


Introduction to the Course

CS-604 : Advanced System Security
Autumn 2024

Deepti Vidyarthi
Assistant Professor, SoCE&MS

Outline

- What will we learn?
- Prerequisites, Syllabus
- Hands-on
- Organization of the course
- Security Threats
- System Security – OS Security Intro
- Security Goals, Threat Model, Trust Model
- Access Control – Defn, Lampson Access Matrix
- References

What will we learn?

- Why is the traditional security mechanism insufficient today?
- How are the processes are separated?
- How do processes run at different privilege levels?
- Can we make memory attacks harder?
- How can the operating-systems be hardened?
  - Enforcing mandatory access control
  - Compartmentalization and virtualization

What will we learn?

- Theoretical concepts of operating system security
- Security architectures of current Operating Systems
- Details of security implementation
- Concept of virtualization, Security mechanisms in virtual machines
- Syllabus

Prerequisites

- Basics of Operating System
  - Processes & threads
  - Memory management
- Linux shell scripting commands
- Web Sources:
  - https://codex.cs.yale.edu/avi/courses/CS-423/slides/index.html
  - https://www.tutorialspoint.com/unix/unix-useful-commands.htm

Hands-on

- Lab Requirements:
  - Virtual environments: VMWare Workstation / Oracle VirtualBox
  - Windows Systinternals
  - Kali Linux
  - LSM by SELinux

(will share sources for VM instances with required tools)

Organization of the course

- Classroom interaction + Reading assignments + Lab work + Paper discussion

Assessment	Marks	Weightage (%)
Test (Three tests one per month)	10 x 3	30
Internal (Lab-work + Research paper study & presentation)	20	20
End semester examination	50	50

Note: Reading assignments are essential to fulfill the pre-requisites & understand classroom sessions more clearly.

Security Threats

Malware attacks rose 53% in India in 2018: SonicWall

Ransomware attacks were up in every geography except India and the UK, showed the findings based on an analysis 3.9 trillion malicious events in over 215 countries.

IANS | Mar 28, 2019, 04.37 PM IST

Save

0 Comments

A+

BCCL

While ransomware attacks were down 49 per cent in India in 2018, the country experienced 53 per cent rise in malware attacks last year, according to a new report from cybersecurity firm SonicWall.

Ref: Economics Times article, Mar28, 2019

150 computers at Maharashtra Mantralaya attacked by Locky virus

The 150 computers will be subjected to forensic tests.

By: Express News Service | Mumbai | Updated: May 26, 2016 6:53 pm

At l
gov
which blocks access to computers, [illegible] targeted files from the

Ref: Indian Express article, May26, 2016

Kia Motors

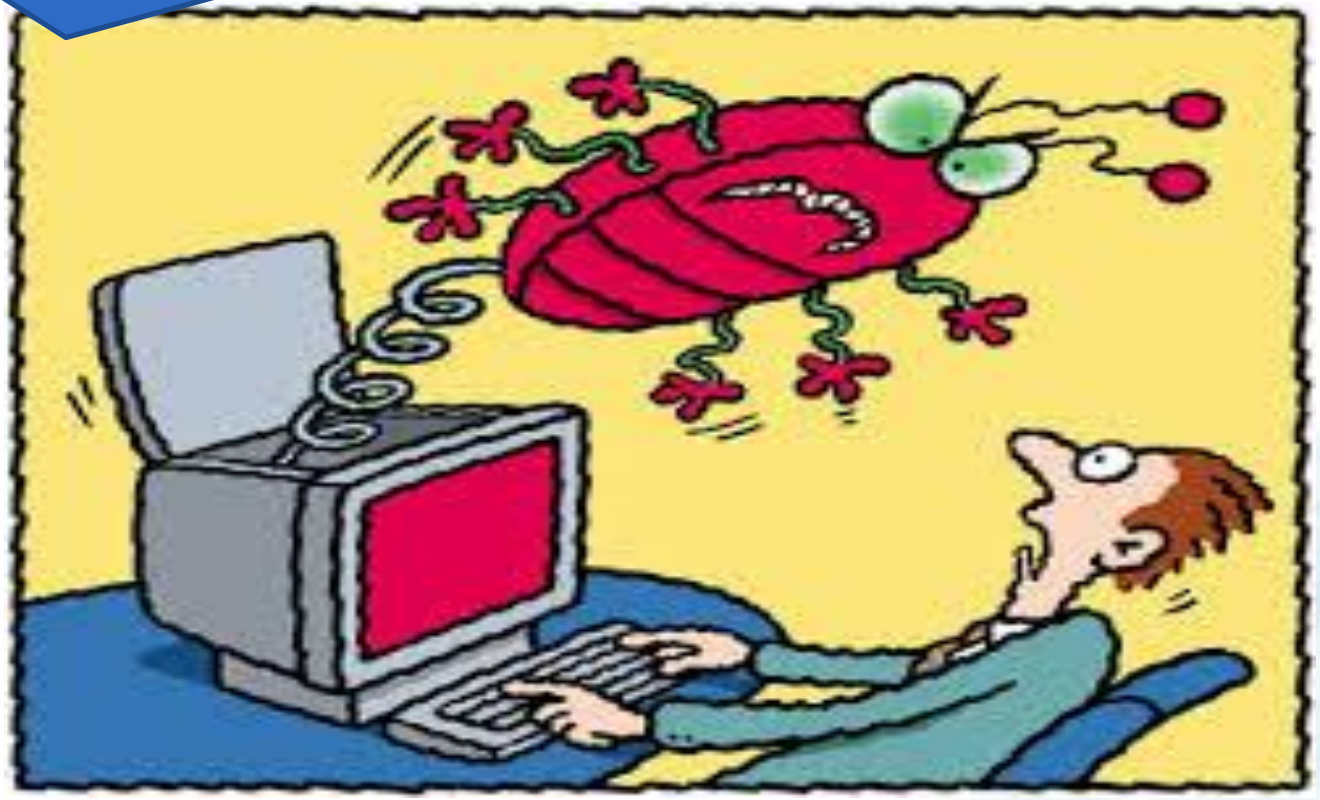
A subsidiary of Hyundai, Kia Motors, suffered ransom in February this year. Attackers DopplePaymer gang reportedly asked for $20 million for a decrypter and not leak the stolen data. As claimed by Kia Motors, the subsequent 'IT outage' affected the mobile UVO Link apps, payment systems, owner's portal, phone services, and internal sites used by Kia Motors America.

While these were global attacks, India isn't far from making headlines for cybersecurity breaches, either. **If one were to go by media reports, India was most hit by ransomware attacks this year, so far. A report by Check Point research suggests that with ransomware attacks shot up by 102 per cent globally in 2021 from last year, India was the worst hit with 213 weekly ransomware attacks per organisation.** Last year, Microsoft appointed a Threat Protection Intelligence Team to deal with the attacks.

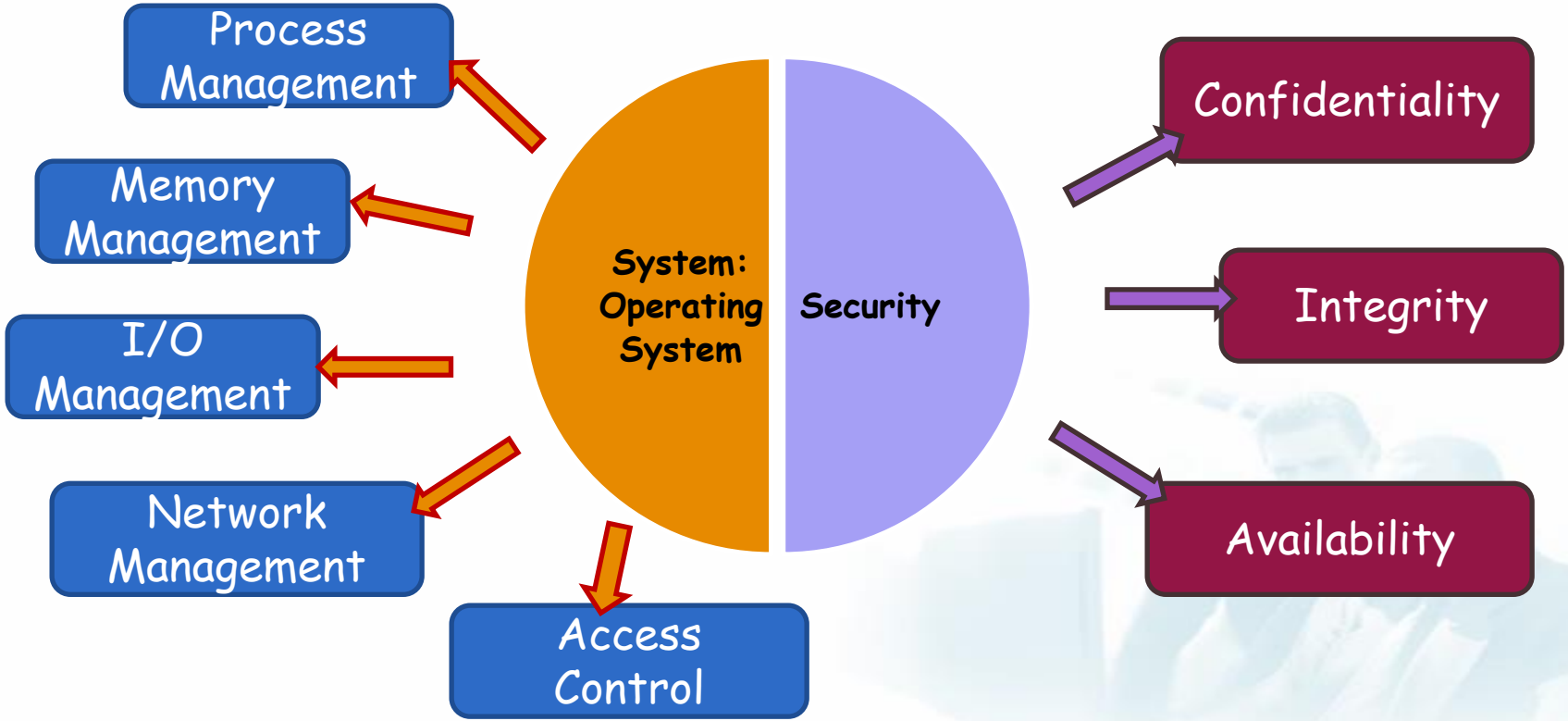
Ref: https://analyticsindiamag.com/5-ransomware-attacks-of-2021-that-blew-the-internet, 26/08/2021


You became victim of the PETYA RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://pety .onion/g
http://pety .onion/g
3. Enter your personal decryption code there:
a6
nF y1
If you already purchased your key, please enter it below.
Key: _

Caught unaware?



System Security



System Security

1. Security goals / requirement
2. Threats Model.
3. Trust

Godrej — 7 levers → Trust.

Secure Operating System

Secure Operating System

- *Provides security mechanisms that ensure that the system's security goals are enforced by trusted components despite threats from attackers.*

- Building any secure system must consider
  - how the system achieves its security goals
  - under a set of threats (i.e., a threat model)
  - given a set of software, including the security mechanisms, that must be trusted (i.e., a trust model).

Security Goals

- Lots of unsatisfying definitions
  - Users can perform only authorized operations (safety)
  - Processes perform only their necessary operations (least privilege)
  - Operations can only permit information to be written to more secret levels (MLS)
- Defining practical and effective security goals is a difficult task

Security Goals

- Define the operations that

  can be executed by a system while still preventing unauthorized access
- Define requirement that the system's design can satisfy
- Defined at a high-level of abstraction

- Describe how system implements accesses to system resources to satisfy the security goals- safety – least privilege – MLS → (*secrecy/ integrity/availability)*

Security Goals

- A system access is stated in terms of:

- which **subjects** (e.g., processes and users)
- can perform which **operations** (e.g., read and write)
- on which **objects** (e.g., files and sockets)

Security Goals

Examples of goal defined:

- *simple-security property of the Bell-LaPadula model*

  This goal states that a process cannot read an object whose secrecy classification is higher than the process's.

- *principle of least privilege*

  It limits a process to only the set of operations necessary for its execution.

Trust Model

- Set of software and data

  Upon which the system depends for correct enforcement of system security goals

security - sensitive operations.

- For Operating system

  Trust model = system's trusted computing base (TCB)

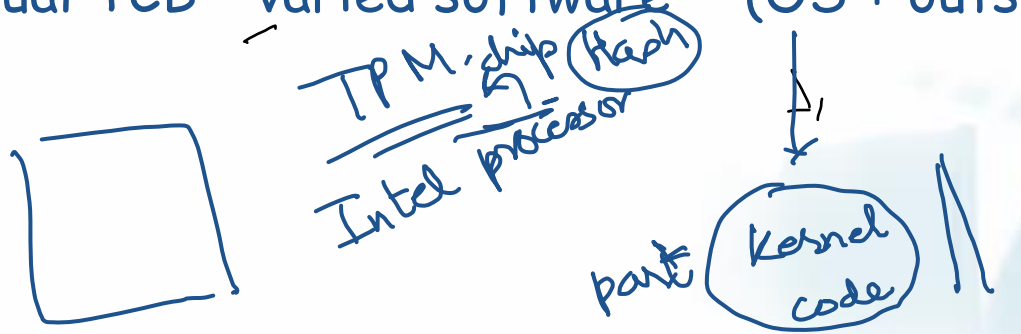
  TCB - minimal amount of software necessary to enforce the security goals correctly

OS code + admin level apps.

Trust Model

- Ideal TCB - bootstrapping mechanism (enabling the security goals to be loaded and enforced)

- Actual TCB – varied software - (OS + outside) code



Trust Model

- Secure OS developer must prove that their systems have a viable trust model

(1) System TCB must mediate all security-sensitive operations

(2) Verification of the correctness of the TCB software and its data

(3) Verification that the software's execution cannot be tampered by processes outside the TCB.

Threat Model

- Set of operations - used to compromise a system
- Attacker can find vulnerability in system
- Provide access to secret information or permits the modification of information
- Get control of a process running on the system

Threat Model

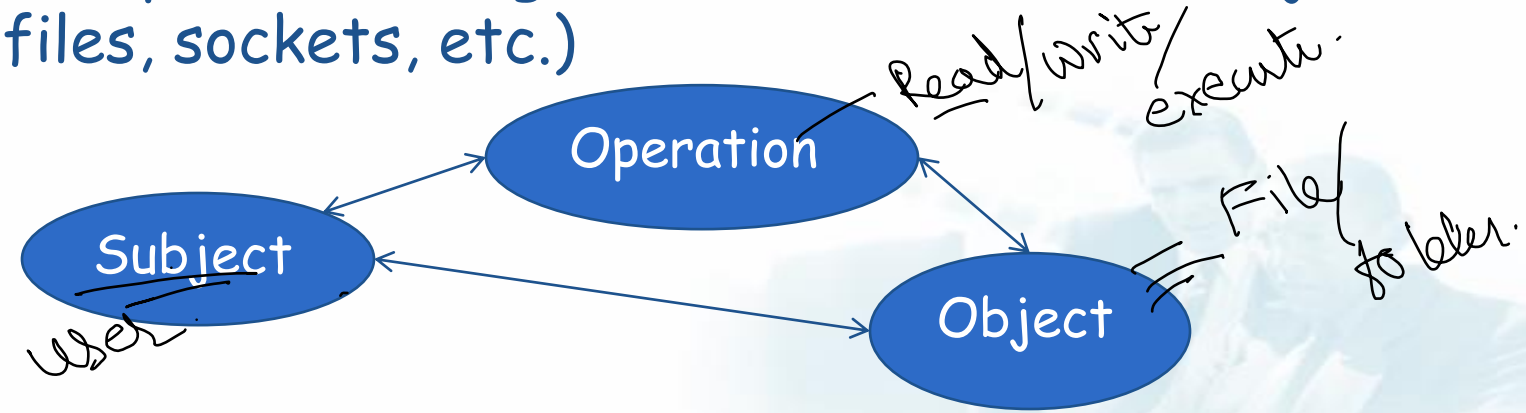
- Cannot trust processes outside of the TCB to behave as expected
- Protecting the TCB:
  - system security goals will always be enforced regardless of the behaviour of user processes
- Restricting user process:
  - Prevent a user process from leaking secret data by limiting interactions of that process

Memory Access

- All access to resources is handled through file-access permissions - through system calls
- Cannot do that for reading/writing memory
- Load/store instructions are very frequent in programs
- OS still needs control over memory access of processes!

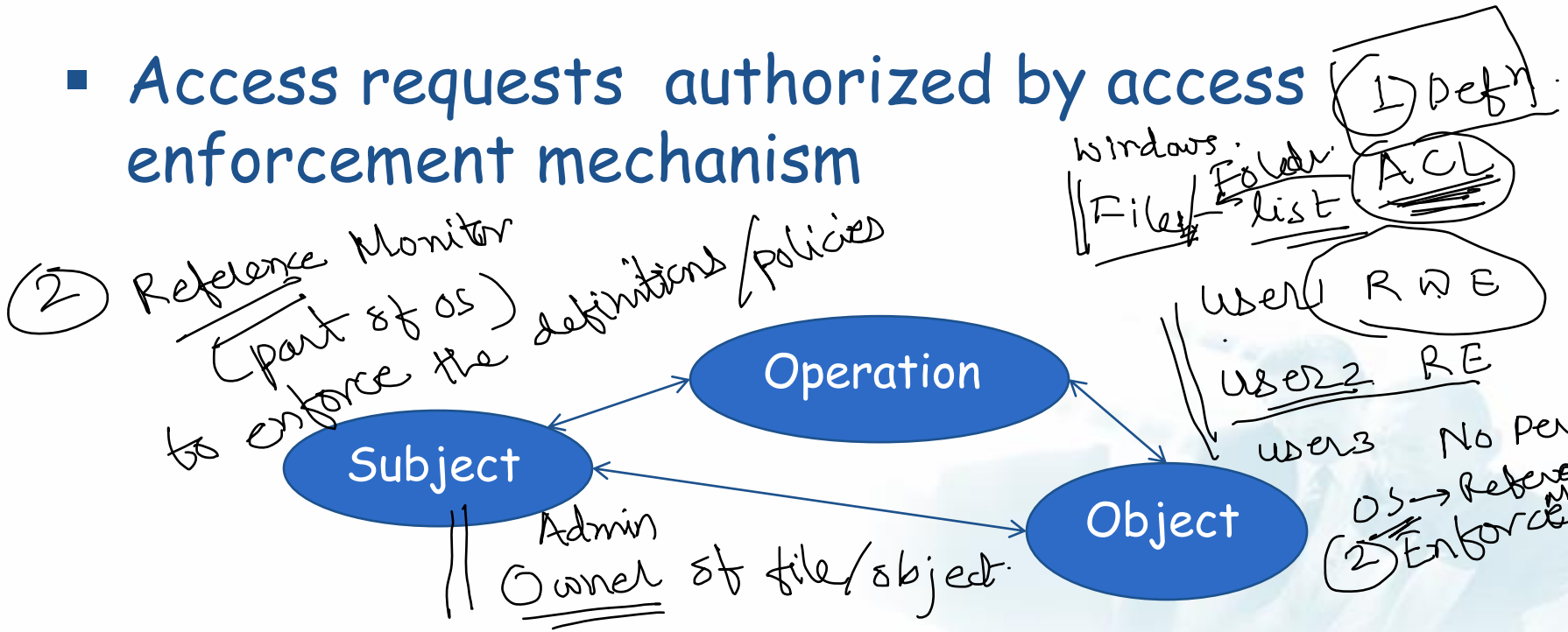
Access

- Access requests - Requests (e.g., system calls) from multiple subjects (e.g., users, processes, etc.) to perform operations (e.g., read, write, etc.) on objects (e.g., files, sockets, etc.)

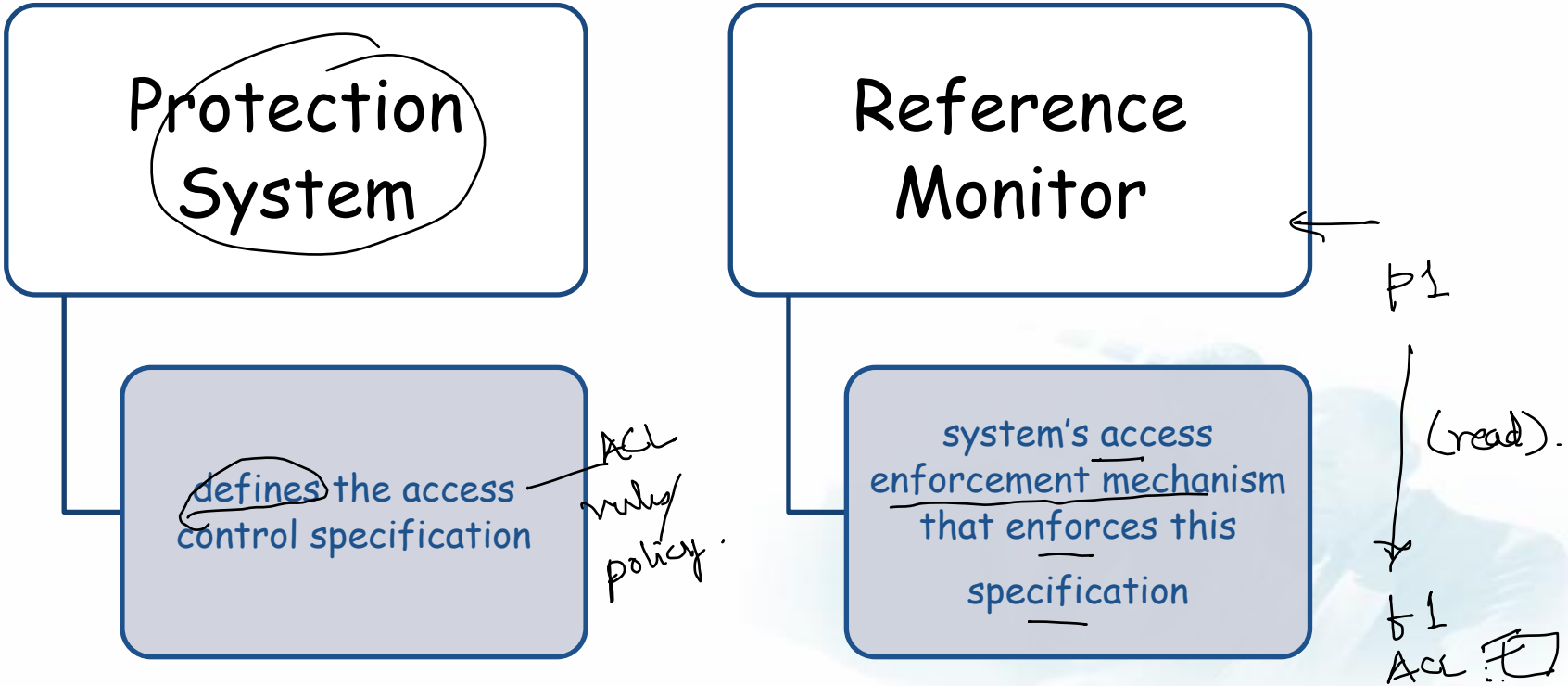


Access Control

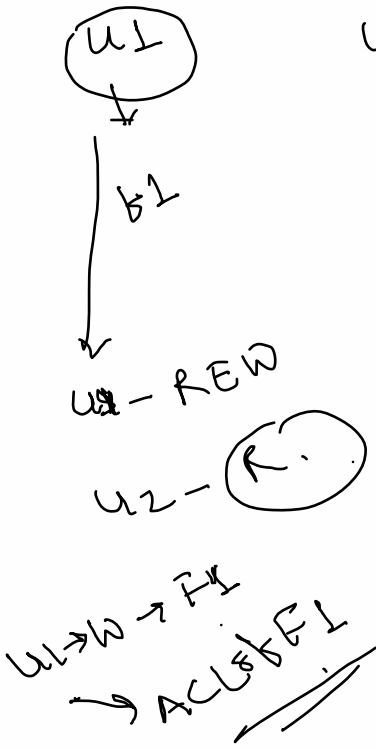
- Access requests authorized by access enforcement mechanism

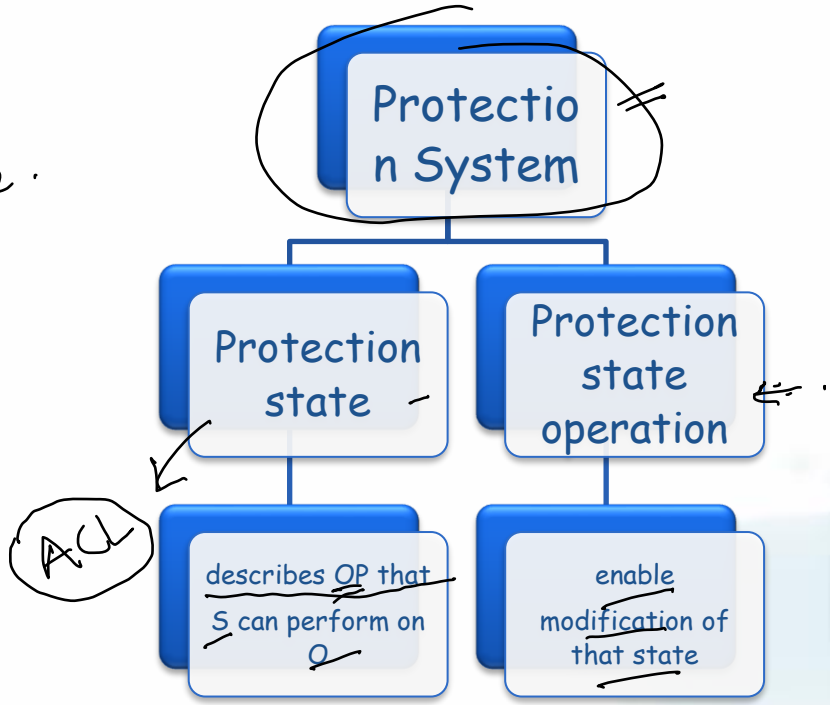


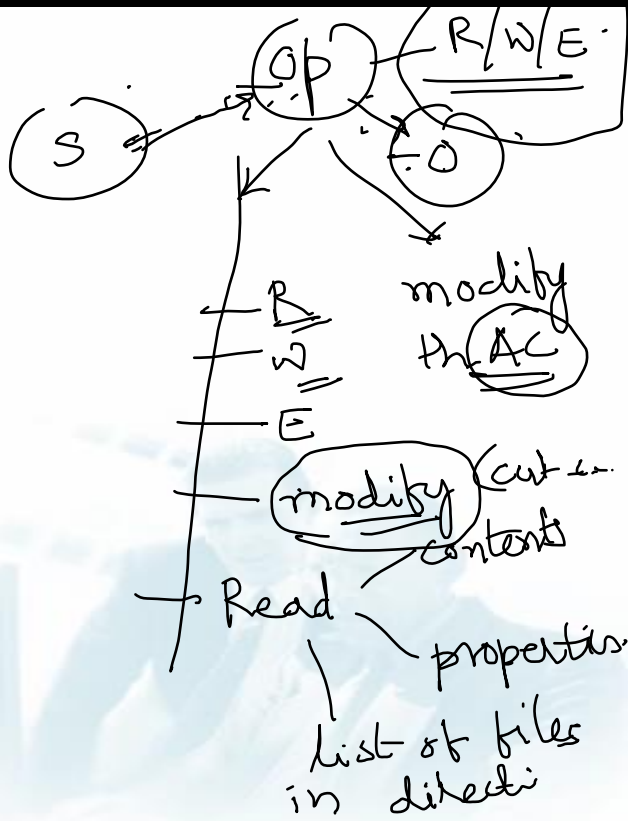
Access Control



Protection System







Lampson Access Matrix

- set of subjects $s \in S$
- set of objects $o \in O$
- set of operations $op \in OP$
- function $ops(s, o) \subseteq OP$

  The function ops(s, o) is said to return a set of operations corresponding to cell (s, o)

Lampson Access Matrix

Protection domain –

- Set of resources (objects) that process can access and the operations that process may use to access such resources
- Rows in Access Matrix
- For a secure OS, we need assurance that protection domain of each process satisfies system Secrecy & Integrity

Lampson Access Matrix

Representations:

- Problem with matrix?

- Access control list or ACL: protection state using individual object columns

- Capability list or C-List: objects that a particular subject can access are stored

Safety Problem

A Matrix → Lampson.

Problem?

- Using protection state operations, untrusted user processes can modify the access matrix by adding new subjects, objects, or operations assigned to cells
- Permits untrusted processes to modify the protection state - discretionary access control (DAC) system
- Protection System is at discretion of users & processes

Future states → may be unsafe.

Safety Problem

- To ensure that a protection state & all possible future protection states derivable – provide no unauthorized access
- Undecidable for protection systems with compound protection state operations
- One process is protected only if all behave benignly

Safety Problem

Secrecy & Integrity

	File 1	File 2	File 3	Process 1	Process 2
Process 1	Read	Read, Write	Read, Write	Read	-
Process 2	-	Read	Read, Write	-	Read

- Process 1 is non-malicious
- Process 1 is malicious
- Process 1 is non-malicious but has interface with Process 2 and is vulnerable

Safety Problem

- Security: where a system's security mechanisms can enforce system security goals even when any of the software outside the trusted computing base may be malicious
- Protection state must be defined based on accurate identification of the secrecy and integrity of user data and processes
- No untrusted processes may be allowed to perform protection state operations

References

Books:

1. **Jaeger, T., "Operating System Security", Morgan & Claypool (online), 2008. as Textbook.**
2. Morrie Gasser, "Building a Secure Computer System".
3. Silberschatz and Galvin: "Operating System Concepts", Addison Wesley, 2006.

- Research papers and tutorials would be shared on the fly.


Homework

Basic Security in Windows/Linux/Android

- Does your system's OS provide access control?
- How does is allow access control for multiple users?
- Can you change permission to access- read/write any file?

Research Challenges

- Foolproof Security
- Security VS User Friendliness
- Security VS Performance

Thank You!