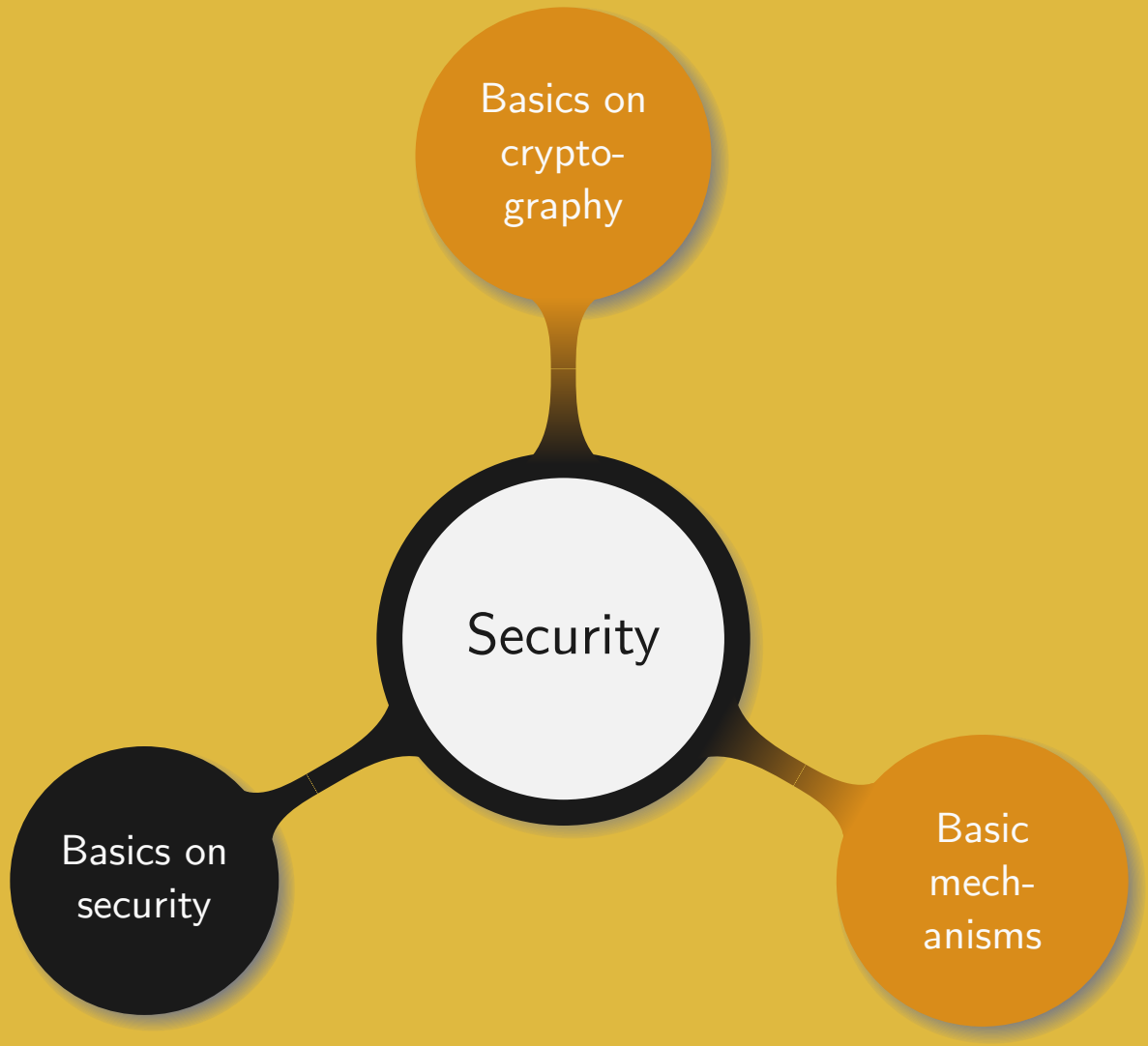
Introduction to Operating Systems

9. Security

Manuel – Fall 2021

Chapter organisation



Security setup and dangers

Simple reasoning:

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

To define the dangers, the setup must be known:

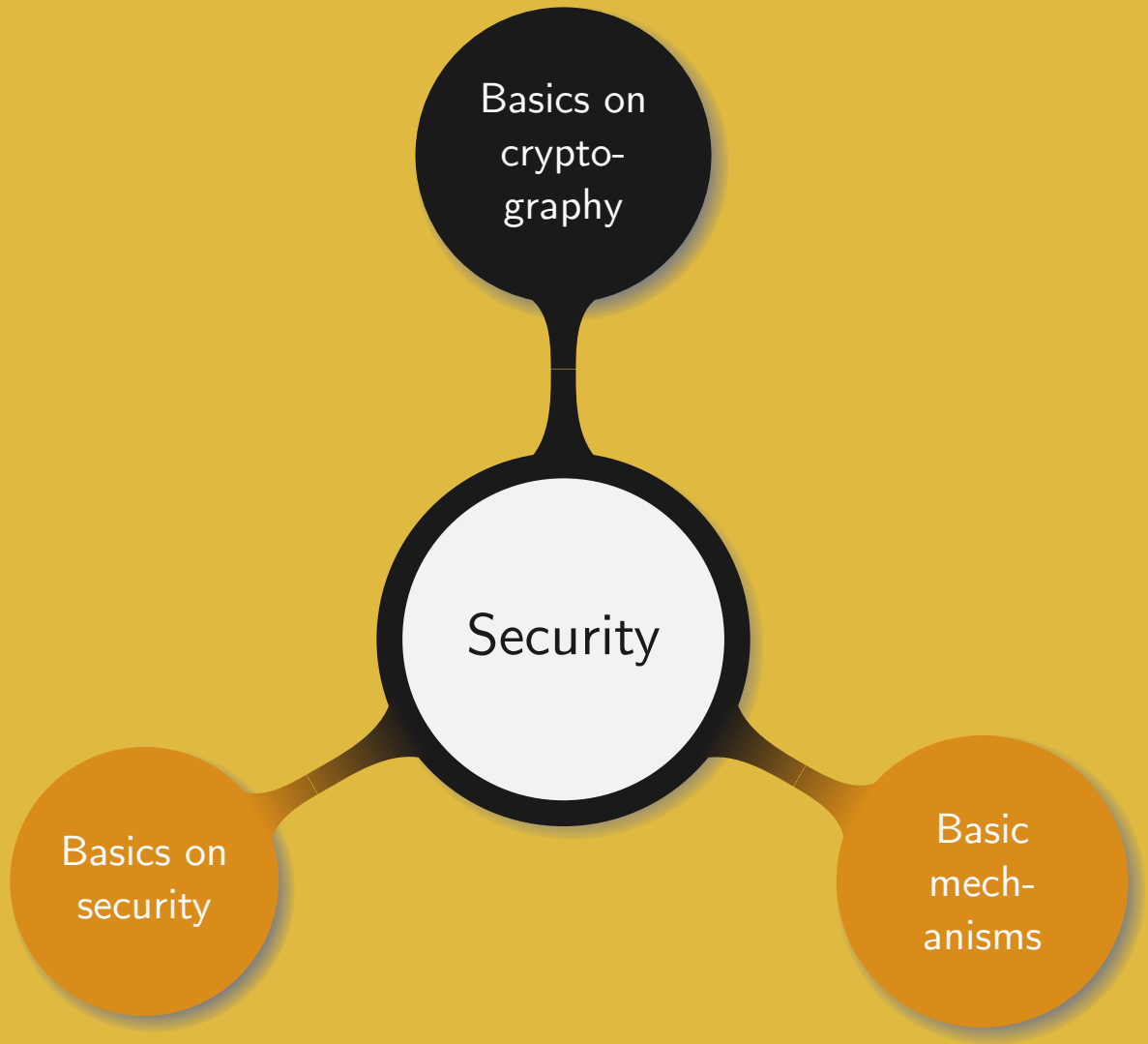
- General setup: operating system
- Processes: privileges
- Memory: sensitive information processed
- IO devices: intruders
- File system: sensitive data

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

Chapter organisation



Security and cryptography

Cryptography, the science of secret:

- Confidentiality
- Data integrity
- Authentication
- Non-repudiation

Two basic encryption strategies:

- Symmetric: same key used to encrypt an decrypt
- Asymmetric: many can encrypt but only one can decrypt

Security and cryptography

Cryptography, the science of secret:

- Confidentiality
- Data integrity
- Authentication
- Non-repudiation

Two basic encryption strategies:

- Symmetric: same key used to encrypt an decrypt
- Asymmetric: many can encrypt but only one can decrypt

In an OS setup:

- Symmetric protocols best fit confidentiality
- Asymmetric protocols best fit authentication

Data integrity and authentication

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

Data integrity and authentication

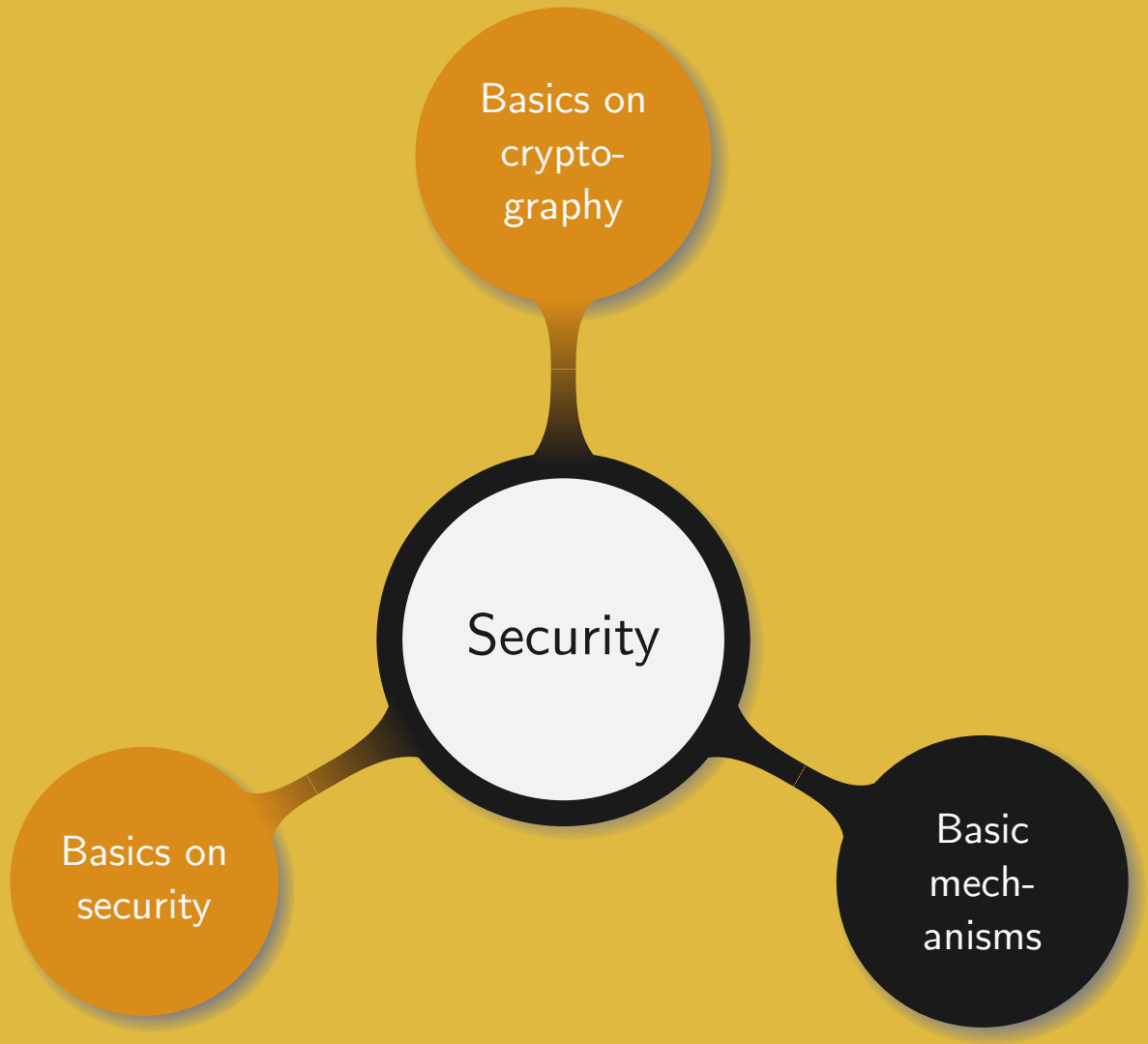
Ensure that data has not been altered using hash functions:

- 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

Prove that a user is really who he pretends to be:

- Secret
- Challenge-response
- Token
- Biometrics

Chapter organisation



Authentication

Most obvious strategy is to 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?

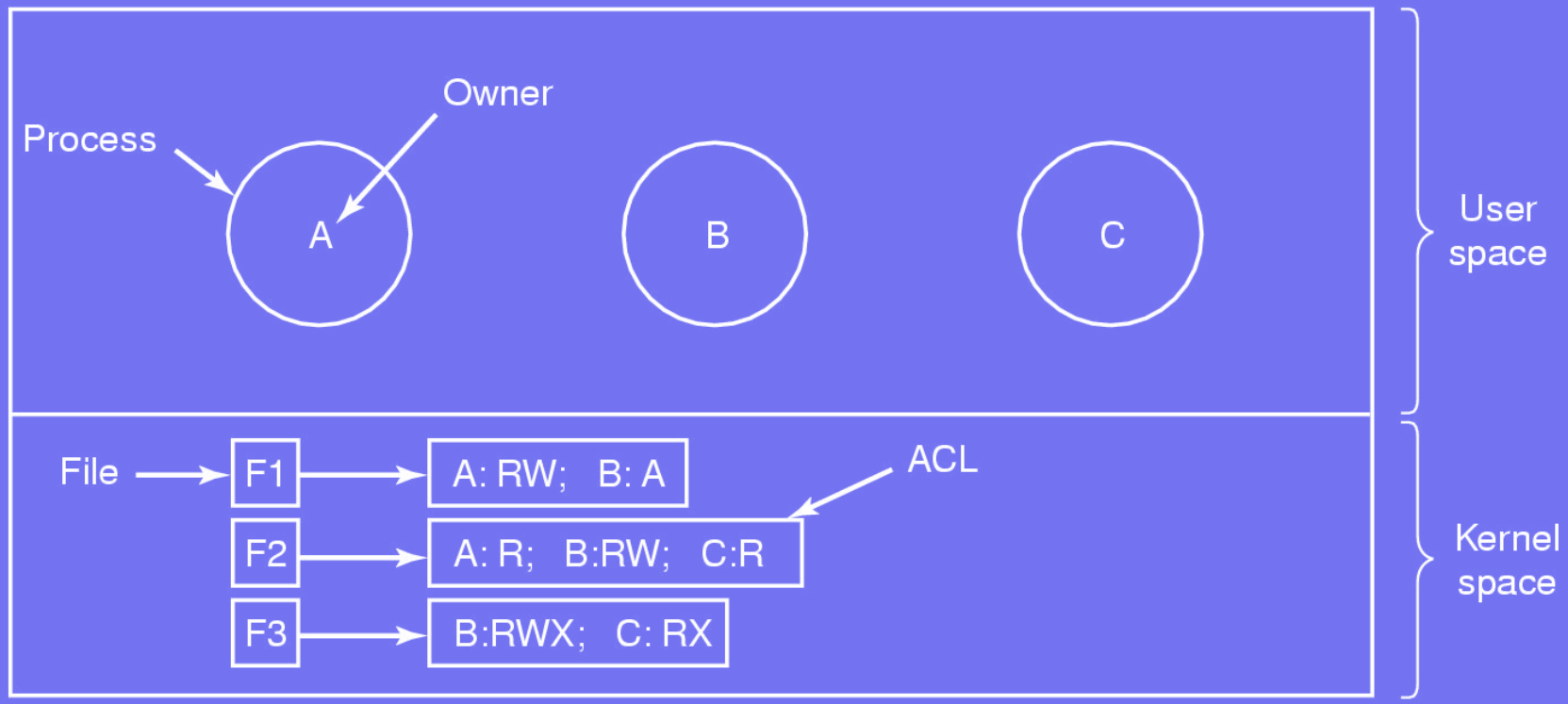
Authentication

Most obvious strategy is to 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?

Solutions based on asymmetric cryptography are safer

Access Control Lists



Access control lists are used to give users different privileges:

- Administrator: root|admin
- Privileged users: belong to special groups
- Regular users cannot access IO devices

Keeping a system secure – Basic

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 strategy
- Encrypt all the disk, including the swap
- Isolate the computer, no network connection
- Keep an encrypted checksum of all the files
- Physically block all the ports, no external device can be connected

Keeping a system secure – Paranoiac

Paranoiac strategy:

- Apply the advanced strategy
- Encrypt all the disk, including the swap
- Isolate the computer, no network connection
- Keep an encrypted checksum of all the files
- Physically block all the ports, no external device can be connected

Can this setup be considered safe?

Key points

- What is security?
- What are the two main types of encryption?
- What are Access Control Lists?
- What is the safest authentication method?
- How safe can a computer be?

Thank you!