Computer System Security

ASSOC. PROF. NOHA A. HIKAL

INFORMATION TECHNOLOGY DEPT.

FACULTY OF COMPUTERS AND INFORMATION SCIENCES

SUBJECT CODE:IT424

4TH LEVEL –IT&IS

WEEK 8 - 29 MARCH 2020

Operating System Security

Outlines:

1- General purpose operating system

2- Protection in General-Purpose OS

3- Protected Objects

4- Security Methods of O.S

5- Separation and Sharing

6- Access control

7- User authentication

1-General purpose OS:

1. OS evolved as a way to allow multiple users use the same hardware
2. OS allows different users to access different resources in a shared mannar by some policy
3. OS needs to control this sharing and provide an interface to allow this access
4. OS also protects users from each other

   Attacks, mistakes, resource overconsumption
5. Even for a single-user OS, protecting a user from him/herself is a good thing

2-Protection in General-Purpose OS

OS system has two goals:

- Controlling shared access.
- Implementing an interface to allow that access.

Underneath those goals are support activities:

- Identification and authentication
- Naming
- Scheduling
- Communication among processes
- Reusing objects.

Each of them has security implications.

(Continued)

Simple supporting a single task at a time.

Complex supporting multiuser and multitasking.

**** Naturally:**

- **security considerations increase as OS become more complex.**
- **Identification and authentication are required for this access control**

3-Protected Objects

The rise of multiprogramming meant that several aspects of a computing system required protection:

- Memory.
- Sharable I/O devices, such as disks.
- Serially reusable I/O devices, such as printers and tape drives.
- Sharable programs and sub-procedures.
- Networks.
- Sharable data.

Security Methods of O.S

The basis of protection **<u>is separation</u>**:

keeping one user's objects separate from other users. That separation in an OS can occur in several ways:

1. ***Physical separation***
2. ***Temporal separation.***
3. ***Logical separation***
4. ***Cryptographic separation***

4-Security Methods of OS

Physical separation, in which different processes use different physical objects, such as separate printers for output requiring different levels of security

Temporal separation, in which processes having different security requirements are executed at different times.

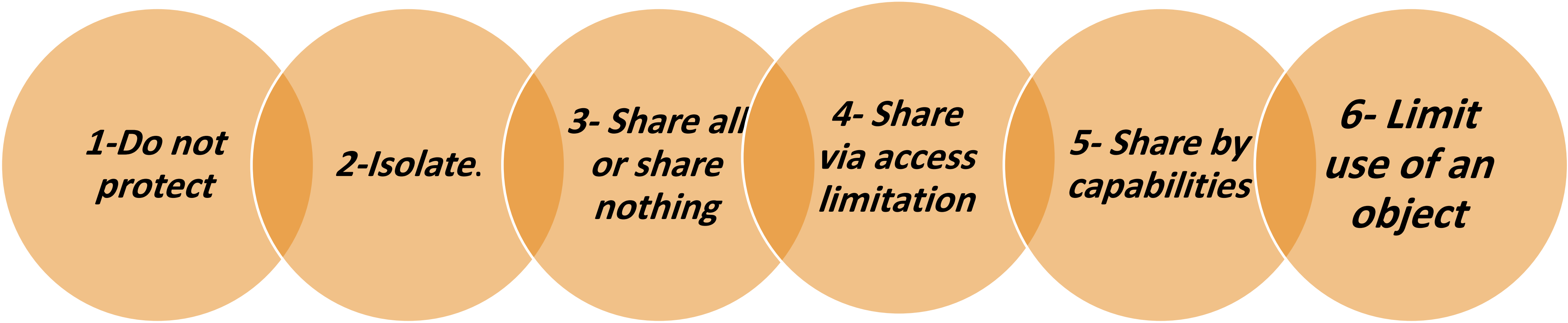
Security Methods of OS (cont.)

- ***Logical separation***, in which users operate under the illusion that no other processes exist, as when an operating system constrains a program's accesses so that the program cannot access objects outside its permitted domain.
- ***Cryptographic separation***, in which processes conceal their data and computations in such a way that they are unintelligible to outside processes. (It is more Complex.)

A combination of these separations is possible.

5- Separation and Sharing

OS can support separation and sharing in several ways, offering protection at any of several levels.



1-Do not protect

2-Isolate.

3- Share all or share nothing

4- Share via access limitation

5- Share by capabilities

6- Limit use of an object

Separation and Sharing (cont.)

Do not protect. OS with no protection is appropriate when sensitive procedures are being run at separate times.

Isolate. When OS provides isolation, different processes running concurrently are unaware of the presence of each other. Each process has its own address space, files, and other objects.

Separation and Sharing (cont.)

Share all or share nothing. With this form of protection, the owner of an object declares it to be public or private.

A *public object* is available to all users, whereas a *private object* is available only to its owner

Share via access limitation. With protection by access limitation, the OS checks the allowability of each user's potential access to an object. That is, access control is implemented for a specific user and a specific object. The OS acts as a guard between users and objects, ensuring that only authorized accesses occur.

Separation and Sharing (cont.)

Share by capabilities. An extension of limited access sharing, this form of protection allows dynamic creation of sharing rights for objects. The degree of sharing can depend on the owner or the subject, on the context of the computation, or on the object itself.

Limit use of an object. This form of protection limits not just the access to an object but the use made of that object after it has been accessed.

6- Access control

In general, access control has three goals:

1. **Check every access:** Else OS might fail to notice that access has been revoked
2. **Enforce least privilege:** Grant program access only to smallest number of objects required to perform a task

   Access to additional objects might be harmless under normal circumstances, but disastrous in special cases

3. **Verify acceptable use:** Limit types of activity that can be performed on an object

   E.g., for integrity reasons

7- User authentication

Computer systems often have to identify and authenticate users before authorizing them

- Identification: Who are you?
- Authentication: Prove it!

Identification and authentication is easy among people that know each other

- For your friends, you do it based on their face or voice

More difficult for computers to authenticate people sitting in front of them

Even more difficult for computers to authenticate people accessing them remotely

User authentication (cont.)

OS bases much of its protection on identifying a user of the system.

Authentication mechanisms use any of three qualities to confirm a user's identity:

- Something the user knows (Passwords or PIN)
- Something the user has, (cards or physical keys).
- Something the user is (biometrics identity),
- Something about the user’s (Location or time)

*** Two or more forms can be combined for more solid authentication.

➢ Passwords as Authenticators

PWs are widely used for authentication.

Other information can be used in addition to PW, s.a. access time and terminal.

PWs suffer from some difficulties of use:

- **Loss**. Depending on how the passwords are implemented, it is possible that no one will be able to replace a lost or forgotten password. If the user loses the password, a new one must be assigned.
- **Use**. Supplying a password for each access to a file can be inconvenient and time consuming.

Passwords as Authenticators (cont.)

- **Disclosure**. If a password is disclosed to an unauthorized individual, the file becomes immediately accessible. If the user then changes the password, all other legitimate users must be informed of the new password.

- **Revocation**. To revoke one user's access right to a file, someone must change the password, thereby causing the same problems as disclosure.

Attacks on Passwords

Here are some ways you might be able to determine a user's password:

- Try all possible passwords.
- Try frequently used passwords.
- Try passwords likely for the user.
- Search for the system list of passwords.
- Ask the user.
- Rainbow table
- Social engineering

Exhaustive Attack

Exhaustive or **brute force attack**, the attacker tries all possible passwords.

The number of possible passwords depends on the implementation of the system.

If passwords are words consisting of the 26 characters A..Z and can be of any length from 1 to 8 characters, then the system as a whole has **$26^1 + 26^2 + ... + 26^8$ = about $5 * 10^{12}$** possible passwords.

Encrypted Password File

To foil an intruder seeking passwords in plain sight, encrypt them:

Conventional encryption, but still some user(s) can decrypt them.

Hash function/one-way ciphers.
A problem: what if two users choose the same pw and one of them see the hash value of the other user?
A solution: add to the pw a unique generated number to the pw before hashing.

Guidelines for PW Selection Criteria

- Use characters , numbers, symbols
- Choose long passwords.
- Avoid actual names or words.
- Choose an unlikely password.
- Change the password regularly.
- Don't write it down.
- Don't tell anyone else.

➢ Biometrics as authentication

Biometrics are biological authenticators, based on some physical characteristic of the human body:

- Fingerprints
- Hand and face geometry
- Retina
- Voice
- Handwriting
- Walking pattern

Advantage over pw: a biometric cannot be lost, stolen, forgotten, forged and is always available.

Problems with Biometrics

Biometrics are relatively new, and some people find their use intrusive.

Biometric recognition devices are costly.

All biometric readers use sampling and establish a threshold for when a match is close enough to accept.

Biometrics can become a single point of failure.

Problems with Biometrics (cont.)

- Although equipment is improving, there are still false readings.
- The speed at which a recognition must be done limits accuracy.
- Although we like to think of biometrics as unique parts of an individual, forgeries are possible.

THANK YOU

Reference:

- Textbook: Security in Computing, 5th Edition , 2015 by Charles P. Pfleeger.
- Stallings W, Brown L, Bauer MD, Bhattacharjee AK. Computer security: principles and practice. Upper Saddle River, NJ, USA: Pearson Education; 2012.
- Internet resources.