Cryptography & Computer Security

Basic Concepts

Contacts

- Guarantor & teacher: Eliška Ochodková
- Office: EA-439
- Email: eliska.ochodkova@vsb.cz
- Web: https://lms.vsb.cz/
  - Course: 460-4046/03 Cryptography and Computer Security (2023/2024 LS)

Requirements

- Attendance at lectures is strongly recommended (in addition, we are required to keep attendance records)
- Seminars are mandatory
- Credit
  - Attendance at seminars - minimum 9 , maximum 12 points
  - Three tasks, each for a minimum of 5, maximum of 11 points, obligation to meet the deadline
- Written exam - minimum 20, maximum 55 points
- Prerequisites
  - at least basic knowledge of programming (C like languages or Python)
  - at least basic knowledge of Linux OS

Literature

- https://ptgmedia.pearsoncmg.com/images/9780132789462/samplepages/0132789469.pdf
- https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf
  chapter 1

ICT security

- Aspects of computer security (better ICT security) are very broad, from threats and vulnerabilities to methods of protection etc.
- Information is a strategic resource
  - We trust ICT with our know-how, privacy, sensitive information, ...,
  - Many processes (industrial, commercial, medical, ...) depend on ICT,
  - ! requirements for information protection within ICT are given directly in the **legal order** (Czech Republic, EU or others), e.g.:
    - eIDAS, EU Regulation 910/2014 on electronic identification and trust services for electronic transactions https://en.wikipedia.org/wiki/EIDAS
    - Council of Europe Convention 185 on Cybercrime of 23 November 2001 https://www.coe.int/en/web/cybercrime/the-budapest-convention
    - …

Cybercrime

- Manifestations of cybercrime
  - Social Engineering (Sociotechnics), Malware, Ransomware
  - Spam, Hoax, Scam offers
  - Phishing, Pharming, Spear Phishing, Vishing, Smishing
  - Fraudulent websites (companies)
  - Hacking, Cracking
  - Internet (computer) piracy
  - Sniffing
  - DoS, DDoS, DRDoS (distributed reflection denial-of-service) attacks
  - Cyberbullying, Cyberstalking, Sexting, Spreading harmful content
  - Identity theft
  - ....

Standards (norms)

- ICT information protection (and ICT security) requirements are also driven by ! **professional standards**
- Standards (norms) *de facto* and *de jure*
- *de* jure
  - International: ISO/IEC 27000 https://www.iso.org/news/ref2266.html is a code of standards that focuses on information security management systems
  - National: CSN - Czech standards, BS - British standards, etc. ....
  - The standards issued by the American institute NIST are important https://www.nist.gov/cybersecurity
- *de facto*
  - W3C standards, see https://www.w3.org/standards/xml/security , e.g. XML Signature (https://www.w3.org/TR/xmldsig-core1/)
  - RFC (https://www.ietf.org/standards/rfcs/), e.g. IP Security (IPsec) https://datatracker.ietf.org/doc/html/rfc6071 ,
  - ITIL https://en.wikipedia.org/wiki/ITIL , COBIT https://en.wikipedia.org/wiki/COBIT , ...

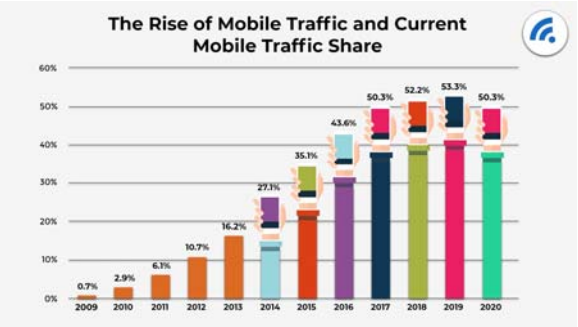
In the past

- For a long time, security was mostly ignored
- The computer industry was "surviving", primarily trying to overcome technological and economic obstacles. As a result, many security compromises were made.
- While there were theories and even examples of systems with very good security, they were unsuccessful or ignored
  - e.g. ADA language, 1980s USA,
    - powerful safe and easy to use, see http://archive.adaic.com/intro/WhyAda.html (Ada has the only compilers that are validated by the U.S. Government and other agencies throughout the world, including the International Organization of Standards (ISO). Each compiler is tested on thousands of programs before it receives validation, strong type system, integrity constraints, ...)
    - named after Ada Lovelace (1815-1852), who is considered the first female programmer

The beginning of the millennium

- "Computers" (understood in a broad sense, i.e. including embedded computers, etc., from automotive control units to industrial robots) are ubiquitous, very powerful and very cheap.
- Internet and other types of networks (sensor, etc.)
  - Computers are interconnected and interdependent
  - This dependency magnifies the impact of potential errors, attacks...
- Since the beginning of the millennium, there has been a sharp increase in interest in ICT security.

Present



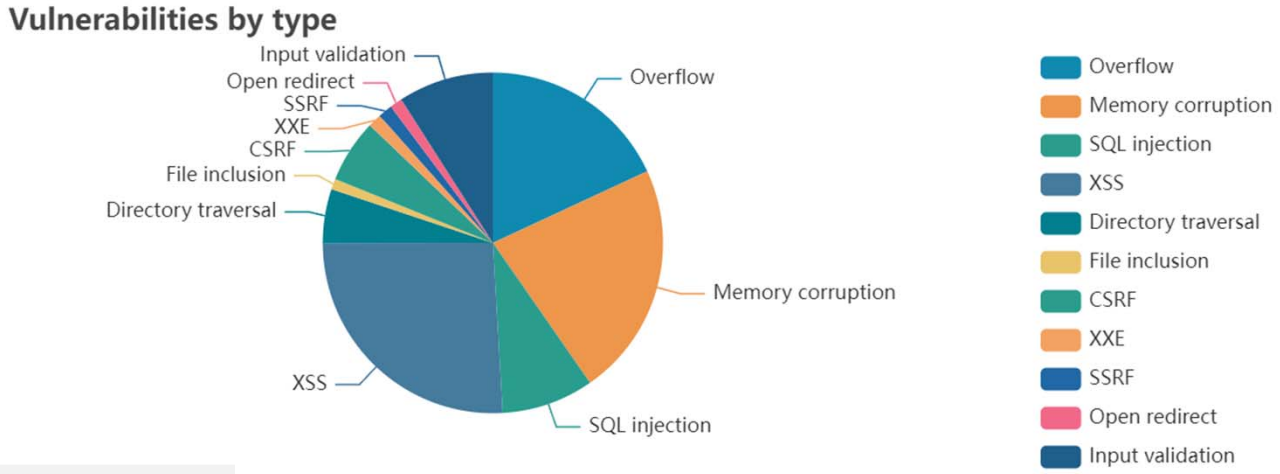
- Global - 2021 Forecast Highlights https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf
- 2023 Global Networking Trends Report https://www.rmol.cz/sites/default/files/prilohy/xa-09-2023-networking-report.pdf
- Key Internet Statistics to Know in 2024 (Including Mobile) https://www.broadbandsearch.net/blog/internet-statistics
- WhatsApp Usage Statistics: How Many People Use It in 2023 https://techjury.net/blog/whatsapp-usage-statistics/
- How Many IoT Devices Are There in 2024? https://techjury.net/blog/how-many-iot-devices-are-there/#gref
- How Much Data Is Created Every Day in 2023? https://techjury.net/blog/how-much-data-is-created-every-day/#gref
- 25+ Impressive Big Data Statistics for 2024 https://techjury.net/blog/big-data-statistics/
- How Many Software Engineers Are There In The US? (2024 Statistics) https://techjury.net/blog/how-many-software-engineers-in-us/
- ...

Present

- Trends:
  - Cybercriminals target deepfakes, cryptocurrencies and mobile wallets, among others (https://thecyberexpress.com/deepfake-technology-trends-for-2024/)
    - Deepfake - simply put, replacing faces in videos or photos thanks to artificial intelligence
    - A phenomenon of recent years, in October 2019 alone, 15,000 deepfake videos have appeared on social media, replacing the original faces with fake ones.
  - 20 Generative AI, ChatGPT & Deepfake Statistics You Should Know For 2024 https://www.thesslstore.com/blog/generative-ai-statistics/
  - Top 10 Threats https://www.mcafee.com/enterprise/en-us/threat-center.html

The Most Vulnerable Software in 2023

https://www.cvedetails.com/top-50-products.php?year=2023



Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2023

Go to year: 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 All Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	1421
2	Windows Server 2022	Microsoft	OS	566
3	Windows Server 2019	Microsoft	OS	541
4	Fedora	Fedoraproject	OS	528
5	Windows 11 21h2	Microsoft	OS	509
6	Windows Server 2016	Microsoft	OS	501
7	Windows 11 22h2	Microsoft	OS	495
8	Windows 10 1809	Microsoft	OS	489
9	Windows 10 22h2	Microsoft	OS	483
10	Windows 10 21h2	Microsoft	OS	477
11	Debian Linux	Debian	OS	476
12	Windows Server 2012	Microsoft	OS	451

Vulnerabilities and threats

- https://owasp.org/www-project-top-ten/
- https://www.clouddefense.ai/owasp-top-10-vulnerabilities/
- NIST
  - https://nvd.nist.gov/vuln
  - https://nvd.nist.gov/vuln/search
- https://www.exploit-db.com/
- https://cve.mitre.org/
- security research blogs, vendor advisories, threat intelligence platforms, and cyber-security news outlet

Definition of security

- **Security** is the state of a system ("well-being") where the possibility of successful undetected theft, tampering, or disruption of information and services is kept at a low or tolerable level.
- ICT security is usually understood as the protection of the corresponding systems and the information they contain
  - stored, processed and transmitted.
  - Part of ICT security as generally understood in this way is also
    - Physical security (protection against natural threats and physical attackers)
    - and personnel security (protection against internal attackers, ...).

(Computer) system

- **(Computer) system** in which data are processed, stored, transmitted, which are carriers of information, contains the following so-called **assets**:
  - **hardware** - network elements, processor, memory, terminals, etc.,
  - **software** - application programs, operating system, etc.,
  - **data** - data stored in the database, results, output reports, input data, etc.
- **Entity** (subject) - person, process, network element, etc.

Security functions (1)

- **Security functions** (services, goals) - services that support and enhance the security of data processes and transfers in a given entity.
- Security functions are provided (implemented) by **security mechanisms**. These are mechanisms designed to detect, prevent, or help recover from attacks.
  - Security functions are typically available to users as a set of security services through APIs or built-in interfaces

Security functions (2)

- A **trustworthy entity** is one that is believed (proven) to be implemented to meet its specification == we can rely on it to behave as we expect it to behave.
- **Authorization** of an entity for an activity is a determination that it is trustworthy for that activity. Granting authorization requires that authentic entities be handled.
- **Confidentiality** – assets are readable only by authorized entities.
- **Integrity** - only authorized entities may modify assets.
- **Availability** (also accessibility) - assets are available to authorized entities, so there is no denial of service when an entity does not get what it is entitled to.
- **Authenticity** (authentication) - the entity or e.g. the origin of information is verifiable. Authentication is the process of verifying the authenticity of the identity of an entity (i.e. user, process, systems, information structures, etc.).
- **CIA** == Confidentiality, Integrity, Availability

Safety features (3)

- **Non-repudiation** - participation in the transaction cannot be denied,
- **Accountability** - a guarantee that entities can be held accountable for their activities,
- **Reliability** - consistency of intended and resulting behaviour.
- A secure system is one that we can rely on, e.g. :
  - Keep our personal and other sensitive information confidential
  - Allows only authorized access to or modification of resources
  - Provides correct and meaningful results
  - Delivers the right and meaningful results whenever we want them
  - ...

Example - AAA

- **AAA** - authentication, authorization and accounting.
- E.g. RADIUS protocol, RFC 2865 http://tools.ietf.org/html/rfc2865
  - **Authentication** (verification of the user's identity by an authentication authority, in this case a RADIUS server using EAP).
  - **Authorization** - assigning access rights to a user who has successfully completed the authentication process, or not assigning these rights to a user who has not met the authentication requirements.
  - **Accounting** - collecting operational information about the authorized user, typically data about the amount of data transferred, the duration of the connection to the network, and the identification of the access point from which the network was accessed.

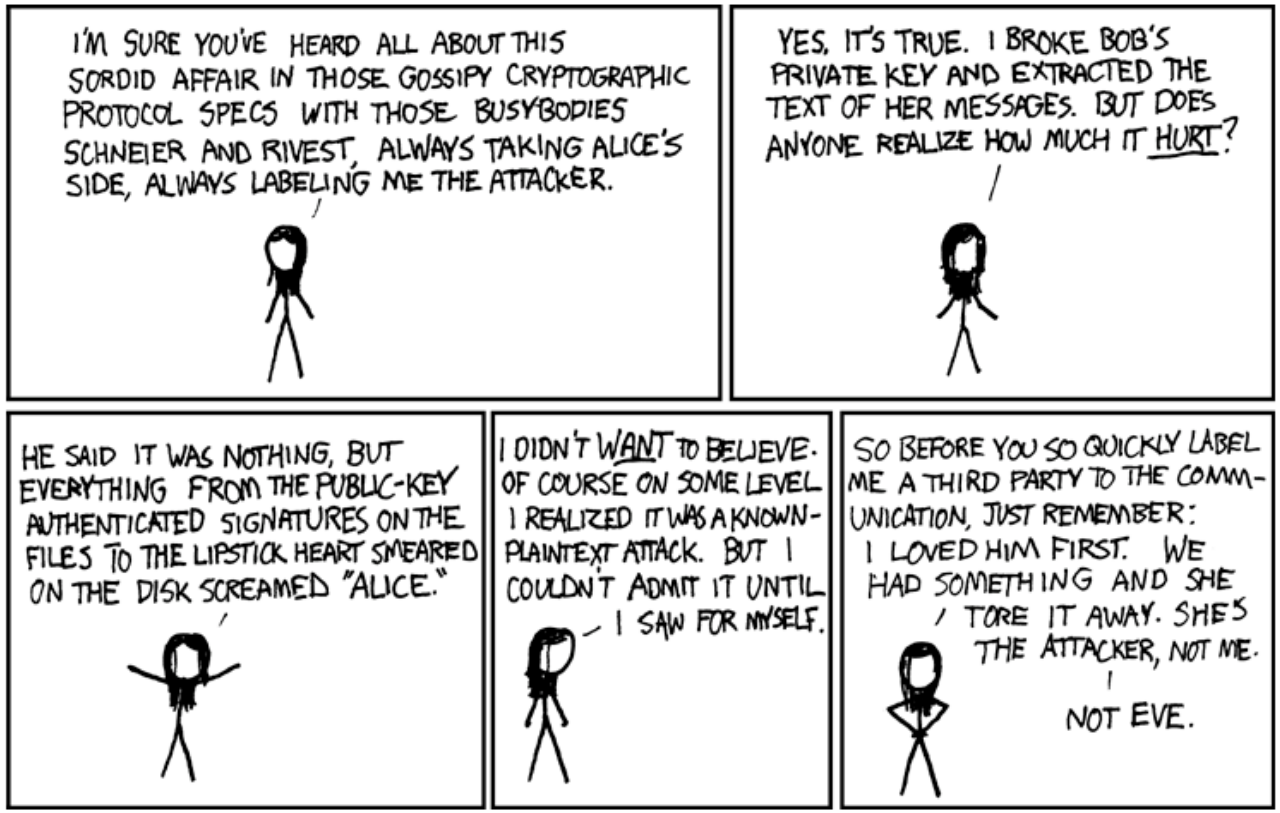
Privacy, security

- **Privacy** can be defined as "informational self-determination", i.e. the ability to control information about one's person.
  - Privacy measures generally govern how personal data is permitted to be accessed and viewed, including how the data is stored and used, e.g. we may determine
    - Who can know them (clean, see, ...)
    - Who can dispose of them
    - For what purposes it can be used
    - To whom they can provide them
    - ...
- **Safety x security** - often understood as synonyms, but
  - Safety - generally refers to the state of being protected from harm, danger or risk. It includes physical well-being, health and the absence of danger.
  - Security - usually refers to mechanisms taken to protect against potential threats, including unauthorized access, criminal activity or other malicious activities.

Participants (roles)

- **Alice and Bob** - are legitimate (good guys) entities (persons, processes, computers,...), first used by Ron Rivest 1978
- Eve, Mallory, Oscar, Trudy - illegitimate subject (bad guy), generally an attacker
  - **A sender** is an entity (someone or something) that legitimately sends a message (we will refer to it as Alice, A).
  - **The receiver** (recipient) is the entity (someone or something) that legitimately receives the message (we will refer to it as Bob, B),
  - **An intruder** (intruder, eavesdropper, adversary, opponent, etc.) is an entity that is neither the sender nor the receiver of a message and that attempts to break through the security mechanism that secures the communication between A and B (denoted by C, E, M, etc.).
    - Who can be the attacker (enemy)? Different types of attackers (Organised crime, Terrorists, Amateurs, "Script kiddies", Crackers, "Cyberwarriors" ...)

Participants (roles)



http://xkcd.com/177/

CIA (Confidentiality, Integrity, Availability) example (1)

- Alice runs Alice's Online Bank (AOB)
- What are Alice's security requirements?
- If Bob is an AOB customer, what are his security requirements?
- How are Alice and Bob's requirements the same? How are they different?
- And how does Oscar (attacker) feel about that?

Example (2)

- C - AOB must, for example, prevent Oscar from discovering the balance in Bob's account
- I - Oscar must not be able to change Bob's account balance. Also, Bob must not be able to incorrectly change his own account balance
- A - AOB must provide information whenever it is needed. And Alice must be able to execute the transaction - if not, she may go out of business.

Example (3)

- How does Bob's computer "know" that "Bob" is really Bob and not Oscar?
- Bob **authenticates with** a password, the password must be verified
  - Addressed by **cryptographic security mechanisms** (by hash function)
- Security problems with passwords
- Is there an alternative to passwords?

Example (4)

- When Bob logs in into the AOB, how does the AOB know that "Bob" is really Bob?
  - Again, Bob's password is verified, but
  - unlike the previous case, **network security** issues are added**.**
- Critically important are the protocols
  - "Simple" authentication protocols
  - "Real-world" protocols (SSH, SSL, IPSec, Kerberos, WPA,...)

Example (5)

- Once Bob is verified by the AOB, then the AOB must restrict Bob's actions
  - Bob cannot view another entity's account information
  - Bob can't install new software, etc.
- Enforcement of these restrictions will ensure **authorisation**
- **Access control** includes both authentication and authorization
  - Authentication (passwords, biometrics, ...)
  - Authorization (Access Control Lists/Capabilities, Multilevel security (MLS), firewalls, IDS)

Security incident

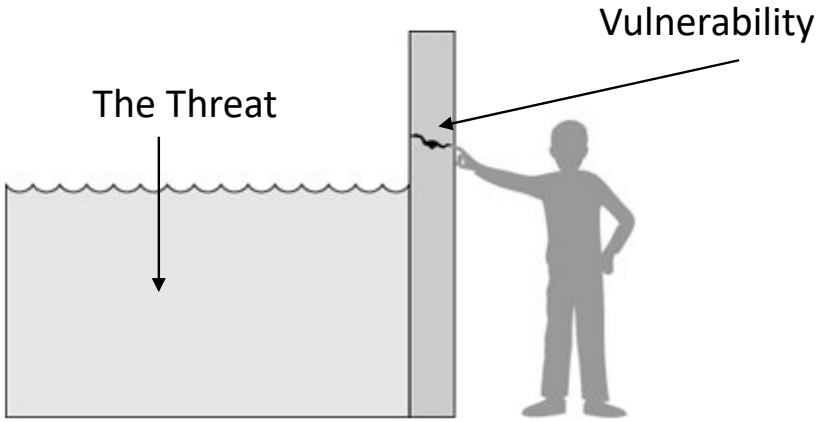
- We understand **a security incident**:
  - either intentional use of a vulnerability to cause damage/loss to so-called assets
    - **attack** requires an active opponent, has an implicit notion of "intent, intention"
  - or the unintentional taking of an action that results in damage to assets
    - A server crash that causes a loss of availability is not necessarily an intentional attack.
- **Impact** - the consequence of the incident, the extent of the damage
- A security incident therefore represents a breach of ICT security and security rules (security policy). It can be e.g.:
  - impersonating another authorised person and abusing their privileges,
  - unjustifiably increase of privileges of access to information,
  - spoiling the functionality of the software by adding hidden features,
  - inclusion as a hidden intermediate in the conversation of other subjects,
  - fire, flood,
  - Denial of Service (DoS), Distributed Denial of Service (DDoS - e.g. CodeRed worm).

Vulnerability

- **A vulnerability** is a weakness in a system that can be exploited to cause damage or loss through an attack. It occurs:
  - in the physical arrangement,
  - in organizational charts,
  - in administrative measures,
  - in logical and technical measures,
  - in personnel policy, administration or management of the organisation,
  - the human factor,
  - For example, a server does not authenticate its users, A particular system may be vulnerable to data tampering because the system does not verify the identity of the user before allowing access to the data.
- Causes
  - errors in analysis, design, implementation,
  - software complexity,
  - existence of hidden (side) channels https://en.wikipedia.org/wiki/Side-channel_attack
  - ...

The Threat

- **Threat** - the potential possibility (set of circumstances) of using a vulnerability to attack (to cause damage, to destroy assets, ...)
  - Threat characteristics - source (external, internal), motivation (financial gain, industrial espionage, ...), frequency
  - We watch (check) for weaknesses, as a prevention of attack and blocking (elimination) of threats.



http://ptgmedia.pearsoncmg.com/images/9780132789462/samplepages/0132789469.pdf

Risk

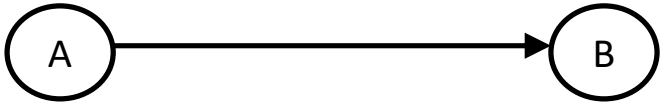
- **Risk** - the existence of a threat poses a risk - the likelihood of exploiting a vulnerability
  - Risk - is a function of the probability of an incident occurring and the damage caused
- The risk assessment includes the following steps:
  1. characterisation of the system
  2. threat identification
  3. vulnerability identification
  4. analysis of control mechanisms
  5. probability determination (of vulnerability exploitation)
  6. impact analysis
  7. determination of risk
  8. control recommendations
  9. documentation of results

Security Policy

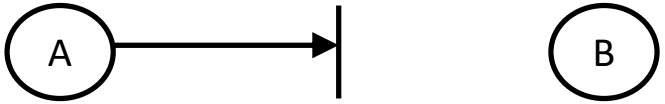
- General security policy of the organisation - a set of principles and regulations defining the way of securing the organisation from physical security, through the protection of professional interests to the protection of privacy and human rights.
- An organisation's **ICT security policy** deals with the selection of security principles and regulations that generally define the safe use of information resources within the organisation**, regardless of** the specific information technology used. It is a statement of what is and is not allowed.
- **ICT System Security Policy**
  - Specifies the details of specific standards and regulations that define how information is managed, protected and distributed within the organisation.
  - It specifies the security measures and how to implement them.
  - It specifies how these measures are to be applied, respecting the ICT used.

Attacks (1)

- Security incident - an intentional or unintentional action resulting in damage to assets.
- Normal flow of information*:*

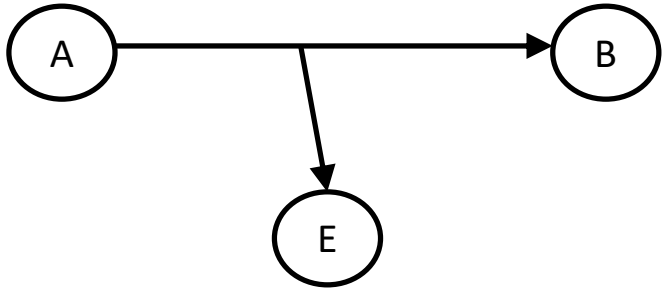


- **Interruption** attack: this is an attack on availability (destruction of hardware, interruption of the communication line, unavailability of files, hardware failure, ...)

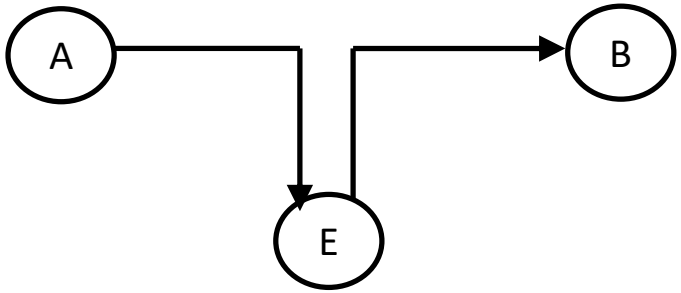


Attacks (2)

- **Message interception**: an attack on confidentiality; an unauthorized entity E (the attacker can be a program, a computer, a person) eavesdrops, illegally copies data,...

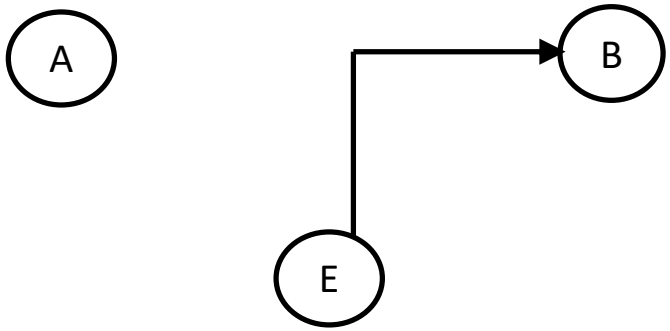


- A **modification** is an attack on the integrity of data; an unauthorized entity E changes data values, program functionality, the content of a message sent over a network, ...



Attacks (3)

- **Adding value**, "fabrication" is an attack on authenticity, integrity; an unauthorized entity E inserts a "fake" into the system (inserting a fake message, adding records to a file, ...).



Attacks (4)

- **Passive attacks** (eavesdropping, monitoring):
  - disclosure of the content of the message (i.e. we want to prevent the attacker from learning about the content of the transmission),
  - traffic analysis - an attacker can track the location and identity of communicating entities, the frequency and length of messages exchanged, which allows to estimate the nature of the communication.
  - Protection: prevention (eavesdropping detection is difficult).
- **Active attacks** (by interrupting, modification and adding value):
  - masquerade (an entity masquerading as another),
  - capture (replay),
  - message modification,
  - denial of service.

Security mechanisms (1)

- **Security mechanisms** - implement (provide) security functions. These are mechanisms designed to detect attacks, prevent them, or help recovery from attacks:
  - there are many of them, they can be physical arrangement (UPS, ...), administrative actions (training, ...), they can be technical devices or logical tools (algorithms),
  - In general
    - cryptography,
    - software control,
    - hardware control,
    - physical inspection,
    - policies and processes (methodology)

Security mechanisms (2)

- **Cryptographic techniques** (design, use and management) are the basis for many security mechanisms
  - Protecting data by making it unreadable to an attacker
  - User authentication using digital signatures
  - Transaction authentication using cryptographic protocols
  - Ensuring the integrity of stored data
  - ...

Security mechanisms (3)

- Software control
  - Passwords and other forms of access control
  - OS - separating user actions from other actions
  - Antiviruses for detecting certain types of malware
  - Personal firewalls
- Hardware control (meaning not protecting the hardware itself, but using separate hardware to protect the system as a whole)
  - Fingerprint readers
  - Smart tokens
  - Firewalls
  - IDS, intrusion detection systems
- Physical control (protection of the hardware itself, as well as physical protection of access to assets)
  - Locks
  - Guard service
  - IPS, ...
- Policies and processes (non-technical means of protection)
  - Password handling policy
  - Training in best practices, safety education

Software

- Cryptographic algorithms, protocols and access control are implemented in software
- What are the software security issues?
  - The real world of software is complex
  - Software bugs lead to security vulnerabilities
  - How can an attacker attack the software?
  - How to reduce bugs in software development?
- Critical software bugs
  - Buffer overflow,...
- Malware - Prevention and detection, the future of malware?

Methods of defence

- How can we defend ourselves?
  - **Preventing an attack**
  - **Deter an attacker**: to make an attack harder or more expensive
  - **Distract**: to make things less attractive to an attacker
  - **Detect Attack**: Detecting an impending or completed attack
  - **Recovering from the attack**
- Absolute prevention of attacks is not possible
- Typical protection (mainly against active forms of attacks) is based on **detection of attacks and subsequent recovery**

Some thoughts at the end of the introduction (1)

- Perfect security is theoretically possible, but not practically possible. Every best security mechanism can be attacked with brute force.
- Any security mechanism used must be acceptable to the user community.
- Safety is not a state, but a PROCESS.
- Safety is not about the technology you buy, but about using it correctly.
- The principle of the simplest attack
  - "A system is only as secure as its weakest link. And people are the weakest link." Bruce Schneier, Secrets and Lies, 2000
  - To be able to build a secure system, we need to think like an attacker
- The principle of adequate protection
  - It makes no sense to spend $100,000 to protect a system that is only worth $1,000.

Some thoughts at the end of the introduction (2)

- "Only amateurs attack machines; professionals target people. And any solutions will have to target the people problem..." Bruce Schneier, Cryptogram, 15 Oct 2000
- "Many systems fail because their designers protect the wrong things or protect the right things in the wrong way." Ross Anderson, Security Engineering, 2008
- "Without usable systems, the security and privacy simply disappears as people defeat the processes in order to get their work done ... The more secure you make something, the less secure it becomes."
  - Why? Because when security gets in the way, sensible, well-meaning, dedicated people develop hacks and workarounds that defeat the security. Hence the prevalence of doors propped open by bricks and wastebaskets, of passwords pasted on the fronts of monitors or hidden under the keyboard or in the drawer, of home keys hidden under the mat or above the doorframe or under fake rocks that can be purchased for this purpose ... The strongest locks in the world do not deter the clever social engineer. Don Norman, When Security Gets in the Way, 2010