

CSGE602055 Operating Systems

CSF2600505 Sistem Operasi

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

C. BinKadal

Sendirian Berhad

<https://docos.vlsm.org/Slides/os02.pdf>

Always check for the latest revision!

REV421: Tue 27 Aug 2024 12:00

OS242³): Operating Systems Schedule 2024 - 2

Week	Topic ¹⁾	OSC10 ²⁾
Week 00	Overview (1), Assignment of Week 00	Ch. 1, 2
Week 01	Overview (2), Virtualization & Scripting	Ch. 1, 2, 18.
Week 02	Security, Protection, Privacy, & C-language.	Ch. 16, 17.
Week 03	File System & FUSE	Ch. 13, 14, 15.
Week 04	Addressing, Shared Lib, & Pointer	Ch. 9.
Week 05	Virtual Memory	Ch. 10.
Week 06	Concurrency: Processes & Threads	Ch. 3, 4.
Week 07	Synchronization & Deadlock	Ch. 6, 7, 8.
Week 08	Scheduling + W06/W07	Ch. 5.
Week 09	Storage, Firmware, Bootloader, & Systemd	Ch. 11.
Week 10	I/O & Programming	Ch. 12.

¹⁾ For schedule, see <https://os.vlsm.org/#idx02>

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 <https://codex.cs.yale.edu/avi/os-book/OS10/>).
- ☐ **Resources** (<https://os.vlsm.org/#idx03>)
 - ☐ **SCELE** — <https://scele.cs.ui.ac.id/course/view.php?id=3841>.
The enrollment key is **XXX**.
 - ☐ **Download Slides and Demos from GitHub.com** —
(<https://github.com/os2xx/docos/>)
[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/>
 - ☐ **This is How Me Do It!** — <https://doit.vlsm.org/>
 - ☐ PS: "Me" rhymes better than "I", duh!

Agenda

- 1 Start
- 2 OS242 Schedule
- 3 Agenda
- 4 Week 02 Security & Protection
- 5 OSC10 (Silberschatz) Chapter 16 and 17
- 6 Cyber Security Resources
- 7 Protection & Security Design
- 8 The Security Problem
- 9 Protection
- 10 Privacy
- 11 C Language
- 12 Week 02: Summary
- 13 The End

Week 02 Security & Protection: Topics¹

- 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

¹Source: ACM IEEE CS Curricula

Week 02 Security & Protection: Learning Outcomes¹

- 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]

¹Source: ACM IEEE CS Curricula

- OSC10 Chapter 16

- The Security Problem
- Program Threats
- System and Network Threats
- Cryptography as a Security Tool
- User Authentication
- Implementing Security Defenses
- Firewalling to Protect Systems and Networks
- Computer-Security Classifications
- An Example: Windows 7

- OSC10 Chapter 17

- Goals of Protection
- Principles of Protection
- Protection Rings
- Domain of Protection
- Access Matrix
- Implementation of Access Matrix
- Revocation of Access Rights
- Role-based Access Control
- Mandatory Access Control (MAC)
- Capability-Based Systems
- Other Protection Implementation Methods
- Language-based Protection

Cyber Security Cases for Beginner (Resource I)

- CrowdStrike Exposes a Fundamental Problem in Software
 - CrowdStrike recently highlighted a significant issue within software management after a major update failure in their Falcon platform, a cloud-based endpoint protection service. The update, meant to enhance security, inadvertently caused widespread system crashes, particularly blue screens of death on Windows devices.
 - <https://youtu.be/UdJr2p5RrF0>
- LockBit, World's #1 Cyber Criminals (An Inside Look)
 - LockBit operates on a "Ransomware-as-a-Service" (RaaS) model, developing and maintaining the ransomware while affiliates deploy it. The group has extorted hundreds of millions in cryptocurrency from victims, making it a significant threat in the cybersecurity landscape.
 - <https://youtu.be/0EQenbbPSaE>
- Chinese Banks Leaked, VPN Bypass, Apple AI Chip
 - This video shows a variety of cybersecurity news.
 - <https://youtu.be/--MLH0MaqUA>

Cyber Security Full Course for Beginner (Resource II)

- Visit:
 - https://youtu.be/U_P23SqJaDc
- Points:
 - Why Study Cyber Security
 - Cyber Security Terminology
 - Demystifying Computers and the Internet
 - Passwords
 - Email
 - Malware
 - Web Browser
 - Wireless Network
 - Social Media, Security, and Privacy

Cyber Security Introduction (Resource III)

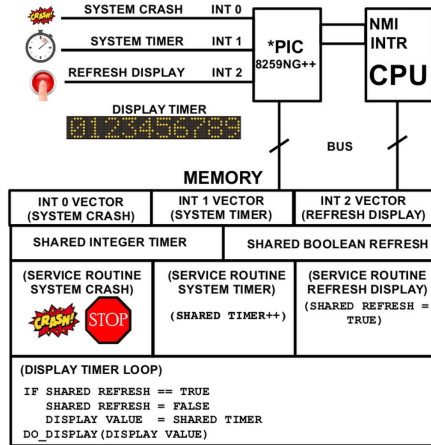
- Visit:

- <https://youtu.be/rcD08km6R6c>
- https://youtu.be/CivG_2UqKMg (first 30 minutes).

- Points:

- Point of Cybersecurity
- Good Administration
- Zero Trust Environment
- Successful Security Attack
- Potential Security Threats
- Security Problems
- Disaster Recovery
- Employee Security Policy
- Corporate Culture

Protection & Security Design



(c) 2017 VauLSMorg – This is a free picture

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, Assessment, 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 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

- The Beginner's Guide to Digital Privacy — [YouTube](#).
- The Beginner's Guide To Online Privacy — [LINK](#).
- The Beginner's Guide To Internet Safety and 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)
- Visit <https://github.com/os2xx/demOS/tree/master/Demos/>

Week 02: Summary

- Reference: OSC10 chapter 16, 17.
- 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, Assessment, Prevention, Detection, Protection, Auditing.
- Privacy.

The End

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