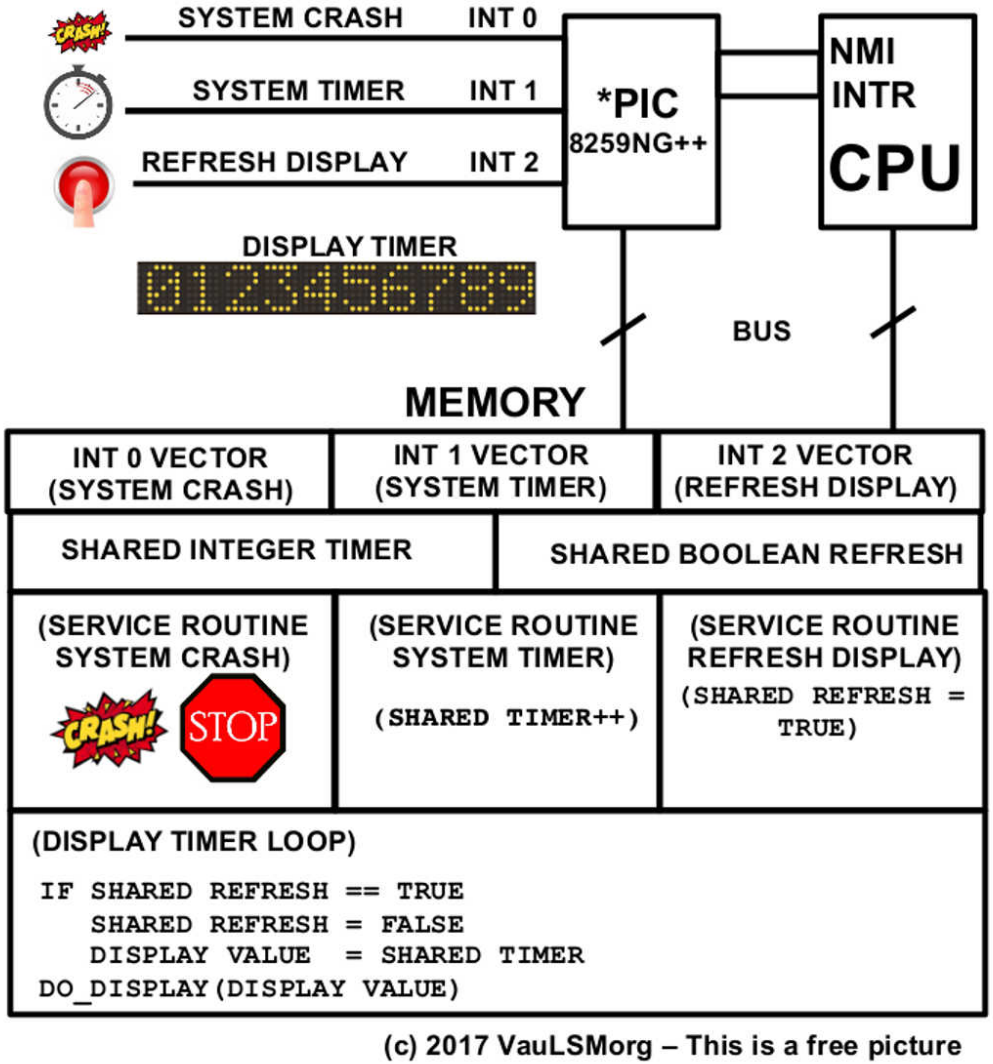

Figure: How to protect and secure this design?

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

C Language

- Reference: (Any C Language Tutorial)
- Visit https://github.com/UI-FASILKOM-OS/SistemOperasi/tree/master/Demos/Week02/c-language

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 (Deadline: 19 Sep 2021).

- Week 02: Assignment (**os02.pdf**). (Eg. **cbkadal**).
  - Visit https://osp4diss.vlsm.org/#idx07
    1. Read OSC10 chapter 16 + chapter 17
    2. Try Demos in https://github.com/UI-FASILKOM-OS/SistemOperasi/tree/master/Demos/.
    3. Watch: Cyber Security Introduction part 1 and the begining of part 2.
    4. Generate a GnuPG Key Pair https://osp4diss.vlsm.org/CBKadal2.html.
    5. List of all GnuPG Keys https://osp4diss.vlsm.org/W02-01.html.
    6. Importing **ospubkey.txt Key** from https://osp4diss.vlsm.org/W02-02.html.
    7. Signing the Operating Systems public key (Optional).
    8. Export **YOUR PUBLIC KEY** to your repo file "TXT/mypubkey.txt".
    9. Update your bookmark links. See C.B. Kadal's "LINKS/"
    10. Review your peer links.
    11. Write (or copy) a simple and useful `bash` script (https://cbkadal.github.io/os212/TXT/myscript.sh).
    12. Update your log. See C.B. Kadal's "mylog.txt"
    13. Run "myscript.sh" script to generate SHA256SUM and SHA256SUM.asc.

The End

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