# SC3010
# Computer Security

## Lecture 6: Operating System Security (II)

# Outline

- **Protection Strategies**
  - Confinement
  - Reference Monitor
- **Hardware-assisted Protection**
  - Basic Functionalities
  - Trusted Platform Module
  - Trusted Execution Environment

# Outline

- **Protection Strategies**
  - Confinement
  - Reference Monitor
- **Hardware-assisted Protection**
  - Basic Functionalities
  - Trusted Platform Module
  - Trusted Execution Environment

# Confinement

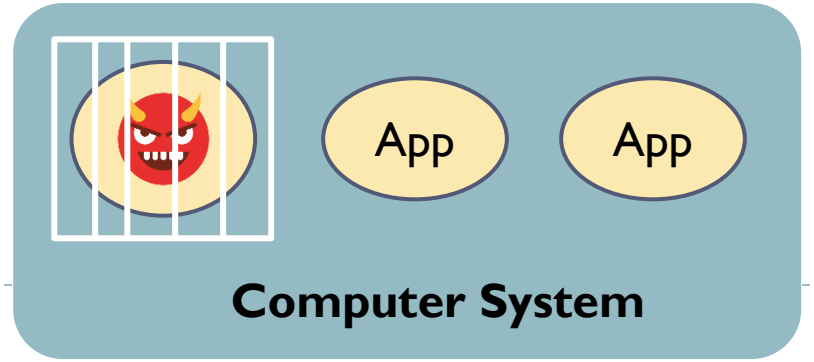
## An important security strategy in OS protection

- When some component (e.g., application) in the system is compromised or malicious, we need to prevent it from harming the rest of system.
- Confinement: restricts the impact of each component on others.
- Follow the principle of least of privilege

## Application scenario

- Cut off the propagation chain.
- Malware testing and analysis

## Can be implemented at different levels



# OS Level Confinement: Virtual Machine

## Virtualization: the fundamental technology for cloud computing

- Different operating systems (virtual machines) run on the same machine
- Each virtual machine has an independent OS, logically isolated from others

## Technical support

- Software layer: hypervisor or virtual machine monitor (VMM) for virtualizing and managing the underlying resources, and enforcing the isolation
- Hardware layer: hardware virtualization extensions (Intel VT-x, AMD-V) for accelerating virtualization and improving performance