Information security overview

Information security

- Protecting information and information systems.
- Defines sets processes and activities performed in order to protect information.
- Goal is to prevent unauthorized users from stealing and misusing information or services.
  - If sensitive information falls in wrong hands, it may cause huge losses including
    - finances, brand reputations, customers.

Essential terms

Hack value

- Hackers' evaluation of whether something is worth or interesting.
- High hack value examples
  - Accessing peoples credit card information as it can generate money.
  - Just accessing peoples names just to show a difficult task is doable.

Vulnerability

- Weakness which can compromise the system and be used for a possible attack.
- E.g.
  - a policy
    - e.g. policy regulating whether a personal should stick in USB drives to computer laptops.
  - design/implementation errors
    - e.g. Linux + macOS + Windows are susceptible to a vulnerability where an USB drive that disguises as keyboard and have greater access on computer

Exploit

- Breach through vulnerabilities.
- Also refers to a software that allows taking advantage of identified vulnerabilities.
- E.g. connecting a malicious USB.

Payload

- Part of malware or exploit code.
- Used for e.g.
  - Creating backdoors in victims machine
  - Damaging or deleting files
  - Committing data

- Hijacking a computer
- E.g. a keylogger or a RAT (Remote Administration Tool) that a malicious USB installs.

Zero day attack

- Also known as • **zero-day attack** • **0-day attack** • **0 day attack**
- Exploiting previously unknown vulnerabilities before patch is released.
- **Zero day vulnerability**
  - Hole in software that is unknown to the vendor and newly discovered.
- E.g. Spectre & Meltdown
  - Vulnerabilities in AMD and Intel CPUs
  - Can be exploited to elevate the privileges in the given system.
  - Still exists but no longer a zero day.
  - Affected all cloud providers, they needed to run firmware updates, updates provided by Intel that caused delays.
- Steps:
  1. Attacker discovers the vulnerability
  2. Attacker exploits vulnerability
  3. Attack happens (called day zero)
  4. Vendor learns about vulnerability
  5. Patch is created
     - Sometimes vendor may not patch it e.g. if software is outdated or has no support.
  6. Patch is applied
     - Sometimes they're not! E.g. home routers has vulnerabilities that has been known for years as ISPs do not usually configure routers after setup
     - Timeframe between patch is created and applied is used by malicious hackers to maximum extend.
       - Many times corporations are slower to react which causes harm.

Daisy chaining

- An attack in which hackers gain access to one network/device and then using it to access next networks/devices.
- **Steps**
  1. Hackers gain access to a device within your system/network
     - e.g. smartwatch, refrigerator, PC.
  2. They move further by gaining access to next device in your network and then next and so on.
     - Potentially hacker owns the network in the end.
- 🌐 **Example for hacking banks or similar**
  1. Go after person that has the most access.
  2. Hack that persons home router as attack vector.
     - Because it has the least resistance compared to corporate network.

- Corporate network: has corporate firewalls, IT stuff, policies etc.
- Home router: Rarely updated, full of vulnerabilities.
- They usually run down-sized linux operating system.
  - An **attack vector** is a method or pathway used by a hacker to access or penetrate the target system.

3. Scan devices that are connected to the router.
  - Can see communication (can be encrypted) but always sees ports, URLs, addresses being used.
  - E.g. mans PC, wifes PC, smart TV/refrigerator, his cell phone, wifes cell phone etc.
4. Attack with different attack vector options:
  - Change the DNS settings, you can set yourself as DNS.
  - Put his computer to DMZ to expose his PC for access from outside world.
  - Apply phishing, exploits to the operating system of the devices.
  - Get access to one of the systems
    - E.g. an Android phone. They have many vulnerabilities.
      - They don't get updates after a while.
      - If they exceed design limits e.g. when operating when it's hot outside, then the hardware flaws occurring causes exploitable software attacks such as Bitsquatting
5. Get access to
  - Information such as bank accounts, credit card details
  - After infecting one device, jump other devices in bank network if e.g. the mobile phone is also used in bank network.

Doxing

- Finding and publishing someone's personally identifiable information (PII) for malicious reasons.
- E.g. an individuals name, e-mail address or sensitive data of an organization.
- E.g. confidential government files get leaked to the public.
- Steps
  1. Gather private and valuable information about a person/organization
     - E.g. photographs, SSN, social accounts, address...
     - Build a profile of target by learning more information e.g. through social media.
  2. Misuse collected information for different reasons.
     - E.g. identity theft, stealing financial information to use, coercing their target's into doing something they don't want to

Bot

- Contraction of "robot"
- A software that can be controlled to execute predefined tasks.
- Used by hackers to control the infected machines for malicious reasons.
- Use-case

- E.g. using a bot to control the computer and perform attacks on other computers
  - E.g. creating a botnet by infecting more machines

CIA triad

- Also known as *three principles of information security*
- Recognized widely as hearth (main focus) of information security

  -
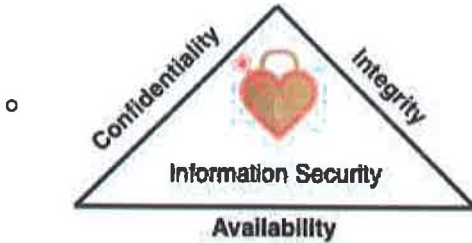
- Should function as as goals and objectives for every security program
- 📝 Ensures

  - Confidentiality: so no one can see what's inside.
  - Integrity: no one tampers data-in transit
  - Availability: data is accessible on demand

Elements of information security

Confidentiality

- Ensures that information is available only to people who are authorized to access it.
- Improper data handling or a hacking attempt leads to confidentiality breaches.
- 💡 Controls: • encryption • classification • access control • proper disposal (e.g. of DVDs, CDs, etc.)

Integrity

- Ensures the accuracy of the information
- Prevents improper and unauthorized changes—the
- 💡 Controls: • hashing • access control

Availability

- Ensuring resources are available whenever the authorized user needs them
- 💡 Controls: • redundancy • data back-ups • antivirus • DDoS prevention

Authenticity

- Ensures the quality of being genuine or uncorrupted, either:

  - **users** are actually who they present themselves to be through authentication
  - or a **document or information presented** is not corrupted.
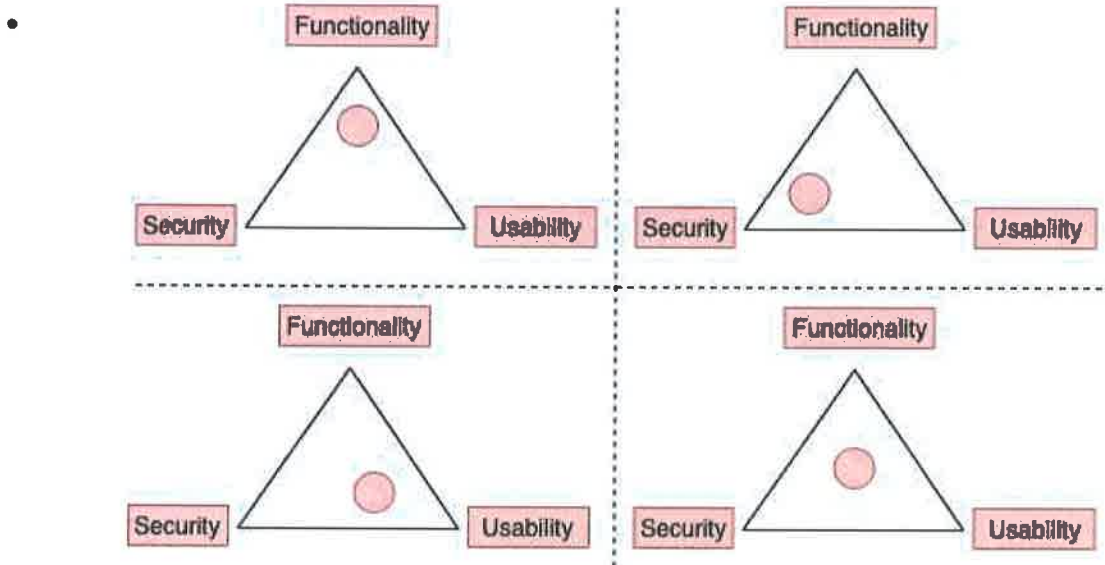- 💡 Controls: • users (biometrics) • smart cards • data (digital certificates)

Non-repudiation

- 📝 Guarantee that
    - sender of a message cannot deny having sent the message
    - recipient cannot deny having received the message
-

Sender	—message + signature→	Reciever
	←------ proof of receipt ------	

- 💡 Controls: digital signatures, logging

Functionality, usability, security triangle

-

- Components
    - **Functionality**: the features of the system
    - **Usability**: GUI of the system and how user friendly it is.
    - **Security**: How the processes of the system are used and who is using them
- Interconnected
    - Any change made to one component directly affects decreases the other two.
    - E.g. if the system security is increased, then the functionality and usability of the system are decreased
        - Because of greater overhead of security with more checks or through greater examination.
    - 💡 Balance each and every one of them to get the desired levels of security, functionality, and usability.

Document types

- **Standard**
    - Mandatory rules used to achieve consistency
- **Baseline**
    - Provide the minimum security level necessary.
- **Guideline**

- Flexible, recommended actions users are to take in the event there is no standard to follow.
- **Procedure**
  - Detailed step-by-step instructions for accomplishing a task or goal

Security threats and attacks

- The more valuable information is the higher the threats and chances for an attack are.

Security threats

- 📝 **Threat** means anything that has potential of causing damage to the system.

Types of threats

Network threats

- **Network** is the set of devices that are connected through communication channels where data exchange happens between devices
- Attacker may break into the channel and steal the information that is being exchanged.
- E.g. • denial of service attacks (DoS) • password-based attacks • compromised-key attacks, firewall and IDS attacks • DNS and ARP poisoning • man in the middle (MITM) attack • spoofing • session hijacking • information gathering • sniffing...

Host threats

- Attack that tries to gain access to information from a system
- E.g. • password attacks • unauthorized access • profiling • malware attacks • footprinting • denial of service attacks (DoS) • arbitrary code execution • privilege escalation • backdoor attacks • physical security threats

Application threats

- Exploitation of vulnerabilities that exists in the application itself

  - Caused by e.g. bad coding practices
  - Rushed programs has mistakes e.g. lack of validation of input data

- Can be found through reverse engineering, or trial and error

- Large codes that are difficult to maintain has more vulnerabilities.

- Mostly because of improper input validation.

- E.g. • SQL injection • cross-site scripting • session hijacking • identity spoofing • improper input validation • security misconfiguration • information disclosure • hidden-field manipulation • broken session management • cryptography attacks • buffer overflow attacks • phishing

Security attacks

- Or **cyber attack**
- Attempt to gain unauthorized access to a system or network.
- Actualization of a threat

Motives

- Attack = Motive + Vulnerability + Method (exploit)
- General core of every motives is access to the valuable information
- Common motives:
    - Interrupting the flow of business activities and processes
    - Stealing valuable information
    - Data manipulation
    - Stealing money and important financial information
    - Revenge
    - Ransom

Types of attacks

- You need to find vulnerability in a system to have an attack
- You can never prove that's its not vulnerable, but can prove it's vulnerable.
    - or You can never prove that a system is secure, but can prove it's insecure.

Operating system attacks

- 🗡 If OS is taken over protecting applications won't matter.
- Vulnerabilities include
    - Bugs (as it's a big codebase)
    - Buffer overflow
    - Unpatched operating systems (can lead to e.g. zero day vulnerabilities)
- Attacks include
    - Exploiting network protocol implementations
    - Authentication attacks
    - Cracking passwords
    - Breaking filesystem security
- 💡 Secure OS is an OS that's updated, monitored, regulated as frequently as possible.

- See also banner grabbing

Misconfiguration attacks

- Hacker gains access to the system that has poorly configured security.
- Can affect works, databases, web servers, etc.
- E.g. • using default accounts (passwords) • forgetting Apache server online to allow proxy requests enabling DDoS attacks
- 💡 Detected mostly by automated scanners

Application-level attacks

- Similar to OS attacks but far less damaging as their scope is far narrower.
- Caused by lack of testing as developers rush development of applications and miss something.
- E.g. • sensitive information disclosure • buffer overflow attack • SQL injection v cross-site scripting • session hijacking denial of service • man in the middle • phishing

- 🙀 E.g. Transmission torrent client (macOS)
    - The store where it was downloaded was compromised
    - They substituted torrent download link to their own application
    - See [Transmission is hacked to spread malware](#)

Shrink-wrap code attacks

- Attacks on libraries and frameworks that the software is depended on.
- Finding vulnerabilities in libraries allows re-using same exploits on more than single application
- 💡 Use libraries: older, more mature, maintained, updated actively with proven track record.
- E.g.
    - A bug is fixed in library but application uses older version.
    - Application uses libraries in debug mode or with default configurations.

Attack vectors

- Attack vector = Means by which hackers deliver a payload to systems and networks
- [Cloud computing threats](#) such as data breach and loss.
- [IoT threats](#) usually caused by insecure devices and hardware constraints (battery, memory, CPU etc.)
- [Ransomware](#): Restricts access to your files and requires payment to be granted access
- [Mobile threats](#)

Advanced Persistent Threats (APT)

- 📝 Stealthy threat actor with continuous attacks targeting a specific entity.
- APT groups include:
    - [APT 10 - Red Apollo @China](#)
    - [Equation Group @USA](#)
    - [APT 29 - Cozy Bear @Russia](#)
    - and [many more](#)...
- **Advanced**
    - Uses special malware, often crafted for specific organizations
        - Usually a modified version of common malware used in botnets
    - Sophisticated techniques against target not generic
- **Persistent**
    - Long-term presence with external command and control
    - Extracting data
        - Usually *low-and-slow* to avoid detection
        - E.g. instead of sending big data, it breaks data to chunks and sends each chunk whenever a user is connected to the internet
- **Threat**
    - Targets high value organizations and information
    - E.g. governments and big companies
- 🙀 E.g.

- Sony Pictures hack where sensitive data from Sony, e.g. unreleased movies was published as torrents.
- 2020 United States federal government data breach where more than 18.000 US companies and government agencies where hacked.
- Common steps

    1. Create a breach e.g. through spear phishing
    2. Exploit inner system vulnerabilities
    3. Control of the system or its segments
    4. Data exfiltration (= unauthorized data transfer)

Viruses and worms

- Both can replicates themselves throughout the system in files, documents.
- Have capabilities to infect systems and networks in a quick time.
- Virus: Requires user action to be activated e.g. running a file that has a virus embedded.
- Worm: can spread independently without any user action i.e. self-replicating

Botnet

- 📝 Used by hackers to control the infected machines e.g. phones, PC, IoT
- Hackers perform malicious activities from the machines on which bots run eg. DDoS attacks.
- Main problem is lack of security software or proper updates on devices.
- See also Botnet trojans and Botnets | Denial of Service

Insider attacks

- Performed by a person from within the organization who has authorized access.

    - E.g. disgruntled employee, employee paid by a third-party
- Presents one of the greatest potential of risk and most difficult attacks to defend against.

- See also Insider attacks | Social engineering types.

Insider threat types

- **Pure insider**

    - Inside employee with normal access rights
- **Elevated pure insider**

    - Insider with elevated access
- **Insider associate**

    - Insider with limited authorized access (e.g. guard, cleaning person)
- **Insider affiliate**

    - Spouse, friend, or client of an employee that uses employee's credentials.
- **Outsider affiliate**

    - Unknown and untrusted person from outside the organization.
    - Uses an open access channel or stolen credentials to gain unauthorized access.

Insider attack countermeasures

- Restricting access
- Logging to know who access what at what point of time
- Active monitoring of employees with elevated privileges
- Trying to not have disgruntled employees
- Separation of duties
    - Also known as **segregation of duties**
    - Concept of having more than one person required to complete a task.
    - See also [Separation of duties | Cloud computing](#)

Phishing

- See [Phishing | Social Engineering Types](#)

Web application threats

- Takes advantage of poorly written code and lack of proper validation of input and output data.
- E.g. buffer overflows, SQL injections, cross-site scripting
- 💡 There are many online scanning tools to detect those.

Modern age information warfare

- Use of information and communication technologies for competitive advantages over an opponent
- Weapons include • viruses • worms • trojan horses • logic bombs • trap doors • nano machines and microbes • electronic jamming • penetration exploits and tools.
- E.g.
    - Corporations spy on each other to use each others technology secrets and patents
        - 👥 Also known as [Industrial espionage](#)
    - Governments spy on other governments by using hackers as proxies to gain information about e.g. defense systems.
    - Intellectual property thefts with reverse engineering to create products without investing in R&D
- Categories include:
    - **Command and control (C2) warfare**
        - Taking down the command center may protect the headquarters but may interfere with their mobility
    - **Intelligence-based warfare**
        - Sensor-based technology to disrupt systems
    - **Electronic warfare**
        - Enhance, degrade, or intercept the flow of information
    - **Psychological warfare**
        - "Capture their minds and their hearts and souls will follow"
        - E.g. propaganda or terror

- **Hacker warfare**
  - Acquire information about subject A, sell it to subject B.
- **Economic information warfare**
  - Channeling or blocking information to pursue economic dominance
- **Cyber warfare**: use of information systems against virtual personas

- Each category can have:
  - **Offensive strategy**
    - Attacks against an opponent
    - E.g. web application attacks, malware attacks, system hacking..
  - **Defensive strategy**
    - Actions taken against attacks.
    - E.g. monitoring, alerts, response, detection, prevention systems
- See also Information Warfare website

Information security overview

Information security

- Protecting information and information systems.
- Defines sets processes and activities performed in order to protect information.
- Goal is to prevent unauthorized users from stealing and misusing information or services.

    If sensitive information falls in wrong hands, it may cause huge losses including

    - finances, brand reputations, customers.

Essential terms

Hack value

- Hackers' evaluation of whether something is worth or interesting.
- High hack value examples
    - Accessing peoples credit card information as it can generate money.
    - Just accessing peoples names just to show a difficult task is doable.

Vulnerability

- Weakness which can compromise the system and be used for a possible attack.
- E.g.
    - a policy
        - e.g. policy regulating whether a personal should stick in USB drives to computer laptops.
    - design/implementation errors
        - e.g. Linux + macOS + Windows are susceptible to a vulnerability where an USB drive that disguises as keyboard and have greater access on computer

Exploit

- Breach through vulnerabilities.
- Also refers to a software that allows taking advantage of identified vulnerabilities.
- E.g. connecting a malicious USB.

Payload

- Part of malware or exploit code.
- Used for e.g.
    - Creating backdoors in victims machine
    - Damaging or deleting files
    - Committing data

- Hijacking a computer
- E.g. a keylogger or a RAT (Remote Administration Tool) that a malicious USB installs.

Zero day attack

- Also known as • *zero-day attack* • *0-day attack* • *0 day attack*
- Exploiting previously unknown vulnerabilities before patch is released.
- **Zero day vulnerability**
  - Hole in software that is unknown to the vendor and newly discovered.
- E.g. Spectre & Meltdown
  - Vulnerabilities in AMD and Intel CPUs
  - Can be exploited to elevate the privileges in the given system.
  - Still exists but no longer a zero day.
  - Affected all cloud providers, they needed to run firmware updates, updates provided by Intel that caused delays.
- Steps:

  1. Attacker discovers the vulnerability

  2. Attacker exploits vulnerability

  3. Attack happens (called day zero)

  4. Vendor learns about vulnerability

  5. Patch is created

     - Sometimes vendor may not patch it e.g. if software is outdated or has no support.
  6. Patch is applied

     - Sometimes they're not! E.g. home routers has vulnerabilities that has been known for years as ISPs do not usually configure routers after setup

     - Timeframe between patch is created and applied is used by malicious hackers to maximum extend.

       - Many times corporations are slower to react which causes harm.

Daisy chaining

- An attack in which hackers gain access to one network/device and then using it to access next networks/devices.
- **Steps**

  1. Hackers gain access to a device within your system/network

     - e.g. smartwatch, refrigerator, PC.
  2. They move further by gaining access to next device in your network and then next and so on.

     - Potentially hacker owns the network in the end.
- 🏦 **Example for hacking banks or similar**

  1. Go after person that has the most access.

  2. Hack that persons home router as attack vector.

     - Because it has the least resistance compared to corporate network.

- Corporate network: has corporate firewalls, IT stuff, policies etc.
- Home router: Rarely updated, full of vulnerabilities.
- They usually run down-sized linux operating system.
- An **attack vector** is a method or pathway used by a hacker to access or penetrate the target system.

3. Scan devices that are connected to the router.

- Can see communication (can be encrypted) but always sees ports, URLs, addresses being used.
- E.g. mans PC, wifes PC, smart TV/refrigerator, his cell phone, wifes cell phone etc.

4. Attack with different attack vector options:

- Change the DNS settings, you can set yourself as DNS.

- Put his computer to DMZ to expose his PC for access from outside world.

- Apply phishing, exploits to the operating system of the devices.

- Get access to one of the systems

    - E.g. an Android phone. They have many vulnerabilities.

        - They don't get updates after a while.
        - If they exceed design limits e.g. when operating when it's hot outside, then the hardware flaws occurring causes exploitable software attacks such as Bitsquatting

5. Get access to

- Information such as bank accounts, credit card details
- After infecting one device, jump other devices in bank network if e.g. the mobile phone is also used in bank network.

Doxing

- Finding and publishing someone's personally identifiable information (PII) for malicious reasons.

- E.g. an individuals name, e-mail address or sensitive data of an organization.

- E.g. confidential government files get leaked to the public.

- Steps

    1. Gather private and valuable information about a person/organization

        - E.g. photographs, SSN, social accounts, address...
        - Build a profile of target by learning more information e.g. through social media.

    2. Misuse collected information for different reasons.

        - E.g. identity theft, stealing financial information to use, coercing their target's into doing something they don't want to

Bot

- Contraction of "robot"
- A software that can be controlled to execute predefined tasks.
- Used by hackers to control the infected machines for malicious reasons.
- Use-case

- o E.g. using a bot to control the computer and perform attacks on other computers
- o E.g. creating a botnet by infecting more machines

CIA triad

- Also known as *three principles of information security*
- Recognized widely as hearth (main focus) of information security

- Should function as as goals and objectives for every security program
- 📝 Ensures
  - o Confidentiality: so no one can see what's inside.
  - o Integrity: no one tampers data-in transit
  - o Availability: data is accessible on demand

Elements of information security

Confidentiality

- Ensures that information is available only to people who are authorized to access it.
- Improper data handling or a hacking attempt leads to confidentiality breaches.
- 💡 Controls: • encryption • classification • access control • proper disposal (e.g. of DVDs, CDs, etc.)

Integrity

- Ensures the accuracy of the information
- Prevents improper and unauthorized changes—the
- 💡 Controls: • hashing • access control

Availability

- Ensuring resources are available whenever the authorized user needs them
- 💡 Controls: • redundancy • data back-ups • antivirus • DDoS prevention

Authenticity

- Ensures the quality of being genuine or uncorrupted, either:
  - o **users** are actually who they present themselves to be through authentication
  - o or a **document or information presented** is not corrupted.
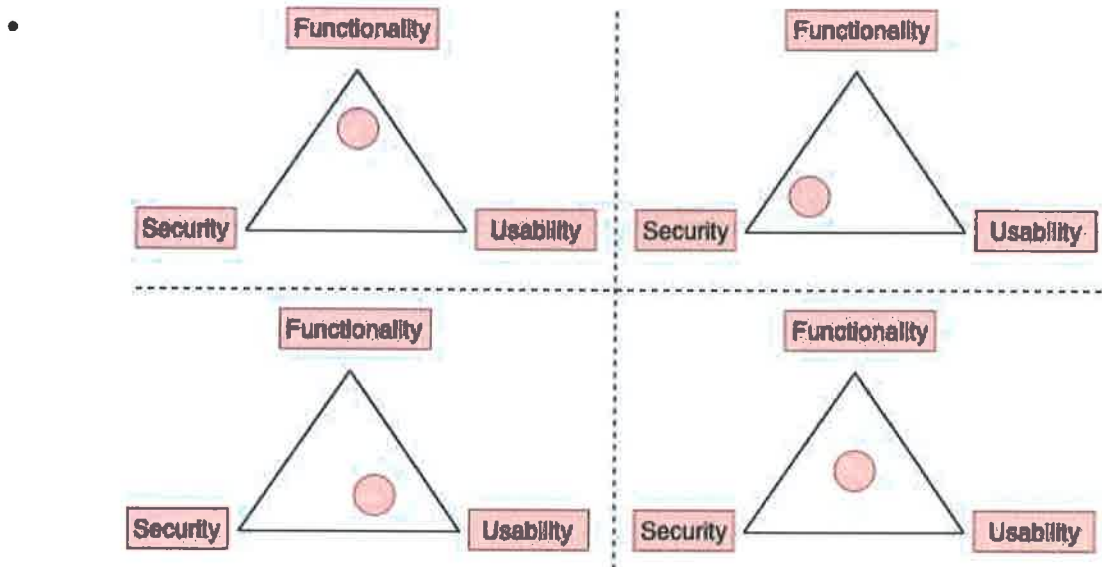- 💡 Controls: • users (biometrics) • smart cards • data (digital certificates)

Non-repudiation

- 📝 Guarantee that
    - sender of a message cannot deny having sent the message
    - recipient cannot deny having received the message
-

```
                        ┌──────message + signature──────▶
   ┌──────────────┐     │                               ┌──────────────┐
   │    Sender    │     │                               │   Reciever   │
   └──────────────┘     │                               └──────────────┘
                        ◀┄┄┄┄┄┄┄ proof of receipt ┄┄┄┄┄┄┄
```

- 💡 Controls: digital signatures, logging

Functionality, usability, security triangle

- Components
    - **Functionality**: the features of the system
    - **Usability**: GUI of the system and how user friendly it is.
    - **Security**: How the processes of the system are used and who is using them
- Interconnected
    - Any change made to one component directly affects decreases the other two.
    - E.g. if the system security is increased, then the functionality and usability of the system are decreased
        - Because of greater overhead of security with more checks or through greater examination.
    - 💡 Balance each and every one of them to get the desired levels of security, functionality, and usability.

Document types

- **Standard**
    - Mandatory rules used to achieve consistency
- **Baseline**
    - Provide the minimum security level necessary.
- **Guideline**

- Flexible, recommended actions users are to take in the event there is no standard to follow.
- **Procedure**
  - Detailed step-by-step instructions for accomplishing a task or goal

Risk management

- Ongoing process of identifying, assessing and acting on potential risks.
- 🗐🗒 Risk management controls reduce risks but one can never fully eliminate all risk
    - Nothing is 100% risk-free.

Risk

- **Risk**
    - Threat of damage or loss
- **Risk mitigation**
    - Also known as **risk reduction**
    - Taking action to reduce an organization's exposure to potential risks and reduce the likelihood that those risks will happen again.
- 🗒 **Risk equation**
    - `Risk = Threat x Vulnerability x Asset`
    - E.g. network is very vulnerable (no firewall), asset is critical: high risk.
    - E.g. network is well protected, asset is critical: medium risk
- 🗒 **Likelihood**
    - Likelihood is how probable it is that an event will occur
- 🗒 **Impact**
    - Estimate of the harm that could be caused by an event

Types of risks

- 🗒 **Inherent risk**
    - Represents the amount of risk that exists before any controls are taken.
    - Raw and untreated risk
- 🗒 **Residual risk**
    - Amount of risk that remains after controls are accounted for.
- **Control risks**
    - Risks that occur due to weaknesses in internal controls
- **Audit risk**
    - Risk of error while performing an audit.
    - Three types: Control risk, detection risk, inherent risk
- **Detection risk**
    - Verifier does not detect a material misstatement

Level of risk

- Defined based on events possible consequences to evaluate.
- **Level of risk equation**
  - `Consequence x Likelihood`

Risk Level	Consequence	Action
Extreme / high	Serious danger	Measures should be immediately taken to reduce the risk
Medium	Medium danger	Measures should be taken as soon as possible
Low	Negligible danger	Preventive measures should be taken to mitigate the risk

Risk matrix

- Used to visualize risk probabilities and its consequences
- Most used method in risk analysis

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Risk assessment

- 📝 Prioritizes risks based on severity and likelihood of occurrence
- 📝 Includes an analysis of threats based on the impact to the business
- E.g. HIPAA security risk assessment tool to assess risks regarding: • administrative safeguards • technical safeguards • physical safeguards as defined in HIPAA rules.
- 💡 Risk assessor should be a trusted entity or contractor
    - As they'll receive detailed vulnerability information and security architecture information

Risk management objectives

- Identify the potential risks
- Identify the impacts of those risks
- Create risk management strategy and plan
- Assign priorities to risks
- Analyze the risks
- Control the risk
    - e.g. education, enforcing a policy, changing a software etc..
- Develop strategies and plans for long lasting risks

Risk management phases

1. 📝 **Identification**
    - What? Why? Consequences?
    - Data gathering activities include • threat identification • vulnerability identification • risk control analysis
        - Read more NIST SP 800-39 (NIST Cybersecurity Framework)
2. **Assessment**
    - Likelihood and impact
3. **Treatment**
    - Prioritize, order and document.
    - Manage risks through risk response types
4. **Tracking and review**
    - Ensures right actions were taken.
    - Is action obsolete? Can it be improved? Can cost be decreased?

Risk responses

- 📝 5 risk responses are: • Avoid • Mitigate • Transfer • Accept • Share
- **Avoid**
    - Change the strategy/plan to avoid the risk.
- **Mitigate**
    - Take action to reduce the risk.

- o 💡 You should mitigate the risk to a low enough level so that the residual risk can be accepted as you will never be able to remove all risks.
- **Transfer**
  - o Transfer risk to another party by e.g. outsourcing or purchasing an insurance.
- **Accept**
  - o Decide to take the risk, as without risk there's no movement/rewards.
- **Share**
  - o Distributing the risk, e.g. having two security architects so service can continue if one quits.

Business continuity and disaster recovery (BCDR)

1. **Risk assessment**
   - o Preparing risk analysis and business impact analysis
   - o See also risk assessment
   - o E.g. **Disaster recovery risk assessment**
     - Describes potential risks and their impact to the functioning of an organization.
     - Describes both natural and man-made disasters and estimates the probability of each scenario occurring
   - o **Business impact analysis (BIA)**
     - Predicts the consequences of disruption of a business function
     - Process and gathers information needed to develop recovery strategies
     - Often includes Annualized Loss Expectancy (ALE) metrics.
     - Should be used identifying the potential consequences of a change, or estimating what needs to be modified to accomplish a change
     - 📝 **Business change impact analysis**
       - Allows you to identify consequences of a change
       - E.g. a new feature can cause resource load and crash the server.
2. **Business continuity plan (BCP)**
   - o Covers critical processes recovery
   - o 📝 Includes **Disaster recovery plan (DRP)** describing:
     - How an organization can quickly resume work after an unplanned incident
     - What to do to recover

Annualized Loss Expectancy (ALE)

- Annual cost of a loss due to a risk.
- Used often in risk analysis and business impact analysis
- 📝 `ALE = ARO (Annual rate of occurrence) x SLE (Single loss expectancy)`
- **Annual rate of occurrence (ARO)**
  - o E.g. if it occurs every month than it's 12, if it's every second year than it's 1/2
- **Single loss expectancy (SLE)**
  - o Total loss value for a single asset after an exploit

- ○ `SLE (Single Loss Expectancy) = AV (Asset Value) x EF (Exposure Factor)`
  - ○ **Asset value (AV)**
    - How much would it take to replace 1 asset
    - Including product prices, manhours etc.
  - ○ **Exposure Factor (EF)**
    - Percentage of asset value lost if threat is realized
    - Usually a subjective value
- E.g. an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000.
- **Total cost of ownership (TCO)**
  - ○ Total cost of a mitigating safeguard
- **Return on Investment (ROI)**
  - ○ Amount of money saved by implementing a safeguard.
  - ○ 💡 Good choice if annual Total Cost of Ownership (TCO) is less than Annualized Loss Expectancy (ALE); poor choice otherwise

Threat modeling

- Assessment to see how secure an application is
  - ○ identify the threats
    - can e.g. use <u>OWASP top 10</u> as guideline.
  - ○ discover application vulnerabilities
  - ○ improve security
    - e.g. configure in better way, improve source code, enable encryption or ditch the application.
- 💡 Do it as soon as and often as possible
  - ○ E.g. by design phase of the software security development lifecycle (SDL) process

Threat modeling steps

1. **Identify security objectives**
   - ○ Understand your integrity, confidentiality, and availability goals
2. **Application overview**
   - ○ Understand application and its components (libraries and services), data flows and trust boundaries.
3. **Decompose application**
   - ○ Document what each component does, entry and exit points, data flows and trust boundaries.
4. **Identify threats**
   - ○ Done for each individual components
   - ○ E.g. a misconfiguration (e.g. bad password policy, outdated encryption)
5. **Identify vulnerabilities**
   - ○ End with vulnerabilities, overall assessment, prioritization of risks.

Security Development Lifecycle (SDL)

- Set of guidance, best practices, tools, and processes by Microsoft
- Consists of different phases with different actions on each phase:

    1. **Training**
        - Core security training for developers
    2. **Requirements**
        - Setting level of security desired
    3. **Design**
        - Threat modeling
        - Attack surface analysis
        - Requirements
    4. **Implementation**
        - Static analysis
        - Turning off unsafe functions
    5. **Verification**
        - Dynamic analysis
        - Fuzz testing
        - Attack surface reviews
    6. **Release**
        - Incident response plan
        - Final security review
        - Certification
    7. **Response**
        - Allow reporting security problems in products

Incident management

- 📝 Process of identifying, prioritizing and solving security incidents.
- Goal: Restore the system back to normal, trigger alerts to prevent any potential risks.
- 📝 Steps (flexible, not a strict rule):
    1. **Preparation for incident handling and response**
        - You know how you'll handle it when it happens.
        - Policies, trainings, tools, guidelines...
    2. **Detection and analysis**
        - Conduct in-depth analysis to what has happened: why, how, where, what
    3. **Categorization and prioritization**
    4. **Notification**
        - Notify proper people who are affected and who can act on it.
    5. **Containment**
        - Prevent the occurring incident from causing more damage.
        - E.g. put them in quarantine then we'll figure out what to do
    6. **Forensic investigation**
        - What happened, why?
    7. **Eradication**
        - Wipe the threat completely
    8. **Recovery**
        - Restore the system to working state
    9. **Post-incident activities** (lessons learnt)
        - Record what happened with final review.
        - Have discussion about how to avoid it in future.
- 🌐 E.g. a developer in Dropbox miscoded authentication function to always return true.
    - Anyone could login as whichever you user you want by just typing their e-mail.
    - They had review policy but no one paid attention.
    - They had protocols against major breach.
    - Realized that it was critical and then they brought down the service to prevent huge damage (containment)
    - Conducted investigation to see what has happened and started recovery process
    - It was recorded and documented for current and future employees

Emergency response plan

- Help companies address various emergency situations that could occur within their organization.
- Should include who to contact, how to act in an emergency, how to mitigate risk and what resources to use to minimize loss

Security incident and event management (SIEM)

- Real-time analysis of security alerts generated by network hardware and applications.
- Helps <u>SOC</u> to perform its functions
- 📝 Combines SIM and SEM
    - **SIM (Security information management)**
        - Long-term storage as well as analysis and reporting of log data.
    - **SEM (Security event manager)**
        - Real-time monitoring
        - Correlation of events
        - Notifications and console views.
- E.g. <u>Splunk</u> is the most popular SIEM.

SIEM use-cases

- Anomaly detection could help detect zero-days, misconfigurations, cyberwarfare
- Automatic parsing, log normalization and categorization
- Visualization to help with pattern detection
- Detection of covert, malicious communications and encrypted channels.

SIEM components

- **Aggregation**: Combining different log data
- **Correlation**: Using e.g. AI to bundle events with common attributes
- **Alerting**: Automated analysis of correlated events
- **Dashboards**: Helps to see anomalies
- **Compliance**: Can gather compliance data to produce reports that adopt to existing processes
- **Retention**: Critical in forensic investigations as network breach is high likely discovered after it happens.
- **Forensic analysis**: The ability to search across logs on different nodes and time periods based on specific criteria.

Security teams

Security Operations Center (SOC)

- Centralized function within an organization
- Continuously monitors and improves an organization's security posture
- Prevents, detects, analyzes, and responds to cybersecurity incidents.
- Uses <u>SIEM</u> tool to perform its function

Security Incident Response Team (SIRT)

- Also known as **CSIRT (Computer Security Incident Response Team)** or **Computer Emergency Response Team (CERT)**
- Focuses on effective and quick incident response.
- Develops and refines the incident response plan.
- Typically receive threat intelligence from the <u>SOC</u>
- 💡 SIRT should first check effort and potential impact of the incident when begin investigation and response process.

- There are also national CERT teams such as US-CERT in USA, CERT-SE in Sweden and TR-CERT in Turkey.

User Behavior Analytics (UBA)

- Monitoring user behavior in attempt to discover potential threats and attacks.
- When patterns are observed and normal is established, an admin can take a look at deviations.
- E.g. monitoring employee behavior against insider threats
- E.g. login attempts based on the location, monitoring access to privileged accounts.

Network security

Network security controls

- Include: Access control, Identification, Authentication, Authorization, Accounting, Cryptography, Security Policy

Access control

- Restrictions that determine who has access to what on a system/network.
- **Physical access control**

    o Restricts access to physical locations and buildings.
- **Logical access control**

    o Restricts the access to networks and information.
- Terminology

    o **Subject** = Who's reaching, user or process which accesses the objects
    o **Object** = What's being reached, resources upon which the restrictions are placed
    o **Operation** = Verb, What's being done, the action performed by the subject on the object
    o **Reference Monitor** = implements the rules which define what actions on the object can a subject perform
- Involves

    o **Identification**: unique identity in any given system

        ▪ There are your credentials
        ▪ e.g. social security number, username and password.
    o **Authentication**

        ▪ You're granted access via credentials
        ▪ You use the credentials
    o **Authorization**:

        ▪ What you can access, where you can go, can you park somewhere
    o **Accounting**

        ▪ Act of logging and creating account of all actions, what has been done.

Network security zoning

- Grouping networks for efficient management of networks.
- Any network has physical firewalls (routers) which has software to act as firewall and control the traffic

    o However it's hard to manage each network instead best to group them in zones and apply rules in that zone.

Security zone

- Group of similar people or systems by characteristics e.g. functionalities to apply same rules.
- Properties include:
  - Active security policies in regard to the network traffic
    - E.g. to implement the policy "secretaries cannot reach twitter", can block those sites through firewall rule in their zone
  - Detection and blocking of malicious traffic
    - Software needs to actively scan and label what's malicious or not and stop malicious traffic
  - List of known IP addresses and address sets
    - IP address of device and interface are different
  - List of the zone interfaces
- A device or an interface can can have multiple IP addresses
  - E.g. wired connection has one interface, another interface to connect to DB
  - **Maintenance interface**
    - Last resort to fix stuff
    - Usually no security boundaries/guards on those interfaces
    - Must have physical security
    - E.g. someone goes in to server room in cold jacket codes, plugs in a laptop and uses maintenance interface to fix something.

Zone examples

- **Internet zone**
  - Uncontrolled zone out of boundaries of an organization.
- 📝 **DMZ Zone**
  - Controlled zone.
  - Also known as demilitarized zone
  - Provides a barrier between the external and internal networks.
  - Included in every router.
  - Uses firewalls control what can go in and out.
- **Production zone**
  - Restricted zone.
  - Firewalls are used to filter inbound and outbound traffic
  - Access from uncontrolled networks is strictly controlled.
- **Intranet zone**
  - Controlled zone with less restrictions
- **Management zone**
  - Secured zone which enforces strict policies and limits access to a few authorized users.

Security policies

- Rules and requirements that the system has to have to achieve information assurance.
- Defines everything about your layout for the employees
- Written documents including
    - Lists of allowed hardware and software
    - Locations for related policies and procedures
    - Exceptions i.e. exemption rules
    - Sanctions for noncompliance e.g. disciplinary actions/punishment/termination
    - ...
- Types
    - **Technical policies**: define the system configuration
    - **Administrative policies**: define the behavior of employees
- Mitigates risks, prevents something costly from happening.
- E.g. a good policy is NDA, distributed and cannot be repudiated (signed)

Policy types for risk tolerance

- 📝 From most permissive to most strict
    1. Promiscuous: No restrictions
    2. Permissive: If something is malicious it's blocked.
    3. Prudent: Restrictive
    4. Paranoid: Highest restrictions

Promiscuous policy

- No restrictions on system resources.
- Do whatever you want
- 💡 Only good when you have bunch of highly trained & well-informed people with proven track record working in a team because otherwise policies would slow them down

Permissive policy

- Begins as wide-open, can do anything
- When it knows something is malicious, it'll be blocked

Prudent policy

- Provides maximum amount of security
- Allows only safe stuff
- Very restrictive
- A lot of things are locked up

Paranoid policy

- Something of such high importance, not worth to take smallest of risks, e.g. government data regarding to citizens

    - E.g. access only from police station, they need to submit why they access, lethal data
- 🙃 In Linux firewall there's a command called panic that's equivalent to this: Drops all traffic

Sub-policies

- Policy types are not limited to the listed.

Password policy

- Guidelines for using strong password protection on available resources.
- E.g.

    - At least 8 characters in length
    - Must include upper/letter/number/symbols

User account policy

- 📝 Defines the account creation process, authority, rights and responsibility of user accounts.
- E.g.

    - Put users in groups and decides what the groups can do.
    - What needs to be done during account creation

Information protection policy

- 📝 Guidelines to users on the processing, storage and transmission of sensitive information
- Goal is to ensure information is appropriately protected from modification or disclosure
- E.g.

    - Setting level of sensitivity to information
    - Dictates who has access to information
    - Determines how information is stored and transmitted
    - Describes how information should be deleted from storage media

Special access policy

- Custom rulings for specific scenarios for specific individuals and services
- The terms and conditions of granting special access to system resources.

Email security policy

- Governs the proper usage of corporate email.
- E.g.

    - Verify proper signature
    - Never click on links, because they'll never be sent

Acceptable use policy

- Same as **Terms of Service** or **Terms of Use**
- 📝 Description of what constitutes acceptable and unacceptable use of the Internet
- Code of conduct governing the behavior of a user whilst connected to the network/Internet.
- E.g.
  - ISP providers allows you to use unlimited bandwidth
    - In contract you see it says it's about "fair use"
    - Fair use can be e.g. to not exceed 50% maximum potential bandwidth that could be used with that bandwidth
  - Prohibiting port scanning or security scanning
  - Never revealing a password

Access control policy

- 📝 Governs resources being protected and the rules that control access to them
- Who can access what (humans <-> services)
  - E.g. limited access to routers and switches on top floor
  - E.g. regulating electric socket placement as someone can connect a Raspberry Pi that can be listening
- What can access what (services <-> services)

Remote access policy

- 📝 Defines acceptable methods of remotely connecting to the internal network
- Applies to both who and what
- E.g. enforcing VPN, strong passphrases, defining vendor access and requiring monitoring

Firewall management policy

- Governs access, management and monitoring of firewalls in an organization.
- Who'll monitor? How will it be monitored?
- What kind of firewall that'll be used?

Network connection policy

- Defines who can install new resources on the network, approve the installation of new devices, document network changes etc.
- Protects both yourself and the company
- E.g. must always use VPN if not working from office

Network security policy

- 📝 Outlines rules for computer network access, determines how policies are enforced
- Governs e.g. • data access • web-browsing habits • use of passwords and encryption • email attachments.

Encryption policy

- Dictates which encryption to use
- Goal is to avoid weak and obsolete algorithms
- Easier if everyone uses same algorithm
- Used by e.g. cloud providers, ISP providers

Authentication policy

- Limits ability to be authenticated under some conditions
- E.g. no coffee shop wireless, only through VPN and using MFA

Implementation

- Steps

    1. Perform a risk assessment
    2. Utilize standard guidelines
    3. Include senior management
    4. Define sanctions
    5. Distribute the final version
    6. Ensure that employees have read the policy
    7. Enforce policies
    8. Educate and train employees
    9. Review and update the policy
- Human Resource department has the responsibility to

    - educate and train employees in practices defined by the company's security policies
    - monitor the implementation of the policies
    - enforce penalties

Top-down vs Bottom-up

- **Top-down**

    - Begins with management establishing a framework for initiating and implementing security practices in the enterprise. ¨
    - Most important way to ensure employees across an organization will support and follow the policies
- **Bottom-up**

    - Occurs when the system administrators and security personnel try to establish a security program on their own without senior management support and enforcement.

Physical security

- The protection of all assets of an organization from all sorts of threats and attacks.
- Helps in

    Preventing unauthorized access to the system
    - Preventing any kind of data manipulation and theft
    - Protecting the system against malicious activities such as espionage, damage and theft
    - Protecting employees and preventing social engineering attacks
- Categories

    - **Natural or environmental threats**

        - E.g. flood, fire, earthquake, dust
    - **Man-made threats**

        - E.g. Terrorism, wars, explosions, <u>dumpster diving</u> and theft, vandalism.
- See also <u>Physical security | Social engineering</u>

Types of physical security controls

Preventive controls

- Implemented before a threat event to reduce or avoid its impact.
- Includes access control mechanisms to prevent access
- Can be **technical** e.g.

    - Firewalls
    - Authentication systems.
- Can be **administrative** e.g.

    - Security policies
- 📝 Can be **physical** e.g.

    - Fire extinguishers
    - Doors e.g.

        - **Mantrap**

            - Also known as air lock, sally port or access control vestibule
            - Has two doors, each door requiring a separate form of authentication to open
        - **Turnstile**

            - Also known as a turnpike, baffle gate, automated gate
            - Allows one person to pass at a time, can enforce one day direction
            - Can require a a coin, a ticket, a pass, or similar
            - E.g. in train stations
    - **Bollard**

        - Sturdy, short, vertical post
        - Used for control road traffic and posts
        - Allows to prevent ram-raiding and vehicle-ramming attacks.

- ▪ 🚪 Used initially for mooring boats

Static electricity

- Low humidity can cause a buildup of static electricity.

    - ○ Leads to corrosion of the components could.
    - ○ 💡 Keep humidity level between 45% and 55%.
- Grounding systems help

    - ○ E.g. antistatic wrist straps are designed to ground people appropriately
    - ○ Provides somewhere for any latent static electricity generated to flow.

Detective controls

- In place to let you know when something has happened or is happening.
- Detects violations and intrusion attempts for investigation.
- E.g. • audit trails and logging • alarm systems • sensors • video surveillance • motion detectors.

Deterrent controls

- Also known as **deterrence controls**
- Warns intruders to stay away
- E.g. signs showing • "Be aware of the dog" • "Under surveillance" • "Authorized personal only"

Recovery controls

- Used after violation has happened to restore the system to its persistent state
- E.g. backup systems and disaster recovery

Compensation controls

- Do not prevent attacks, used when everything else fails
- Goal is to restore everything back to normal
- E.g. when there's power shortage you need a grid, alternative energy backing: generators, batteries..

Physical security measures

- Secure premises and company surroundings
- Secure the reception area
- Lock servers and workstations when not in use
- Lock devices such as modems, removable media, and fax machines when not in use
- Implement access control
- Regularly maintain computer equipment
- Prevent wiretapping
- Monitor the environment by checking the humidity and temperature
- Positive pressure is great at keeping contaminants (e.g. dust, dirt) out of the data center

Data leakage, backup and recovery

Data leakage

- Any sort of unauthorized disclosure of sensitive information from anyone/any system.
- Includes emails, malicious links, device theft etc.
- Data leakage leads to
    - loss of trust e.g. trust to governments decreased during late years
    - loss of profit e.g. Sony lost profit of their movies after they were leaked before publishing

Data leakage threats

External threats

- Corporate espionage, phishing, malware
- Business partners, consultants when company outsources
    - Less surveillance than own employees.

Internal threats

- Also known as **insider threats**
- Dangers are greater than external threats as they'll have greater access to the company
- See also insider attacks
- E.g. eavesdropping, shoulder surfing, dumpster diving can be used to acquire data.

Data loss prevention

- Also known as **DLP**
- Identification and monitoring of important information that is not to be shared outside the organization.
- Can block, notify the sender or lets admins to analyze, react and report to sensitive data in transit.
- Important tool for enterprise message systems
- Uses different techniques of data access control
    - E.g. when e-mailing where content is scanned for fingerprints, classifications and bank account numbers.

Data backup

- Process of making a duplicate copy of data that already exists.
- Protects against data loss and corruption as it can lead to great financial damages.
- No backup = Far more suspectable to all sorts of attacks, especially ransomware.

Backup mediums

Magnetic tapes

- Oldest form, still used by many enterprises.
- Retention time: ≈30 years
- 📝 To pull anything off the tape, you have to fast-forward to wherever the correct file is stored
    - Good for restoring systems in one go.
    - Bad for incremental backups or storing a few files.
    - ⏻ Only way to tell if backups are working is to fully restore from the tape and check if it's correctly restored.

Optical disks

- 2 to 3 times slower than hard drives
- Retention time: ≈25 years

Hard disks

- Cheaper, easily accessible
- Less stability than magnetic tapes
- Retention time: ≈9-20 years

SSD disks

- Includes also usb drives known as Flash storage or thumb-drive.
- Resistant to shock, temperature, being run through the washing machine
- Retention time: ≈10 years

Cloud storage

- Requires little infrastructure
- Depends on stable internet connection
- No retention time, high reliability

SD and micro-SD

- Little capacity and pricy.
- Retention time: ≈10 years

Steps of data backup strategy

1. **Identify important data**
    - because backing-up everything is too costly and takes up much storage.
2. **Choose appropriate backup media**
    - Reliable, solid, preferably cheap
    - E.g. USBs or portable media for personal users, and HDD/SDDs for companies for more speed.
3. **Choose the appropriate backup strategy**

- Check features such as scheduling, monitoring file changes to update back-ups, protocols, integrations...
- Paid vs Free
  - Free requires more knowledge and work, training costs (one time)
    - E.g. in Linux, set cron job from point A to B
  - Paid versions has recurring license costs including training

4. Choose appropriate RAID levels

- **RAID 1**
  - 2 disks
  - All that are written in disk A is also written to B, if one disk fails, other works
- **RAID 5**
  - 3 disks
  - If A fails you can reconstruct based on data in B and C
- RAIDing is not only for backups, can also use for faster read and writes
  - E.g. BIG = Everything is seen as one drive. File is written two all of them. Crazy write & read speeds. If single disk dies all data is gone.

5. Choose the appropriate backup method

- **Cold backup**
  - Performed while system is not in use.
  - E.g. at nights, during weekends.
- **Hot backup**
  - Performed when system is still used.
  - E.g. you type a document, power shortage happens but it's still saved.
- **Warm backup**
  - Hybrid of the two.
  - Period backups while system is in use, but you might lose longer time period than hot backup.

6. Choose the appropriate backup locations

- Three options:
  1. **On-site**: Same building / room
     - Susceptible to same types of problems like other servers.
     - If there's a breach, fire or earthquake = all data are gone
  2. **Off-site**: backup is performed at a remote location
  3. **Cloud**:
     - Most secure: most cost effective and safe where data won't be loss, no electricity, no hardware, no maintainable.
     - Can be replicated in same building, different buildings in same data center or different regions.
     - Can have privacy/trust issues: encrypt

7. Choose the backup type

- **Full backup**: Costly, you back up everything
- **Incremental backup**

- Backs-up on each change of the previous back-up
- When restoring, you need to restore everything from the first full back-up
  - **Differential backup**:
    - Back-ups on difference to the initial backup on each backup.s
    - Faster restoring time as you only need the last point and the initial full back-up

8. **Appropriate backup solution**: Combination of all of this

9. **Perform a recovery test**

- Ensure you can recover a data that's lost with DR tests e.g. twice a year.
- **Recovery drill**
  - Simulating data tier outage
  - Recovering
  - Validate application integrity post recovery

Data recovery

- Recovering lost data
- Reasons
  - Accidental lost e.g. • natural disaster • corrupted data
  - Or can be intentionally destroyed
- DR stands for "Disaster Recovery"
- Most of data is recoverable but you can have recovery failure if backed up data becomes corrupt.

Identity and access management (IAM)

- Ensures right users have access to right resources at right time
- Framework of best-practices used by organizations
- Main modules:

  1. **Access Management Module**: • Authentication • Authorization.
  2. **Identity Management Module**: Management of users and enterprise directory service components of IAM.

IAM components

Access management

Authentication

- Session Management
- Password Service

Single sign-on (SSO)

- Also known as *single sign on*
- 📝 Allows one set of login credentials to be used to access multiple applications
- Centralized session and user authentication service
- Easier administration
- Benefits for users including remembering one password instead of many
- Many user authentication problems can be resolved at a central location at SSO point.

Multi-factor authentication (MFA)

- Authentication method that requires the user to provide two or more verification factors to gain access to a resource

- **Two-factor authentication (2FA)** is subset of MFA using two different factors

- 📝 Authentication factors include
    - **Knowledge** - something only the user knows

        - E.g. password or PIN
        - Vulnerable to recording user screen, e.g. <u>attack against PayPal</u>
    - **Possession** - something only the user has

        - E.g. smart cards, security token
        - Vulnerable to be cloned/copied
    - **Inherence** - something only the user is

        - E.g. biometrics (• fingerprint, face, voice, iris, retinal recognition • behavioral: keystroke dynamics)

            - **Retina**: Sending an intrusive close light to compare blood vessels
            - **Iris**: Mapping structures of iris using a camera.

- - - Vulnerable to manually prompting users, e.g. <u>touch ID scams that targeted Apple devices</u>
  - ○ **Location**: somewhere the user is
    - - E.g. based on network, known country
    - - Vulnerable to proxies

One-time password (OTP)

- A password that's only used once and only valid for a limited of time-
- Enforces strong password authentication as it protects against someone getting access to password.
- Usually used when authenticating to VPN, and online Internet banking systems.

OTP Token

- Tool used to generate one-time passwords
- Can be a hardware device or software token installed on the computer or phone.
- Authenticating server use the same algorithm as token to be able to validate the code.
- 📝 **Token types**
  - ○ **Synchronous Tokens**
    - - **Clock-based tokens**
      - - Also known as **Time-based tokens**
      - - Tokens have same time configuration as the authenticating server.
      - - Both use algorithms that are based on a time and a shared secret key.
    - - **Counter-based tokens**
      - - Both the token and the authenticating server maintain a counter.
      - - Code consists of the value from the counter and a shared secret key.
      - - Requires one or more actions from users (e.g. powering on or PIN number) to increment the counter.
  - ○ **Asynchronous Tokens**
    - - Also known as · **challenge-response tokens** · **challenge/response tokens**
    - - Server sends a challenge (random value) to user and expects user to enter it.
    - - Protects against replay attacks

Authorization

- Rule-based Authorization
- Attribute-based Authorization
- Remote Authorization

Role-based authorization

- Restricting system access to authorized users
- Can implement
  - ○ **Mandatory access control** (MAC)
    - - OS-enforced access control based on subject's clearance and object's labels

- Assigns sensitivity labels to data and controls access by matching the user's security level to the resource label.
- E.g. traditional Unix system of users, groups, and read-write-execute permissions
    - **Discretionary access control** (DAC)
        - Restricting access to objects based on the identity of subjects and/or groups to which they belong
        - Allows the data owner to set security permissions for the object
        - E.g. unix file mode which represent write, read, and execute in each of the 3 bits for each of User, Group and Others
        - E.g. on Windows, you can set sharing and permissions on files/folders you create
- RBAC vs MAC vs DAC

Access Control	User rights	Popular
Discretionary	Full control	OS file systems
Mandatory	No control, policies are predefined by root/admin	OS file systems
Role based access	No control, policies are predefined by root/admin	Cloud computing

Identity management

User management

- Delegated administration
- User and Role Management
- Provisioning
- Password Management
- Self-service
- **Compliance Auditing**
    - Conduct security audit for company to be compliant with policies/regulations

Enterprise directory service

- Central repository where all others components gets their data
- Includes
    - Directory service
    - Data synchronization
    - Metadirectory
    - Virtual directory

Threat intelligence and forensics

Cyber kill chain

- Framework for identification and prevention of cyber intrusions activity.
- Developed by Lockheed Martin
- Identifies what the adversaries must complete in order to achieve their objective.
- 😄 Based on military kill chains, a concept consisting of • target identification • force dispatch to target decision • order to attack the target • the destruction of the target
- 😄 Critiques states it only defends "perimeter" and isn't suitable model to insider threats.
- E.g. A "Kill Chain" Analysis of the 2013 Target Data Breach

Cyber kill chain steps

- ▯ Not same in every organization as different organizations have constructed their own kill chains to try to model different threats

1. **Reconnaissance**
   - Collecting as much as information about the target.
   - E.g. harvesting email addresses, conferece information etc.
   - See also footprinting

2. **Weaponization**
   - Analyzing collected data to identify and vulnerabilities to exploit to gain access
   - E.g. creating a phishing campaign based on collected data

3. **Delivery**
   - Weaponized bundle to the victim via email, web, USB, etc.
   - Key to measure the effectiveness of the defense strategies implemented by the target.
   - E.g. sending phishing emails

4. **Exploitation**
   - Execute code on victim's system.
   - E.g. arbitrary code execution, authentication and authorization attacks

5. **Installation**
   - Installing malware on the asset
   - E.g. backdoor to gain remote access and maintain access in the network

6. **Command and control**
   - Allows remote manipulation/exploation of victim
   - Done by establishing two-way communication between the victim and the attacker.
   - Evidence is usually hidden using encryption techniques

7. **Actions on objectives**
   - With hands-on access, intruders accomplish their original goals.
   - E.g. • distrupting network • gaining access to confidential data

Defensive courses of action

1. **Detect**: determine whether an attacker is poking around
2. **Deny**: prevent information disclosure and unauthorized access
3. **Disrupt**: stop or change outbound traffic (to attacker)
4. **Degrade**: counter-attack command and control
5. **Deceive**: interfere with command and control
6. **Contain**: network segmentation changes

Threat identification

Tactics, Techniques, and Procedures (TTPs)

- Concept in terrorism and cyber security studies

- Identifies patterns of behavior of the threat actors (= bad guys)

- Aids in

    - counterintelligence for threat prediction and detection
    - implementing defenses
    - profiling threat actors e.g. APT groups

- E.g. In 2020 United States federal government data breach, used TTP were stealing SAML tokens to attack SSO infrastructure according to TTP analysis from NSA.

- Read more at NIST Special Publication 800-159

Tactics

- Also called **tools** in the acronym

- Highest-level description of the behavior

- Describes ways attacker attacks from start to end

- E.g.

    - Way of gathering information e.g. open-source intelligence, social engineering.
    - Way of initial compromise e.g. tools, zero-day vulnerabilities, obfuscation methods

Techniques

- Technical methods used by an attacker

- Gives a more detailed description of behavior in the context of a tactic.

- E.g.

    - social engineering techniques in early stages
    - exploit tools at middle stages
    - and software tools to clear logs to cover tracks at later stages.

Procedures

- Lower-level, highly detailed description in the context of a technique.
- Sequence of actions done by attackers
- E.g. an actor collects business e-mails of target company then launches a spear phishing campaign

Adversary behaviors

- Method or techniques used by attacker to penetrate victim network.
- E.g. using PowerShell, DNS Tunneling, Web Shell etc.

Indicators of Compromise (IoCs)

- Artifacts observed that indicates computer intrusion with high confidence.
- 4 categories:
  - **Email indicators**
    - E.g. sender's email address, subject, attachment, links.
  - **Network indicators**
    - E.g. URLs, domain names, IP addresses, unusual DNS requests
  - **Host-based indicators**
    - E.g. filenames, file hashes, registry keys, DDLs, mutex
  - **Behavioral indicators**
    - E.g. memory code injection, remote command execution, document execution PowerShell script.

Laws, standards, and regulations

Legal systems

- Two main categories of legal systems in World. Many systems mix those:

  1. Common law

     - Unwritten laws based on legal precedents established by the courts.

     - E.g. USA, UK, India and Canada

     - Two main branches:

       - **Civil law (in common law)**

         - Between individuals, organizations, or between the two
         - Focuses on dispute resolution and victim compensation
       - **Criminal law**

         - Includes the punishment and rehabilitation
         - Proscribes conduct threatening, harmful, or otherwise endangering to the property, health, safety, and moral welfare of people inclusive of one's self

  2. Civil law

     - Codified statutes and legal codes predominate
     - E.g. majority of countries including Germany, France, Spain, Sweden, Turkey..

PCI DSS

- Payment Card Industry Data Security Standard

- Applies to organizations that card payments and all entities involved in the process of card payment.

- Global data security standard

- Common sense steps presenting best security practices

- 📝 Requires tester to notify organization if cardholder data is accessed during a penetration test

  "If cardholder data is accessed during the penetration test, it is important that the tester notify the organization immediately" PCI DSS Guidance recommends:

- See also the official guide, or the simpler version.

PCI DSS Requirements

- Build and maintain a secure network

  - **(1)** Install and maintain a firewall
  - **(2)** Do not use vendor-supplied defaults for any security parameters (e.g. passwords)
- 📝 Protect cardholder data

  - **(3)** Protect stored data

    - Storing cardholder data is discouraged, but if stored it must be encrypted or hashed.

- Never store sensitive data on the magnetic stripe or chip including PIN and CAV2 / CVC2 / CVV2 / CID.
    - **(4)** Encrypt transmission of cardholder data across public networks
- Maintain a vulnerability management program
    - **(5)** Use and regularly update anti-virus software
    - **(6)** Develop and maintain secure systems and applications
- 📝 Implement strong access control measures
    - **(7)** Restrict access to cardholder data by business need-to-know
    - **(8)** Assign a unique ID to each person with computer access
    - **(9)** Restrict physical access to cardholder data
        - Store media back-ups in a secure location, preferably off site.
        - Review and confirm that back-up media is secure at least annually.
- 📝 Regularly monitor and test networks
    - **(10)** Track and monitor all access to network resources and cardholder data
    - **(11)** Regularly test security systems and processes
        - **(11.1)** Test presence of wireless access points on a quarterly basis
        - **(11.2)** Network vulnerability scans at least quarterly and after any significant change
        - **(11.3)** Penetration testing at least once a year and after any significant change
- Maintain an information security policy
    - **(12)** Maintain a policy that addresses information security

ISO/IEC 27000-series

- Set of worldwide information security standards
- Also known as ***ISMS Family of Standards*** or ***ISO27K***
- ISO/IEC stands for
    - "The International Standard for Standardization (ISO)"
    - and "The International Electrotechnical Commission (IEC)"

ISO/IEC 27001:2013

- Titled as "Information technology - Security Techniques - Information security management systems — Requirements"
- Defines requirements for the organization's information security management system.
- Applies a risk management process
- Used
    - To create security requirements and objectives
    - To ensure the cost efficiency of managing the security risks
    - To ensure that laws and regulations are followed
    - For defining new information security processes
    - For identifying and clarifying existing information security processes.
    - For determining the status of information security management activities in an organization
    - For implementing business information security
    - For providing relevant security information to customers

ISO/IEC 27002

- Titled as "Information technology – Security techniques – Code of practice for information security controls".
- Information security controls to enforce best-practices
- Includes controls for e.g. • Access Control • Cryptography • Access Control • Physical and environmental security...

HIPAA

- Health Insurance Portability and Accountability Act
- 📝 Provides data privacy and protection of medical information.
- Specifies administrative, physical, and technical protection for all entities involved.
- 🙊 Initially created to protect people from losing their health insurance e.g. when changing jobs.
    - Extended to reduce costs and administrative burdens of healthcare transactions.

HIPAA transactions

- **Healthcare transaction**
    - A transaction is an electronic exchange of information between two parties to carry out financial or administrative activities related to health care
    - Usually represented by claims and enrollment data
    - E.g. a health care provider will send a claim to a health plan to request payment for medical services.
- 📝 **Standard transactions**
    - Adopted standard by HSA (U.S. Health & Human Services) under HIPAA
    - Include • payment and remittance advice • claims status • eligibility • premium payment • enrollment and disenrollment • referrals and authorizations.

HIPAA rules

- **Electronic transaction and code sets standards**
    - Every provider who performs electronic transactions needs to use the same health care transactions, codes, and identifiers.
- **Security rule**
    - Ensures the confidentiality, integrity, and security of health information
- **Enforcement rule**
    - Details provisions in regard to the compliance, investigations, violations, and hearing procedures.
- **Privacy rule**
    - Protects a person's health information and defines who has the access to the information.
    - Controls include
        - **Administrative safeguards** such as • performing risk analysis • employee training • security policies and procedures • business associate agreements
        - **Physical safeguards** such as • access controls • policies for workstations (e.g. laptops) • workstation security

- **Technical safeguards** such as • access control • audit control • integrity control • transmission security
- 📝 **National identifier requirements**
    - **National Provider Identifier (NPI)**: A 10-digit number used for covered healthcare providers
    - **National Health Plan Identifier (NHI)**: An identifier that is used for identifying health plans.
    - **Employer Identifier Standard**: A number that identifies employers on standard transactions.

FISMA

- Federal Information Security Management Act
- 📝 US legislation that regulates federal data security standards and guidelines.
- Protects government information, operations and assets against various threats.
- Provides
    - Standards for
        - categorizing information and information systems by mission impact
        - minimum security requirements for information and information systems
    - Guidance for
        - choosing appropriate security controls for information systems
        - assessing security controls in information systems
        - the security authorization of information systems

NIST SP 800-53

- Shorthand for National Institute of Standards and Technology Special Publication 800-53
- 📝 Security and privacy controls for federal information systems and organization
- Guidelines to assist in FISMA compliance

Sarbanes-Oxley act

- Also known as **SOX** or **Sarbanes Oxley** act.
- US federal law
- Protect investors by making corporate disclosures more reliable and accurate
- Regulates what records organizations must keep and for how long
- E.g. banks need to save financial reports for a very long time
- The act contains 11 titles
    1. Public company accounting oversight board
    2. Auditor independence
    3. Corporate responsibility
    4. Enhanced financial disclosures
    5. Analyst conflicts of interest
    6. Commission resources and authority
    7. Studies and reports

8. Corporate and criminal fraud accountability
9. White-collar-crime penalty enhancement
10. Corporate tax returns
11. Corporate fraud accountability

DMCA

- Digital Millennium Copyright Act

- Copyright laws in the USA

- Implements

  - WIPO (World Intellectual Property Organization) Copyright Treaty
  - WIPO Performances and Phonograms Treaty
- Against theft of intellectual property

- E.g. platforms must act as they can not benefit from what is yours, most platforms have copyright notice that you can issue.

- Act contains five titles:

  1. WIPO Treaty Implementation
  2. Online Copyright Infringement Liability Limitation
  3. Computer maintenance or repair
  4. Miscellaneous provisions
  5. Protection of certain original designs

COBIT

- Framework created by ISACA for information technology (IT) management and IT governance.

- Helps companies follow law, be more agile and earn more.

- Links business and IT.

- Ties in with COSO, ITIL, BiSL, ISO 27000, CMMI, TOGAF and PMBOK.

- Defines processes for the management of IT

  1. Evaluate, Direct and Monitor (EDM)
  2. Align, Plan and Organize (APO)
  3. Build, Acquire and Implement (BAI)
  4. Deliver, Service and Support (DSS)
  5. Monitor, Evaluate and Assess (MEA)
- Components include

  - **Framework**: Link IT objective and best practices to business requirements.
  - **Process descriptions**: Process model to build common language for planning, building, running and monitoring.
  - **Control objectives**: High-level requirements to be considered by management.
  - **Management guidelines**: Helps assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.
  - **Maturity models**: Assesses maturity and capability per process and helps to address gaps.

EU Laws

SCCs

- Standard Contractual Clauses
- Contract between an EU based data exporters and a non-EU-based data importers
- Protects personal data sent from the European Union (EU) to countries with lower level of data protection rights
- Ensures GDPR requirements in territories which are not considered to offer adequate protection to the rights and freedoms of data subjects

EU–US Privacy Shield

- Also known as **PrivacyShield**
- Framework for regulating exchanges of personal data for commercial purposes between the European Union and the United States
- Enables US companies to more easily receive personal data from EU entities
- Became invalid in 16 July 2020 as it did not protect EU citizens on government snooping

Safe Harbor

- Also known as **International Safe Harbor Privacy Principles, Safe Harbour Privacy Principles, Safe Harbour decision**
- Signed between US and EU to prevent customer data leakage from private organizations
- Seven principles include: notice, choice (can opt out), onward transfer (only share with compliant companies), security, data integrity, access (can be accessed and deleted by individuals), enforcement
- Abolished in October 2015 and replaced with EU–US Privacy Shield

GDPR

- Regulates data processing of EU citizens
- Applies in EU and outside of EU if personal data is collected from EU
- Requires consent to collect data
- **Privacy by design**: Enforces privacy and security measures
- Gives rights such as: • right to be informed • right of access • right to rectification • right to erasure (right to be forgotten) • right to restrict processing • right to data portability • right to object • right in relation to automated decision making and profiling.

Common Criteria

- Also known as **ISO/IEC 15408**
- Standard for computer security certification
- Tests to evaluate vendor claims of security about its products
- Four aspects to the of evaluation
  - **TOE**: the system being tested
  - **ST** (security target): he documentation describing the TOE and requirements)
  - **PP** (protection profile)
    - The requirements for the type of product being tested)
    - The evaluation assurance level (EAL, the rating level, ranked from 1 to 7).

Other laws, standards and regulations

- **RFC 1918**: Private IP Standard
- **RFC 3227**: Collecting and storing data
- **CAN-SPAM act**: Email marketing
- **GLBA**
  - Gramm-Leach-Bliley Act
  - Requires financial institutions to take steps to protect customer information
- **FERPA**: Education Records

Hacker types

Hacker

- An individual who uses their computer and technical skills to gain access to systems and networks.
- 😬 A common theory is that a hacker meant initially anyone who possessed skills and knowledge and determination to solve problems in a creative way.
    - There are arguments against it never was a benign term and the malicious connotations of the word were a later perversion is untrue.

Black hat hackers

- 📝 Uses knowledge and skills to discover and exploit security vulnerabilities for financial gain or other malicious reasons
- Bad guys
- No regard of law & regulations etc.
- Activities include stealing personal and financial information or shutting down websites and networks
- E.g. bank robbing

White hat hackers

- Also known as **ethical hackers**
- 📝 Uses knowledge and skills to improve a system's security by discovering vulnerabilities before black hats do.
- Will not break laws and regulations
- Scope is determined by the client
- E.g.
    - Publish vulnerabilities
    - Do penetration tests
    - Participate in bounty programs to claim rewards.
        - Benefiting financially from hack is not illegal

Ethical hacking

- Also known as white hat hacking
- Performed by security specialists to help companies identify vulnerabilities in their networks and systems.
    - Helps them analyzing and strengthening their system and network security
    - Allows for creating preventive measures that should prevent any future security breaches as well as protect data and information stored in the system.
- Difference from black-hat hacking:

- Hacking with permission of system owner
      - They remain compliant to the law
      - Purpose is to prevent hackers from breaking into systems and networks.
  - Flow

    1. Find vulnerabilities
    2. Assess problems & threats about them
    3. Offer solutions e.g. you can do to fix this
    4. Inform within the company
  - Ethical hackers should ask themselves when evaluating a system: (also companies asks often "why would we fix it?" in three questions)

      - What is it that an attacker can see on this network/system?
      - What could the attacker do with that knowledge?
      - Are there any traces of attempted attacks on the system/network?

Ethical hacking scope

  - No test should be performed without appropriate permissions and authorization.
  - Test results should be kept confidential
  - Only those tests that the client requested should be performed

Grey hat hackers

  - Also known as *grayhat*, *gray hat*, *gray-hat*, *grey hat*, *greyhat* or *grey-hat* hackers.
  - 📝 Might break laws, regulations and ethical standards but do not have explicitly malicious indent.
  - Middleground; Not as bad as black, not as ethical as white hackers.

Suicide hackers

  - 📝 Perform attacks for a cause despite the risk of being caught and prosecuted.
  - E.g. they'll know for sure that they'll get caught but they still attempt the hack for a "cause".

Script kiddies

  - 📝 Inexperienced hackers who don't have enough knowledge or skills to perform hacks on their own

      - Instead, they use tools and scripts developed by more experienced hackers.
  - Dangerous because running the closed-sourced tools on one's own system is a big risk.

Cyber terrorists

  - Money is not the priority, but to destroy stuff.
  - Influenced by religious or political beliefs.
  - 📝 Goal is to promote fear, unrest and disruption.

State sponsored hackers

  - 📝 Recruited by governments
  - Gain access to classified information of other governments

- Information source can be governments, individuals or corporations.

Hacktivists

- 📝 Break into government and corporate systems out of protest.
- Promotes political or social agenda.
- E.g. steal and leak data on public domain

Hacking stages

1. Reconnaissance

- Also known as **footprinting**, **fingerprinting** or **information gathering**
- 📝 Reconnaissance, *noun*, preliminary surveying or research about the target.
- 📝 Necessary first step as an attack would not be successful without it.

2. Scanning

- Hacker utilizes information from previous stage to conduct more technical scan.
- Often maps the routers and firewalls
- Use tools such as port scanners, network mappers, vulnerability scanners, etc.

Reconnaissance vs Scanning

- In scanning you're acting on gathered information to gather information
- Examples

Reconnaissance	Scanning
Scan the perimeter network you need the IP addresses	Use e.g. `nmap` to figure out what the configuration is.
Get e-mails.	Use phishing to gather personal data
Learn where service physically are	Do dumpster diving

3. Gaining Access

- Attack stage
- Steps:

  1. Find an entry point to the target OS or application on the system

  2. Use it to perform the attack

     - Hackers may escalate privileges to gain complete control over the system/network.
- Examples:

  - Password crack with brute-force or dictionary attack
  - Exploit buffer overflow
  - Session hijack
  - DoS attacks

4. Maintaining Access

- Keeping admin/root privileges so hacker can continue using the system.
  - After breaking into a system, you attempt to elevate privileges to do more.

- Maintain persistent access, because your connection might break, then you start again
- Can prevent other hackers from accessing the system by installing backdoors, rootkits, or trojans.
- 💡 You can install tools to give you persistance access and gathers data to use compromise more such as keylogger.
- 💡 You can use the machine as proxy so all traces are lead back to the proxy.
    - You can minimize the risks being discovered this way.
    - 🗡 As pen-tester document those as you'll get other people in trouble

5. Clearing tracks

- Hackers do everything they can do to hide their activities
- Goal is to maintain the access to the system but remain unnoticed in the process.
    - If you're detected: the vulnerability will be patched and you'll lose access.
- Vital to clear all tracks as fast as possible, or if it's possible generate none.
- Activities:
    - Clear certain entries in log files: Not all, or it'll be suspicious
    - Masquerade your activities: Make them as similar as possible as legitimate activities
        - E.g. a good keylogger masquerade itself behind legitimate activities
            - Mimics other programs behavior by adding more behavior.

Penetration Testing

- Simulating of an security attack to
    - discover vulnerabilities (and document)
    - evaluate the security
- Detailed analysis of weaknesses in design, technical flaws, and vulnerabilities in organizations information security.
- E.g. • phishing • testing authentication using dictionaries • test if router is using an obsolete OS

Purpose

- Identify threats
- Reduce security expenses
    - E.g. you can recommend cheaper router and switches that'll be enough for their capacity and still secure.
    - **ROSI = Return on security investment**
        - E.g. you'll save company for 100% payback if they implement anti-junk system and junk e-mails cost more to the company.
- Provide complete security assessment
- Maintain industry standards and regulations
- Follow best practices
- Test security controls
- Improve current security infrastructure
- Pay particular attention to severe vulnerabilities
    - E.g. explain what one single vulnerability can lead to what kind of damage.
- Prepare steps for preventing exploitations
- Test network security devices

Activities for a good penetration test

- Defining the penetration test parameters
    - States what pen-tester can do and cannot do.
    - Have both signed.
- Engaging skilled penetration testers
- Following non-disclosure agreement
    - Companies don't want to work with someone with bad reputation, e.g. who broke NDA before.
- Selecting appropriate tests
    - Done by the company and the pen-tester together
    - Find cost/benefit ratio of tests
- Using and following a methodology

- ○ 💡 Good to test for all known vulnerabilities to save time and make documentation easier.
- Documenting the results of the test
- Creating a final report

Audit vs Vulnerability Assessment vs Penetration Test

Security audit

- Compliance = Inspects if an organization is following security standards and policies.
- E.g. interviewing staff, vulnerability scans, reviewing access controls, analyzing physical access.
- Often blue/red teaming approach is used by penetration testers.

Vulnerability assessment

- Finds the vulnerabilities in the network
- Will not state if they're exploitable, nor the potential harm

Penetration test

- Includes both security audit + vulnerability assessment
- Discovers vulnerabilities in a system and evaluates its security
- Demonstrates how attackers can exploit the identified vulnerabilities.
- Tells you what measures should be taken to prevent the vulnerabilities.

Blue and red teaming

- Two teams in company, or sometimes outside of the company who battles against each other.
- Similar to capture the flag contest, red is aggressor, blue protects.
- More cost-efficient then hiring an external company to do full penetration testing.
- **Blue team**
    - ○ Defender: Detects attackers (red team) and predict possible attacks.
    - ○ Has full access to the system to analyze the security.
- **Red team**
    - ○ Attacker: Finds vulnerabilities in the system and penetrates to examine what real attackers could do.
    - ○ Has no access to the system
- **Purple team**
    - ○ Both worlds
    - ○ Both attacks and also repairs/suggests improvements

Types of penetration testing

- Consists of white box, black box and grey box testing.
    - ○ 💡 The darker the box is the more credible test results and the higher the costs are. As going from nothing to something as opposed to something to nothing would simulate real-world hacks but would take more time.
- 📝 Each type can be

- Announced vs. Unannounced
  - **Announced testing**
    - IT team are aware of security being tested.
    - Often it occurs when testing a specific segment where IT admins give you access to test different components.
  - **Unannounced testing**
    - IT team is unaware of the security being tested
- Internal vs External
  - **Internal**
    - Targets assets within an corporate network
  - **External**
    - Targets internet-facing assets such as web, mail and FTP servers.

Black box testing

- Also called *zero-knowledge Testing*, *blackbox testing* or *black-box testing*
- 📝 Testers have very little information about the client's infrastructure.
- The goal is to simulate an external hacking or cyber warfare attack.
- provides a very realistic scenario for testing of the defenses
- Can be costlier as it takes much more time to conduct.

Blind testing

- Tester has little information to none about target.
- Target itself (e.g. system administrator) knows about the test and its scope.
- Demonstrates what a real attacker would do.

Double-blind testing

- Also called **zero-knowledge approach**
- Neither the pen-tester nor the target knows anything about each other.
- Good & reliable results
- Most difficult, time-consuming and expensive to perform.

Grey box testing

- Also called *greybox testing*, *grey-box testing*, *gray box testing*, *graybox testing*, *gray-box testing*
- 📝 Tester has partial knowledge i.e. knowledge of the internal workings is limited.
- Combination of black box and white box testing.
- Helps to reduce the cost of the test by gaining knowledge that would be harder to gain otherwise.

White box testing

- Also called *Complete-Knowledge Testing*, *whitebox testing* or *white-box testing*
- 📝 Tester knows the company inside out
  - fully aware of the network, infrastructure policies.
  - e.g. ap of the subnets, ruling list of firewalls, intrusion detection system details.

- Cost-effective and can be good when testing a single component

Security testing methodology

- Approach to attempt to find vulnerabilities in the system's security mechanisms.
- Used during e.g. <u>security audit</u>, <u>vulnerability assessment</u> and <u>penetration test</u>.
- ♀ Using a good security testing methodology provides a repeatable framework

Proprietary methodologies

- Usually done by security companies who offer pen testing services and as such are kept confidential.
- Includes
    - **IBM**
        - Good for mid-sized companies
        - Gives fast result without much effort
    - **McAfee Foundstone**
        - Used mainly in enterprises.
        - Anything that's custom not generic has big chance of slipping through
    - **EC-Council LPT**
        - Auditing framework

Open-source Methodologies

- Publicly available and can be used by anyone

OWASP (Open Web Application Security Project)

- Online community, produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security
- Produces Top 10 lists of the most common vulnerabilities and how to fix them.
    - E.g. • <u>Web Application Top 10 threats</u> • <u>Docker Top 10</u> • <u>Top 10 Mobile Threats</u>
- Good for developers and system architects (anyone working with coding/application)

OSSTMM (Open Source Security Testing Methodology Manual)

- Open-source security testing methodology manual
- Standard set of penetration testing tests
    - Attempt to standardize pen-testing and making consistent
- Defines three types of compliance:
    - **Contractual**: requirements enforced by an industry or non-government group.
    - **Legislative**: regulations enforced by the government.
    - **Standards based**: actions that are recommended and must be adhered to in order to be certified by a group.

ISSAF (Information Systems Security Assessment Framework)

- Like an instruction manual "how to conduct a pen-test"

NIST (National Institute of Standards and Technology)

- Federal technology agency
- Applies a lot of standards to comply.
- They do much research and publish most.
- E.g. • NIST SP 800-53 • NIST definition of cloud computing

Penetration testing phases

1. Pre-Attack Phase

- Planning
- Preparation
- <u>Reconnaissance</u>

Contracts

- Ethical hackers proceed only after an agreement is in place—to protect both parties.
- **Non-disclosure agreement**
    - Also known as **NDA**
    - 📝 Prohibits you from sharing your findings
- **Penetration testing contract**
    - Should include all information and requirements that the penetration tester needs.
    - Ensures the tester won't be sued or prosecuted and can legally perform an attack.
        - as damage can incur during penetration testing
- 💡 Good idea to go through those with a lawyer.

Rules of Engagement (ROE)

- Formal document that gives permission to perform a penetration test.
- 📝 Guideline for testers and as such should clearly state what is and isn't allowed
- E.g. which IP addresses should be tested, which hosts are not to be tested, which techniques, time frame when test can take place etc.
. E.g. ok with SQL injection tests and brute force attacks but no DDoS attacks to not have service disruption or to not have network costs.
- 🌐 Used also by armies, e.g. US army cannot fire on somebody unless they're firing on them.

Understanding the clients requirements

- Pen-tester needs to understand the client's requirements.
    - 💡 Also make sure client understands that themselves as well as they may not understand what they're asking you to do
- Important for testers reputation and clients satisfaction.
- 💡 Create checklists.
    - Make suggestions
    - Ensure everything is clear without loose ends
    - Best to be clear as changing something during testing is not good as it would postpone the deadline and cost more for the client.

Defining the scope

- Ensures that requirements are fulfilled, and objectives are met.
- Objectives should be determined first e.g.
    - **Deliverables**: Different reports and often a final report where all results are placed and documented.
    - **Functionality**: Verifies the system you're pen-testing is working as intended
    - **Technical structure**: Design of the whole project
    - **Data definition**
- Defines areas/parts of the system that'll be tested e.g.:
    - Network security
        - E.g. check routers for faulty configurations, outdated operative systems.
    - System software security
    - Client-side application security
    - Client-side to server-side communication security
    - Server-side application security
    - Document security
    - Physical security
        - E.g. how are people tracked? How is access granted and controlled? How are the access policies enforced?
    - Application communication security
    - Dumpster diving
    - Insiders
    - Sabotage intruder confusion
    - Intrusion detection
    - Intrusion response
    - Social engineering

Information gathering

- To goal is to gather as much information about the target as possible
- Information is used to map out the target's network and plan the attack.
- See also Reconnaissance | Hacking stages and Footprinting
- Information can include
    - **Physical and logical locations**
        - e.g. for servers
    - **Analog connections**
        - E.g. phones, GSM networks
        - 🤑 You can create your own cellphone tower and take over their connections as you'll have the strongest signal.
    - **Contact information**

- E.g. sitting in a near coffee to take photos and take names. You can then look at their contact information in list of employees (if publicly available somewhere). They become suspectable to social engineering.
  - **Information about other organizations**
    - 😁 E.g. You can come with a rack suit to fix air-conditioning devices and say "hey there's a problem in air conditioning on floor 14" or "regular maintenance" or "one of your devices is due.". A security personal mey escort you but he won't watch everything carefully, you can place a Raspberry Pie and connect it to electricity. Refer to the following video: Sneaking in EVERYWHERE for FREE (Yellow Vest Experiment)
      - Stupid and simple. Something too complex has higher risks of not working as the dumber it is, the simple it is, it'll probably work.

2. Attack phase

- Phase where target gets compromised.
- Information gathered in the previous one is used to carry out an attack.
- Steps

  1. Penetrate the perimeter
  2. Acquire target
  3. Escalate privileges
  4. Execute, implant, retract

a. Penetrating the perimeter

- Trying to bypass IDS (Intrusion Detection System) and firewall
- A way is to use social engineering to test out the boundaries and find a way into the system.
- **Firewall testing** techniques include
  - ICMP probes
  - Checking access control
  - Evaluating protocol filtering rules
  - Evaluating IDS
- Probing allow you to see what the perimeter detects & drops & won't detect
  - You can craft own packets and see the reactions
    - e.g. by modifying source/destination IPs
  - E.g. check if certain port always drops, maybe port is open but only goes through the VPN where employees access network.
- Figure out what devices are running under perimeter to select as a target.
  - **Enumerate devices** collecting:
    - ID of the device
    - Description
    - Hostname
    - Physical location
    - IP and MAC address

- - 🌐 MAC address lets you know who the manufacturer is. Manufacturer information can give you idea of what kind of OS they run. You might get what devices they are running and how they are shipped. You can go to the distributor and put some physical keyloggers or sniffers e.g. a Raspberry Pi into a large router/switch.
  - By cross checking them later again, it is possible to identify unauthorized devices.

b. Target acquisition

- Done after scanning and penetrating of the perimeter and selecting a target machine/device
- Involves vulnerability scans to find vulnerabilities which can be later exploited
- 📝 Includes:
  - **Active probing assaults**
    - Scanning the network and gathering more information
  - **Running vulnerability scans**
    - Completing vulnerability scans to see what vulnerabilities that the target has.
  - **Attempt to access services and obtain data**
    - Trusted systems and trusted process assessment
    - Trying to access the resources on the system using the credentials obtained during the information gathering process
      - E.g. using credentials that you have obtained through social engineering or general research of the company/system
    - You attempt to access and extract as much as data as you can
    - Pick-locking: try to unlock it in every possible way

c. Privilege escalation

- 📝 Done once the access to the system is granted
- Goal is to grant elevated access.
- Techniques include
  - **Password crackers**
    - E.g. bruteforce, dictionary-based attack
  - **Exploit vulnerabilities in a code** e.g.
    - Poorly written security policies
    - False code in the code / applications
    - Web app version is not updated, there's a vulnerability in this version
    - Use flaws in a system e.g. older version of OS.
  - **Trojans**
  - **Social engineering**
    - E.g. you realized that there's no strict policy regarding e-mails. You send an e-mail for phishing scheme, gain more information when the person clicks on that link, you can then execute arbitrary code if e-mail client is old (unlikely).
    - E.g. phone-call and ask what you need: works way more than it should
- 🌐 A lot of companies have state-of-the-art perimeter

- inside perimeter they have very old equipment and OS
- they don't emphasize much on security interior as they do in external
  - once you pass the perimeter, you're more likely to find something inside
- Defenses include
  - Running services with the least privileged accounts
  - Implementing multi-factor authentication/authorization

d. Execute, implant, retract

- Involves compromising the system with code.
- Techniques include
  - DoS, DDoS attacks
  - buffer overflows to execute arbitrary code.
  - using viruses, trojans, rootkits
  - installing backdoors
- Retract means being able to exit without leaving any traces behind
  - Traces left behind can cause suspicions and in effect vulnerablities would be patched and you cannot gain access to the target machine back using the same method.
  - Delete all the logs that indicates you existed to ensure persistent remote access.
  - Good idea is to figure out their antiviruses, and test your execution in a VM with same antivirus and security measures to not get detected by a random scan.
  - If alarm is raised, you might be detected, put it in the report and result of whether the flag was investigated.

3. Post-attack phase

- The tester restores the system to the pretest state.
- Don't leave your stuff be it accidentally or on purpose as it breaks the law either way.
  - Examples
    - Delete any malware/rootkit installed
    - Recover all files that were deleted
    - Reverse any elevated privileges.
    - Restore network settings to its original state
    - Remove created vulnerabilities and exploits
- Documentation / clear log of activities, results and security flaws.