Basics

Exercise: Name and explain 2 protection goals and measures to meet them.

Confidentiality means protecting information form access by unauthorized persons. Measures to ensure confidentiality are acces control, physical protection and encryption.

Integrity means that data is complete and correct when created, transmitted and stored by an authorized person. Intentional or unintentional changes can cause a violation of integrity. Measures to ensure integrity include hashing, storing copies for comparison, and using access rules.

Availability of an IT system means that the system is available and accessible to authorized persons. Measures to ensure availability are the use of backups, the use of a redundant design and the possibility of having a replacement (e.g. in the event of absence).

Authenticity of data/messages is guaranteed if the sender of the data can be clearly identified by the recipient and his authorship can be proven. Measures to ensure authenticity are digital signatures, hand signing of an document, personal data transfer.

Non-Repudiation of the data is guaranteed if the creator of the data cannot deny the creation afterwards. Measures to ensure non-repudiation digital signatures, manuel signatures or using trustworthy witnesses.

Exercise: Explain the difference between safety and security.

Safety means the protection against negative consequences from legitimate actions.

Security means the protection against negative consequences of unauthorized actions.

Exercise: Explain the difference between pseudonymity and anonymity.

Pseudonymity means that personal data is modified so that it can only be assigned to a person by someone who knows the assignment rule.

Anonymity means that personal data is changed in such a way that it can no longer be assigned to a person or can only be assigned with disproportionate effort.

Exercise: Name 3 attacks Mallory can perform against Alice and Bob.

Mallory can *eavesdrop* on the line. (passive attack)

Mallory can *cut* the line. (active attack)

Mallory can *manipulate* the communication. (active attack)

Exercise: Name for each protection goals a cryptographic method that is suitable for

the implementation of this protection goal.

Listen to the communication → Encrypt message e.g via PGP, authentication methods like passwords, access control (different right, roles, ...)

Cut the line → Redundancy, e.g backup line, more servers

Manipulate the communication → Hash functions, digital signatures

Exercise: Explain what a threat is.

Anything that is capable of affecting an object in a harmful way is called a threat. A threat has a direct effect on an object as the result of a vulnerability.

Exercise: Explain what a threat Threat agent is.

Methods and things used to exploit a vulnerability.

Exercise: Name 3 Information Security Threats.

Masquerade means an entity claims to be another entity.

Eavesdropping means an entity read information it's not intended to read.

Authorized Violation means an entity uses a service it's not intended to use.

Loss or Modification of information means data is being altered or destroyed.

Denial of Communication Acts means that an entity falsely denies its involvement in a communication.

Forgery of information means an entity creates information in the name of another entity.

Sabotage means an entity destroys resources.

Exercise: Explain what a Attack is and how to classify them.

An attack is the unauthorized access or attempt to access an IT system or information. They can be classified in *active* and *passive* attacks. Passive attacks are about obtaining information. Active attacks are about changing information.

Exercise: Explain what a Vulnerability is.

A vulnerability is a weakness in the design, implementation, operation, or internal control of a process that could expose the system to adverse threats from malicious events.

Exercise: Give the formula for measuring the availability of a system.

$$\text{Availability} = \frac{\text{Total Runtime} - \text{Downtime}}{\text{Total Runtime}}$$

Exercise: Give the formula for measuring the maximum allowed downtime of a system.

$$\text{Downtime} = \text{Total Runtime} - (\text{Availbility} \cdot \text{Total Runtime})$$

Cryptology

Exercise: Explain what the Kerckhoffs's principle is.

The Kerckhoff's principle defines requirements that all cryptosystems should meet. These requirements are if a system is not provably secure, it should be practically secure. The structure of a system should not depend on the secrecy of the encryption, but on the secrecy of the key. A cryptosystem must be easy to use.

Exercise: Explain what symmetric cryptography is.

The communication partners use the same key for encryption and decryption.

Exercise: Explain what asymmetric cryptography is.

A key pair is generated that consists of a public key and a secret key. The public key can be shared with anyone and can be used for encryption of a message. The secret key should not be shared and is used to decrypt messages encrypted with the public key.

Exercise: Compare symmetric cryptography and asymmetric cryptography

Symmetric	**Asymmetric**
Low complexity, higher efficiency. (Hardware implementation)	Higher complexity, lower efficiency. (despite HW implementations)
Complex key distribution.	Simple key distribution.
No meaningful and effective realization of digital signatures.	Digital signatures easy to implement.

Exercise: Explain what hash functions are and what properties they must fulfill.

A hash function maps a bit string of *any length* to a bit string of finite, always *same length*.

A hash function should be *efficient* in its calculation.

A hash function should be *preimage resistant*. This means that there should be no clues, such as a pattern in the hash value, that can be used to infer the original message.

A hash function should be *collision resistant*. This means there should not be two different messages that generate the same hash value. In practice, however, collisions exit for every hash function since we map an infinite set of possible messages to a finite set of possible hash values, even it's practically impossible.

Exercise: Why is the Electronic Codebook Mode (ECB) insecure?

Identical plaintext blocks are always encrypted to identical ciphertext blocks. This allows patterns to be found in the encrypted ciphertext and conclusions to be drawn about the plaintext.

Exercise: Compare the Electronic Codebook Mode (ECB) to the Cipher Block Chaining Mode (CBC).

ECB	**CBC**
Plaintext is divided into blocks and each block is encrypted independently. For the encryption of each block the same key is used.	Plaintext is divided into blocks. The first block is combined with an random initialization vector via XOR and then encrypted with the key. The result is used to combine the next plaintext block with XOR and then it's encrypted with the key again and so on.
The encryption in ECB can be executed parallel as the encryption of each block is independent of the encryption of another block.	The encryption of CBC cannot be excuted parallel as the encryption of the blocks depends on the result of last block.
Since the encodings are independent of each other, errors that occur in one block have no effect on other blocks.	Since the encodings are dependent on each other, errors that occur in one block will affect the following blocks.
Even without knowledge of the key, the plaintext can be guessed, since each plaintext block is mapped to the same ciphertext block, resulting in patterns in the ciphertext.	The ciphertext does not have any patterns that would allow you to guess the plaintext.

Trust Models

Exercise: Name and briefly explain the three models of trust.

Direct Trust means the user receives the public key directly from the key holder. It can be used only in small groups, because adding a new partner causes an exchange with n people.

Web of Trust means a user A signs another users B public key. If user B signs then the public key of a user C, A trusts C as well. However, this requires that B only signs trustworthy keys.

Hierarchical trust means

Exercise: How can the exchanges needed in Direct Trust be calculated?

$\frac{n(n-1)}{2}$, where n is the number of persons.

Exercise: Explain what a Certificate is and how it works?

A certificate is used to confirm the trustworthiness of a person. To do this, people must trust a certification authority (CA) that manages public keys and can issue certificates. It signs a person's public key and thus confirms their trustworthiness. The user receives the certificate, which contains the CA's signature and other information. It can be verified by anyone with the CA's public key.

Exercise: What information does a Certificate contain?

- Subject
- Name of the issuer (CA)
- Public key
- Signature algorithm
- Validity period
- What the key is used for
- Signature of the CA

Malware

Exercise: Explain the following terms.

a) Backdoors

A Backdoor can be used to gain control over a system. It manipualtes various parts of an operating system to ensure it's not discovered and to monitor the system.

b) Bots/Zombies

An infected system with Internet connection that can be used for all kinds of malicious activities.

c) Botmaster

The Botmaster is the entity controlling the bots.

Exercise: Explain the following types of malware.

a) Virus

A Virus is malware which spread uncontrollably on a system by infecting a host, e.g files or programs.

b) Worm

A Worm is a standalone programm, i.e it doesn't require an host. It replicates itself to spread via computer network or removable devices.

c) Spyware

A spyware is installed together with other programs and is used to analyse a user's behavior.

d) Adware

An adware is installed together with other programs and serves to display unwanted advertisements to the user.

e) Trojans

A trojan is a malware that looks like a normal, non-malicious software, but contains hidden features that negatively affect a system.

f) Ransomware

A ransomware is a software that blocks access to the userÄs data unless a ransom is paid.

g) Rootkits

A rootkit is a set of tools that run on a target computer when you have gained access with root privileges. It is used to create temporary access to an always-open backdoor.

Exercise: Name measures to ensure protection against malware.

Firewalls can be used to filter a network's traffic and block possible attackers from gaining unauthorized access.

Pentesting can be used to test systems for vulnerabilities in order to close them.

Sciptblockers can be used to disable certain scripts on a website that can change the behavior of the website.

Exercise: Give four possibilities of what damage malware may cause and what purpose the attacker could pursue with it.

1. The attacker could encrypt the data and blackmail the affected person, e.g. either the person pays or the data is destroyed.
2. The attacker could gain access to the computer to include it in a bot-network. The computer is then used for attacks like DDos, spam mails or other things without the owner's knowledge. The malware thus also harms third parties and not only the infected computer.
3. The attacker might not have malicious intentions, instead it could be a pentester trying to discover security vulnerabilities in a system or of a software.
4. The attacker could use the malware to obtain information. The purpose could depend on the party, e.g., a central authority, a hacktivist, or a blackhat.

Exercise: Explain how virus scanners work in your own words.

A virus scanner knowns two modes *manuel monitoring* and *realtime monitor*.

Manuel monitoring scan for patterns in the code, based on a blacklist of viruses or virus patterns.

Realtime monitoring checks read and write access to detect viruses.

Authentication

Exercise: Name and briefly explain the three classes of authentication techniques.

Knowledge-based authentication aims at proving a user's authenticity based on knowledge of private information about the them. It is used to prove that the person providing the identity information is the owner of the identity. (e.g Passwords, PINs, Cryptographic Keys)

Possession-based authentication aims to prove a person's identity using items that the user carries, usually a hardware device such as a security token or a phone. (e.g smart card, USB token, Sim card)

Inherence-based authentication aims to verify the identity of a person based on the unique biological characteristics of a person. (e.g fingerprint, iris, face, voice, dna tests)

Exercise: Name two strengths and two weaknesses that a biometric authentication process has compared to a 2-factor authentication based on knowledge and possession.

Strength:
- 2-factor authentication requires an extra device (No loss possible)
- Make sure only people suppose to access can really access (cannot share it)

Weakness:
- Item Results of biometric security can have *false accepts* and *false rejects*
- Information about real identity of person are stored, while 2FA don't store information that can be used to identify users (privacy issue)

Exercise: Explain what biometric authentication is and how it works.

Biometric authentication uses a biologically unique identifiers of a user to authenticate them. Software creates data from given biological information. information from the unique characteristics are used to identify (key).

1. Register information (taking samples) of biological information (stored in database)
2. Measured and extract features
3. extract freatures compared with stored information
4. looking for matches

Exercise: Describe the process of password-based challenge-response authentication.

1. First both Parties (Alice, Bob) agree on a secret key
2. Alice want to confirm her identitdy to Bob
3. Bob creates a random challenge and sends it to Alice (random value)
4. Alice compute the anwser/encrypts the challenge using the shared the secret key and sends the solution to Bob
5. Bob computes the anwser as well and compares it with the receive result of Alice. If the anwser is the same alice confirmed her identity.

Exercise: Name and explain four requirements that affect the security of password-based methods.

- Don't store password in plain text
- store them in hash form
- store them with a salt
- Should have minimum standards (complexity)
- Weak passwords can be guessed
- Sometimes passwords are transmitted in clear text
- Passwords need to be remembered

Exercise: Compile the main advantage and disadvantage of one-time passwords (e.g., based on an ID token) compared to ordinary passwords and compare them.

Advantage:
- not knowledge based
- only used once

Disadvantage:
- An extra device is required

Access Control

Exercise: What are the main objectives of Access Control?
- Monitoring and controlling access to resources
- Ensuring integrity, confidentiality and availability of information
- Management of access rights

Exercise: Explain the Access Control Model DAC.

When using DAC rights are granted to individual objects, so it's an object-related security properties, but not a system-wide.

Exercise: Explain the Access Control Model Role-Based Access Control (RBAC).

RBAC can be used to implemented both DAC and MAC. It defines certain roles with rights and assigns subjects to these roles.

Exercise: What are the 3 components of Role-Based Access Control (RBAC)?.

- Set of subjects (users) S
- Set of roles R
- Set of permissions P for objects

Exercise: Explain the Access Control Model DAC.

When using DAC rights are granted to individual objects, so it's an object-related security properties, but not a system-wide.

Exercise: What two types of role exlucion in RBAC exist?

- Static Role Exclusion
- Dynamic Role Exclusion

Exercise: How does Access Control in Linux work?

The Linux filesystem defines three types of permissions. Users, Groups, Others. Those types are granted three types of access read (`r`), write (`w`), execute (`x`).

Network Security

Exercise: Explain what IPSec is used for?

IPSec is used to establish secure communications over insecure networks. It can be used to ensure confidentiality, integrity and authenticity.

Exercise: On which Layer is IPSec implemented?

It's implemented on the Network Layer.

Exercise: Name and briefly explain the two operating modes of IPsec.

In the *transport mode* the hosts are the endpoints of the communication and have a direct and secure connection.

In the *tunnel mode* the connection is established by a tunnel between two gateways. Different hosts can be on the gateway using the tunnel. The tunnel between the gateway is secured.

Exercise: Name an advantage and disadvantage the tunnel mode has compared to the transport mode.

Advantage:
- Many devices but don't need to speak IPSec (endpoint don't need to change, Packet is changed on Gateways)

Disadvantage:
- No End-To-End Connection on Gateways)

Exercise: What is Authentication Header (AH) used for?

AH provides authenticity and integrity of the transmitted IP packets and a replay protection.

Exercise: Draw the structure of an AH packet.

Exercise: What is Encapsulating Security Payload (ESP) used for?

ESP provides authenticity, integrity, confidentiality of the transmitted IP packets and a replay protection.

Exercise: Draw the structure of an ESP packet.

Transport Mode:

Tunnel Mode:

Exercise: What is Internet Key Exchange (IKE) used for?

IKE is used to agree on the procedures and keys.

Exercise: Explain what the Security Association (SA) is.

The SA contains all information about the IPsec connection between two systems. it's created when the connection is established for the first time, usually using the IKE protocol.

Exercise: What does the SA contain?

- Security Parameter Index (SPI) to identify IPSec connection
- Security Protocol: AH or ESP
- AH or ESP related information

- Mode: Transport or Tunnel Mode
- Recipient IP address
- Lifetime of SA, sequence number, ...

Exercise: How are the SAs maintained?

SAs are maintained in a Security Association Database (SAD).

Exercise: Explain what the Security Policy Database (SPD) is.

The SPD defines the rules for handling IP-Packets. The following actions what to do with IP-Packets exist:
- `BYPASS`: Direct forwarding of packets
- `PROTECT`: IPSec must be used, reference to SA (`PROTECT`: Apply *protocol mode* with *encryption*)
- `DISCARD`: Drop packet

Exercise: Explain what TLS is used for.

TLS is used to ensure end-to-end security. It ensures the secure delivery of data over the Internet, avoiding possible eavesdropping and/or alteration of the content.

Exercise: On which layer is TLS implemented?

It's implemented on the Transport Layer.

Exercise: Shortly explain how tls works.

It uses combination of asymmetric and symmetric cryptography. Asymmetric cryptography used for securly sharing the cryptographic symmetric key (session keys). Symmetric cryptography used for data encryption and decryption using the transmitted session key.

Exercise: Explain the working of the TLS Handshake

1. ClientHello
2. ServerHello
3. ServerCertificate, ServerKeyExchange*, CertificateRequest*
4. ServerHelloDone
5. ClientCertificate*, ClientKeyExchange, CertificateVerify*
6. ChangeCipherSpec
7. Finished
8. ChangeCipherSpec
9. Finished

Exercise: What is end-to-end (E2E) security?

Continously security between two endpoints (sender and receipient). General seucity of sender and receipient, e.g secure transmission of data → confidentiality when sending

from sender to receiver.

Exercise: Where in hybrid reference model can end-to-end be implemented?

Between Applications - Application Layer (Layer 5) (security within the application)
Between Devices - Transport Layer (secutity via TLS) or Network Layer (seucity via IPSec)

Exercise: In which layer of hybrid reference model does TLS provides services?

Implemented in Transport Layer and provides service to Application Layer

Exercise: Name protocols that TLS secure.

HTTP, FTP, SMTP, ...

Exercise: What is a Firewall used for?

Firewalls are used for monitoring and control of communication. Using rule-based filtering (possibly malicious) data packets are filtered out.

Exercise: Briefly name and explain the two types of Firewalls.

Two types of packet filters exist, *stateless* and *stateful*.
Stateless means that no relationship is established between the packets.
Stateful means that the state/relationship between the packets is detected (e.g. whether a connection already exists).

Example: Access List

- Direction: `IN`, `OUT`
- Source IP, Destination IP: IP-Addresse, `EXTERNAL`, `ANY`
- Protocol: TCP, `ANY`
- Source Port, Destination Port: `>1032`, `25` (SMTP), `80` (HTTP), `443` (HTTPS)
- State: `ANY`, `ACK`
- Actions: `PERMIT`, `DENY`, `REJECT`

Example: State Table

- Direction: `IN`, `OUT`
- Source IP, Destination IP: IP-Addresse, `EXTERNAL`
- Protocol: TCP, `ANY`
- Source Port, Destination Port: `>1032`, `25` (SMTP), `80` (HTTP), `443` (HTTPS)
- State: `NEW`, `ESTABLISHED`, `ANY`
- Actions: `PERMIT`, `DENY`, `REJECT`

Exercise: Briefly describe the tasks of the three tables `filter`, `nat` and `mangle` of the Linux Kernel Netfilter.

- `filter`: contains filter rules for filtering packet (drop or accept)
- `nat`: used to translate IP addresses and ports (network address translation).
- `mangle`: Used for packet manipulation.

Exercise: Briefly describe the standard chains `INPUT`, `OUTPUT`, `FORWARD`, `PREROUTING` and `POSTROUTING` and their tasks.

- `INPUT`:The packet is delivered locally, i.e. the firewall is the destination.
- `OUTPUT`: The packet is created by the firewall.
- `FORWARD`: The packet is routed (and not delivered locally)
- `PREROUTING`: The modification (NAT) of packets before a routing decision is made.
- `POSTROUTING`: The modification (NAT) of packets after the routing decision

Exercise: Briefly describe the standard chains `INPUT`, `OUTPUT`, `FORWARD`, `PREROUTING` and `POSTROUTING` and their tasks.

- `ACCEPT`: the packet can pass
- `REJECT`: the packet is rejected and an error message is sent
- `DROP`: the packet is ignored and no response is sent
- `LOG`: writes an entry in the syslog
- `REDIRECT`: the destination address of the packet is changed such that it is sent to the local computer
- `MASQUERADE`: the source address of the packet is replaced by the IP address of the interface on which it leaves the computer

Exercise: Draw the functioning of the Linux Kernel Firewall.

Security Management

Exercise: What is an information security (IS) risk? How can the value of a risk be estimated?

A risk is a potential impact that can have a either positive or negative impact on a organization or a company. An information security risk is the probability that a protection goal (confidentiality, integrity, availability, authenticity) will be broken, and the amount of damage resulting therefrom (risk = probability $\cdot$ damage)

Exercise: What are the objectives of IS risk management?

- Coordinated management and control of risks $\rightarrow$ effective use of resource to reduce most important risk.
- Helps to prioritize measures to be implemented.

Exercise: What are the five steps of the IS risk management cycle according to ISO 27005? Briefly describe each of the steps.

- **Risk Identification:** Disover and describe the risk
- **Risk Estimation:** What does it cost
- **Risk Evalulation:** Do we need to fix the risk?
- **Risk Treatment:** How do we treat the risk
- **Risk Acceptance:** The manager checks if the done steps to reduce the risk are acceptable or more needs to be made (List of all risks is checked)

Exercise: Name and describe the four options for *risk treatment*.

- **Risk Reducation:** Modify the risk in such a way it's reducing (add a technology, procedure or employee training)
- **Risk Avoidance:** The conscious decision not to perform any action that make the risk become present
- **Risk Transfer:** The risk is transferred to someone else (e.g insurance or outsourcing)
- **Risk Acceptance:** The conscious decision to accept the existing risk but not to treat it

Exercise: Name three standards for Information Security Management Systems (ISMS).

- ISO 27001
- IT-Grundschutz
- NIST Cybersecurity Framework

Exercise: What are the four areas of measures that should be addressed within an ISMS?

- **Technical:** Technical measure to solve problem
- **Organizational:** Who is responsable for what (Roles)
- **Personnal:** Traing personal
- **Infrastructure:** Phyiscal security of devices, building, etc.

Exercise: Why should the ISMS be a cyclic process that is constantly repeated?

- A cyclic process aims for constant improvement
- New components/products added will may cause new vulnerabilities
- The threat landscapes changes
- Change of technologies (technologies that hasnt been there before)

Exercise: Name and briefly explain at least five of the 14 control domains of ISO 27001.

- **Access Control:** Ensure restricted access to employee, so they only see and use information which are assinged to their roles
- **Cryptography:** Use encryption for important data to ensure data integrity and confidentiality.
- **Physical and Environmental Security:** Prevents unpermitted physical access and or damage to the environmental equipment of an organisation.
- **Communication Security:** Protect the communcation of an orgainzation.
- **Compliance:** Identify laws and regulations that apply in order to understand legal requirements.

Practical tasks

Exercise: Caesar cipher encryption and/or decryption

Exercise: Vigenère cipher encryption and/or decryption

Exercise: Skytale encryption and/or decryption

Exercise: One Time Pad and/or decryption

Exercise: ECB, CBC encryption and/or decryption

Exercise: Fill Statful or Stateless table