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!

REV217 04-Feb-2020

Operating Systems 2020-1

A [08-10, Rm 3114, Mo/We] — B/M [10:10-12, Rm 3114, Mo/We] — C [13-15, Rm 3114, Mo/We]

D [10-12, Rm 2307(Mo), Rm 3113(We)] — E [08-10, Rm 2307(Mo), Rm 3113(We)]

Week	Schedule	Topic	OSC10
Week 00	27 Jan - 02 Feb 2020	Overview 1, Virtualization & Scripting	Ch. 1, 2, 18.
Week 01	03 Feb - 09 Feb 2020	Overview 2, Virtualization & Scripting	Ch. 1, 2, 18.
Week 02	10 Feb - 16 Feb 2020	Security, Protection, Privacy, & C-language	Ch. 16, 17
Week 03	17 Feb - 23 Feb 2020	File System & FUSE	Ch. 13, 14, 15
Week 04	24 Feb - 01 Mar 2020	Addressing, Shared Lib, & Pointer	Ch. 9
Week 05	02 Mar - 08 Mar 2020	Virtual Memory	Ch. 10
Reserved	09 Mar - 13 Mar 2020	Q & E	
MidTerm	14-21 Mar 2020 (TBA)	MidTerm (UTS)	Subject to change.
Week 06	23 Mar - 31 Mar 2020	Concurrency: Processes & Threads	Ch. 3, 4
Week 07	01 Apr - 07 Apr 2020	Synchronization & Deadlock	Ch. 6, 7, 8
Week 08	08 Apr - 14 Apr 2020	Scheduling + W06/W07	Ch. 5
Week 09a	15 Apr - 19 Apr 2020	Storage, Firmware, Bootldr, & Systemd	Ch. 11
OCL	20 Apr - 26 Apr 2020	OnLine & CoLearnIng	
Week 09b	27 Apr - 28 Apr 2020	Storage, Firmware, Bootldr, & Systemd	Ch. 11
Week 10	29 Apr - 05 May 2020	I/O & Programming	Ch. 12
Reserved	06 May - 10 May 2020	Q & A	
Final	11-18 May 2020 (TBA)	Final (UAS)	This schedule is subject to change.
Extra	25 Jun 2020	Extra assignment confirmation	

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 http://codex.cs.yale.edu/avi/os-book/OS10/.
- **Resources**
  - **All In One** — BADAK.cs.ui.ac.id:///extra/ (**FASILKOM only!**).
  - **Download Slides and Demos from GitHub.com** https://github.com/UI-FASILKOM-OS/SistemOperasi/
  - **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).
- **Try Demos**
  - Your own Ubuntu system.
  - Ubuntu on VirtualBox, or VMWare, or ...
  - Windows Subsystem for Linux (**Windows 10 only!**).
  - SSH to BADAK.cs.ui.ac.id (**FASILKOM only!**).

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

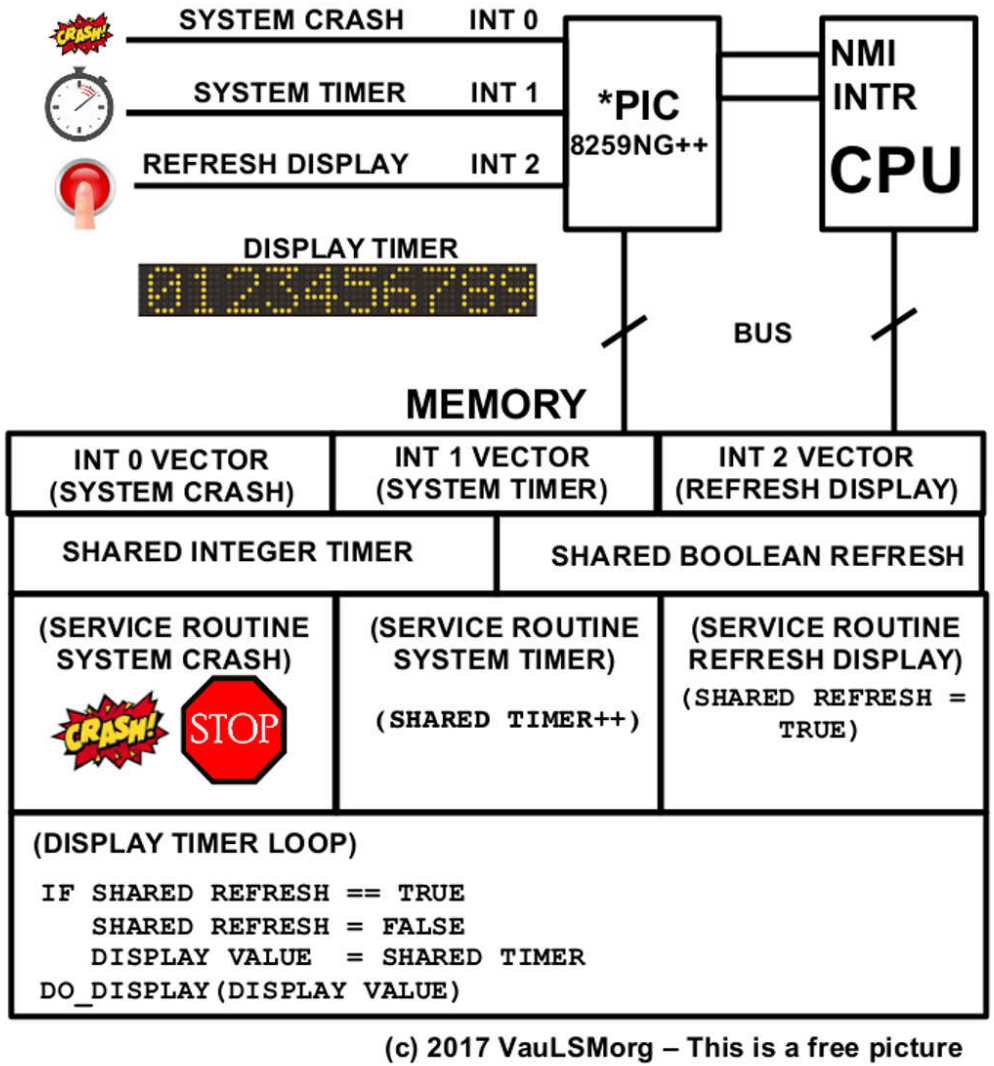

Figure: How to protect and secure this design?

The Security Problem

- **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)

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.