Introduction to Operating Systems

Chapter 9: Security

Manuel

Fall 2017

Outline

What is security?

Simple reasoning:

- Security is needed to protect from some danger
- If the danger is unknown it is impossible to avoid it

What is security?

Simple reasoning:

- Security is needed to protect from some danger
- If the danger is unknown it is impossible to avoid it

What are the dangers?

Setup and dangers

To define the dangers, the setup must be known:

- General setup: operating system
- Processes: privileges
- Memory: sensitive information processed
- I/O devices: intruders
- File system: sensitive data

Threats

In an OS threats can be divided into four categories:

- Data stolen: confidentiality
- Data changed: integrity
- Intrusion: exclusion of outsiders
- Denial of service: system availability

Who?

Knowing who is likely to attack is of a major important:

- Local user reading other users files
- Regular other users on the same network
- Mafia
- Espionage
- Bad luck

Outline

Security and cryptography

Cryptography: science of secret

- Confidentiality
- Data integrity
- Authentication

Security and cryptography

Cryptography: science of secret

- Confidentiality
- Data integrity
- Authentication

Two basic strategies:

- Symmetric
- Asymmetric

Confidentiality

Encrypted data will remain confidential. How to encrypt data?

Symmetric:

- Shuffle all the letters of the alphabet and map the first one to A, the second one to B...
- One-time-pad: take a message and a key of same length and xor them

Question: are those strategies secure?

Confidentiality

Encrypted data will remain confidential. How to encrypt data?

Symmetric:

- Shuffle all the letters of the alphabet and map the first one to A, the second one to B...
- One-time-pad: take a message and a key of same length and xor them

Question: are those strategies secure?

Asymmetric:

- Based on the concept of one-way-function
- Common examples: RSA, ELgamal

Symmetric protocol better fit the OS setup

Data integrity

Ensure that data has not been altered using hash functions

- Easy to compute
- Infeasible to generate a message with a given hash
- Infeasible to modify a message without modifying the hash
- Infeasible to find two different messages with same hash

Authentication

Prove that a user is really who he pretends to be

- Secret
- Challenge-response
- Token
- Biometrics

Outline

Authentication

Most obvious strategy: setup a login and password

- Password should not be displayed when entered
- Should something be displayed when typing the password?
- When to reject a login: before of after the password input?
- What if the hard disk is mounted from another OS?

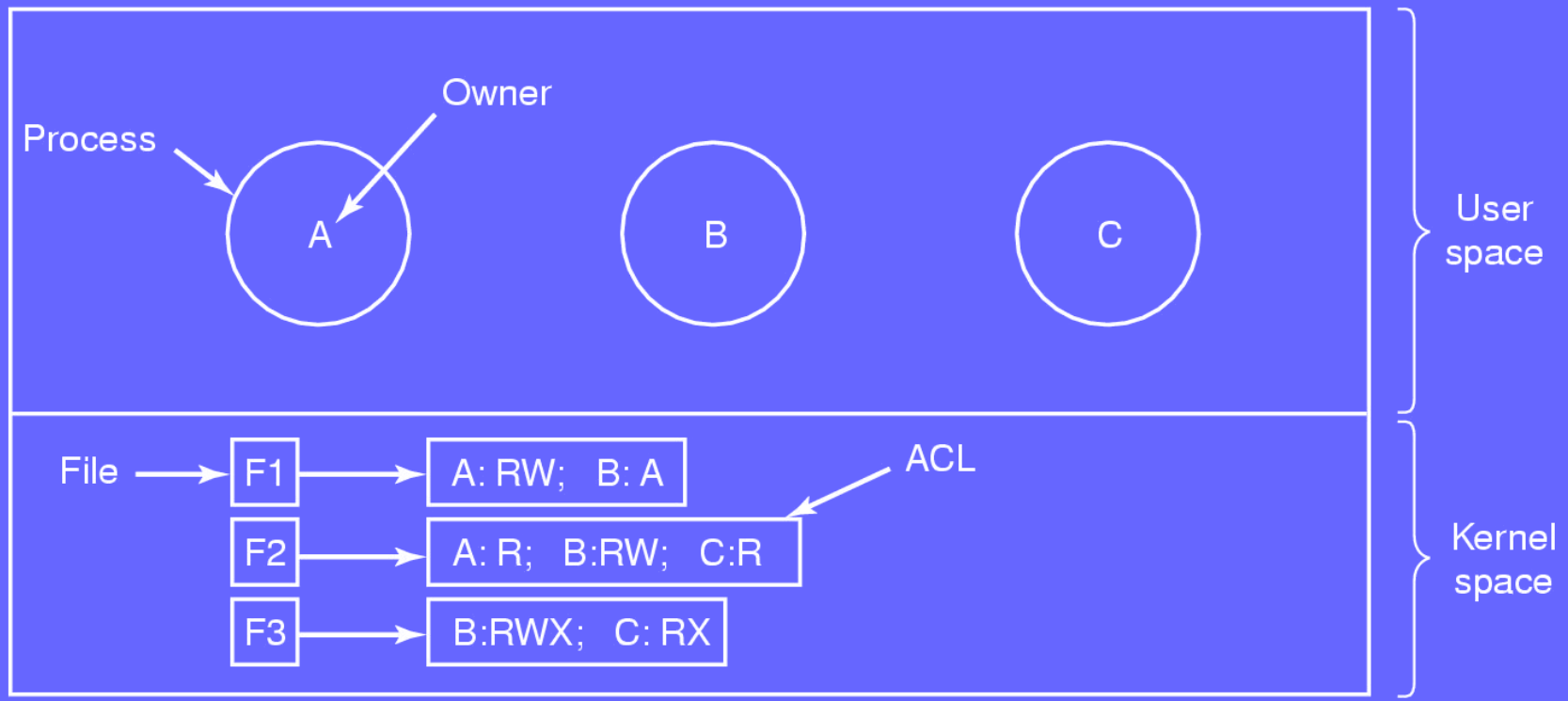
Authentication

Most obvious strategy: setup a login and password

- Password should not be displayed when entered
- Should something be displayed when typing the password?
- When to reject a login: before of after the password input?
- What if the hard disk is mounted from another OS?

Other common strategy: use a key

Access Control Lists



Security layers

ACL are used to give users different privileges:

- Administrator: root/admin
- Privileged users: belong to special groups
- Regular user cannot access I/O devices

Keeping a system secure

Basic

Important note: an OS cannot be kept 100% secure

Basic strategy:

- Keep the system minimal
- No new software versions
- Regularly update the system
- Install software only from trusted parties
- Strong passwords or no password

Keeping a system secure

Advanced

Advanced strategy:

- Apply the basic strategy
- Filter any outgoing network traffic
- Block any incoming new connection
- Keep a checksum of all the files
- Only use encrypted network traffic
- Use containers or virtual machines to run sensitive services
- Associate with each program a profile that restricts its capabilities

Keeping a system secure

Paranoiac

Paranoiac strategy:

- Apply the advanced startegy
- Encrypt all the disk (including the swap)
- Isolate the computer (no network connection)
- Keep an encrypted checksum of all the files
- No extra device can be connected

Keeping a system secure

Paranoiac

Paranoiac strategy:

- Apply the advanced startegy
- Encrypt all the disk (including the swap)
- Isolate the computer (no network connection)
- Keep an encrypted checksum of all the files
- No extra device can be connected

Extra question: is it now safe?

Key points

- What is security?
- What is the difference between symmetric and asymmetric cryptography?
- What are Access Control Lists?
- How safe can a computer be?

Thank you!