

SC3010

Computer Security

Lecture 5: Operating System Security (I)

Security Challenges in Modern OS

From single-user to multi-user

- ▶ DOS is truly single user
- ▶ MacOS, Linux, NT-based Windows are multi-user
- ▶ Cloud computing allows multiple users all over the world to run on the same system, and they do not know each other.
- ▶ **Not all users are trusted!**

From trusted apps to untrusted apps

- ▶ Simple real-time systems: only run one specific app from trusted sources
- ▶ Modern PCs and smartphones: run apps from third-party developers
- ▶ **Not all apps are trusted!**

From standalone systems to networked systems

- ▶ Isolated computer systems only need to protect against physical threats.
- ▶ Once connected to networks, the system faces external unknown threats.
- ▶ **Not all network components are trusted!**

Outline

- ▶ **Security Protection Stages in OS**
 - ▶ Authentication
 - ▶ Authorization with Access Control
 - ▶ Logging, Monitoring & Auditing
- ▶ **Privilege Management in OS**

Outline

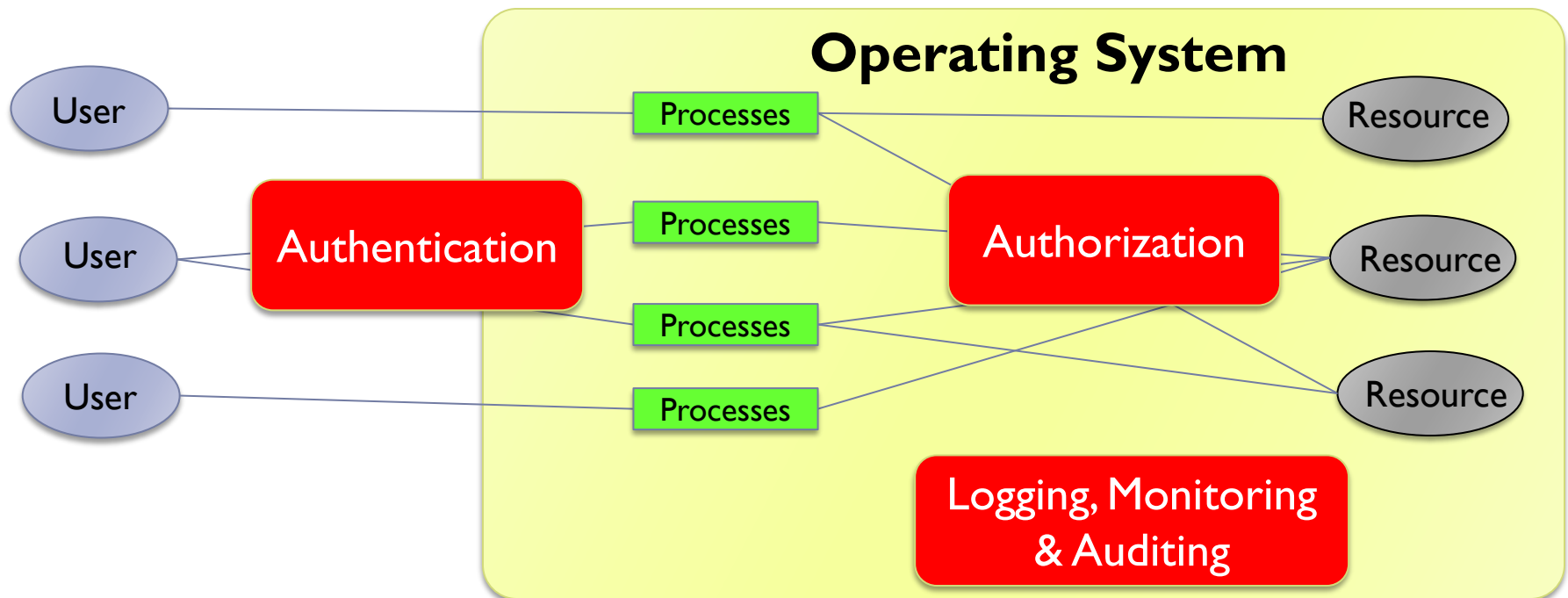
- ▶ **Security Protection Stages in OS**
 - ▶ Authentication
 - ▶ Authorization with Access Control
 - ▶ Logging, Monitoring & Auditing
- ▶ Privilege Management in OS

Security Protection from OS

OS is responsible for protecting the apps and resources inside it.

- ▶ OS controls what users/processes can do
- ▶ OS prevents what users/processes cannot do







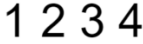


Protection Stages



Authentication

How does a computer know if I am a correct user?

- ▶ **Something you know:** password, PIN, public/private keys...
- ▶ **Something you have:** smartcard, hardware tokens...
- ▶ **Something you are:** biometrics, face recognition, voice recognition...

Knowledge Factor (something you know)	Possession Factor (something you have)	Inherence Factor (something you are)
 Password	 Smartphone	 Fingerprint
 Security Question	 Smart Card	 Retina Pattern
 PIN	 Hardware Token	 Face Recognition

Something You Know: Password

Password is the most common way to prove who you are

- ▶ Adopted by various networking websites and applications
- ▶ The security of the password-based authentication mechanism depends on the strength of the selected password, i.e., the chance attacker can guess the password.
- ▶ The trade-off between the password security and convenience:
 - Weak password is easy to memorize, but also easy to be guessed.
 - Complex password is strong but results in frustrated users



Nanyang Technological University

Sign in with your organizational account

Sign in

Sign in using your network account e.g

- username@staff.main.ntu.edu.sg
- username@student.main.ntu.edu.sg
- username@assoc.main.ntu.edu.sg
- username@niestaff.cluster.nie.edu.sg
- username@niestudent.cluster.nie.edu.sg

Weak Password

A weak password is a character combination that is easy for friends, bad actors or password-hacking software to guess

- ▶ Short passwords: a single word (e.g., password) or numerical phrase (e.g., 12345).
- ▶ Recognizable keystroke patterns: take a look at your keyboard and find QWERTY
- ▶ Personal information in passwords: e.g., date of birth, address, name
- ▶ Repeated letters or numbers: e.g., 55555, aaaa

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856