Information Security
CS3002
(Sections BDS-7A/B, BSE-7A)
Lecture 02

Instructor: Dr. Syed Mohammad Irteza

Assistant Professor, Department of Computer Science

21 (22) August, 2024

Administrative Information

- Office: 036, 1st Floor, Block F / New Building

- Email-01: m.irteza@nu.edu.pk
- Email-02: mohammad.irteza@lhr.nu.edu.pk

- Office Hours:
  - Tues/Thursday 11:30 am ~ 12:30 pm

Administrative Information

- Course Website (Google Classroom):
  - BDS-7A → https://classroom.google.com/c/NzA5NDIzMjIxNTY0
  - Code: 2pxbc6i
  - BDS-7B → https://classroom.google.com/c/NzA0ODg2MjIzNDMx
  - Code: zhbekn3
  - BSE-7A → https://classroom.google.com/c/NzA3MjM5MTcyMDUx
  - Code: yuc5ldq

- Class Schedule:
  - BDS-7A – Mon/Wed (08:30 - 10:00, Venue: NB-308)
  - BDS-7B – Mon/Wed (11:30 - 13:00, Venue: NB-308)
  - BSE-7A – Tue/Thu (08:30 - 10:00, Venue: CS-3)

Risk estimation

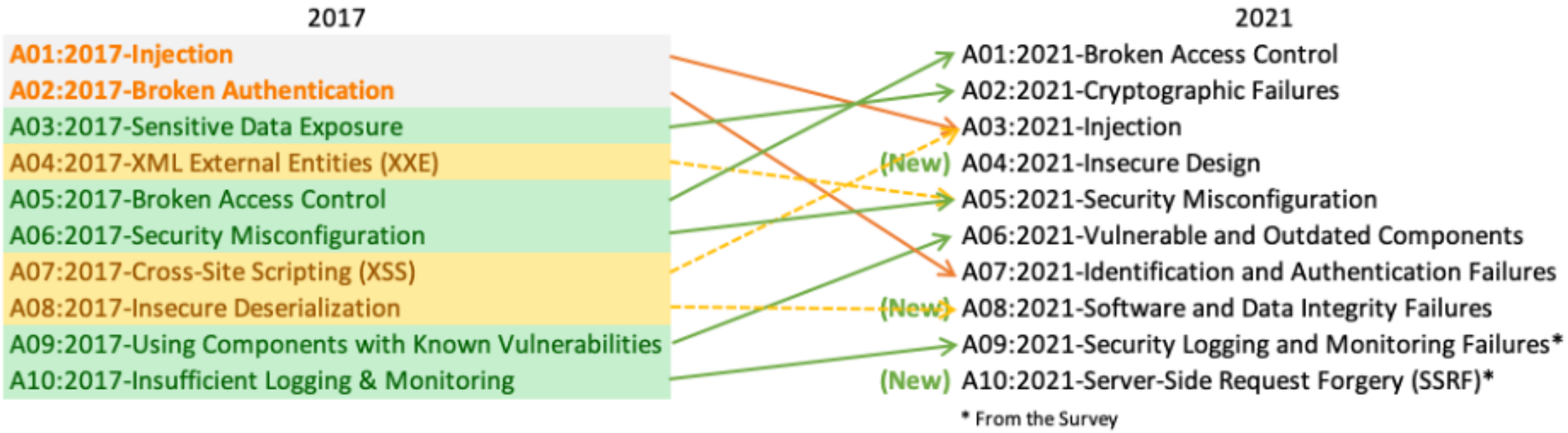
- Assets: Objects, data, people
- Vulnerability: Weakness of an asset
- Threat: loss of security due to vulnerability
- Attack: threat occurrence

- Risk estimation is the process of identifying vulnerabilities and threats and their impact and probability of an attack occurring.

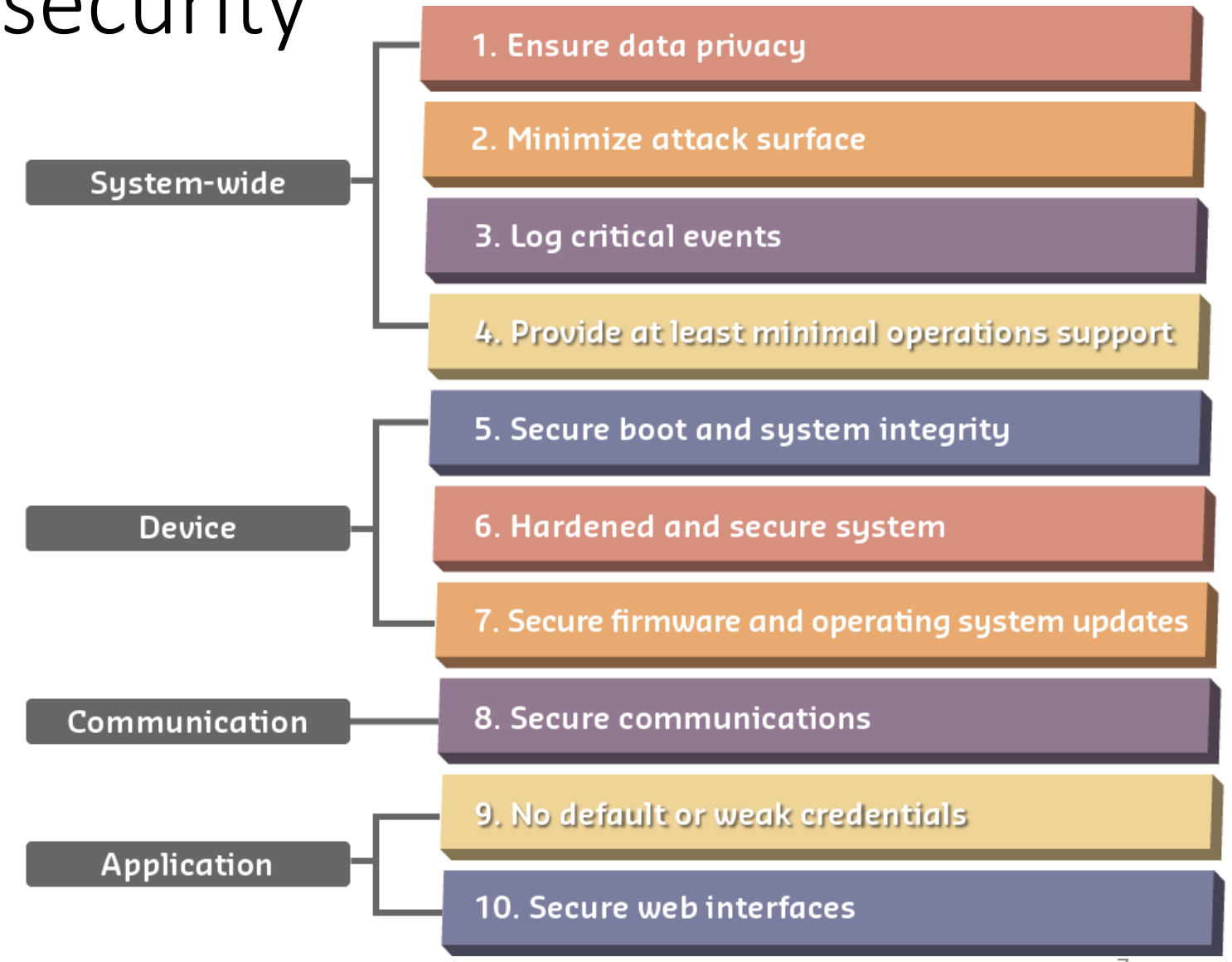
OWASP top 10 Vulnerabilities

Category	IoT Security Consideration	Recommendations
I1: Insecure Web Interface	•Ensure that any web interface coding is written to prevent the use of weak passwords …	When building a web interface consider implementing lessons learned from web application security. Employ a framework that utilizes security …
I2: Insufficient Authentication/Authorization	•Ensure that applications are written to require strong passwords where authentication is needed …	Refer to the OWASP Authentication Cheat Sheet
I3: Insecure Network Services	•Ensure applications that use network services don't respond poorly to buffer overflow, fuzzing …	Try to utilize tested, proven, networking stacks and interfaces that handle exceptions gracefully...
I4: Lack of Transport Encryption	•Ensure all applications are written to make use of encrypted communication between devices…	Utilize encrypted protocols wherever possible to protect all data in transit…
I5: Privacy Concerns	•Ensure only the minimal amount of personal information is collected from consumers …	Data can present unintended privacy concerns when aggregated…
I6: Insecure Cloud Interface	•Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces) …	Cloud security presents unique security considerations, as well as countermeasures. Be sure to consult your cloud provider about options for security mechanisms…
I7: Insecure Mobile Interface	•Ensure that any mobile application coding is written to disallows weak passwords …	Mobile interfaces to IoT ecosystems require targeted security. Consult the OWASP Mobile …
I8: Insufficient Security Configurability	•Ensure applications are written to include password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication)…	Security can be a value proposition. Design should take into consideration a sliding scale of security requirements…
I9: Insecure Software/Firmware	•Ensure all applications are written to include update capability and can be updated quickly …	Many IoT deployments are either brownfield and/or have an extremely long deployment cycle...
I10: Poor Physical Security	•Ensure applications are written to utilize a minimal number of physical external ports (e.g. USB ports) on the device…	Plan on having IoT edge devices fall into malicious hands...

OWASP (Current) – Top Ten



Requirements of security



Data Protection

- One of the most *valuable assets is data*
- *Without* data, an organization *loses its record of transactions* and/or its ability to deliver value to its customers
- An effective information security program is essential to the protection of the *integrity and value of the organization's data*
- Organizations must have *secure infrastructure services* based on the size and scope of the enterprise
- Additional security services may have to be provided

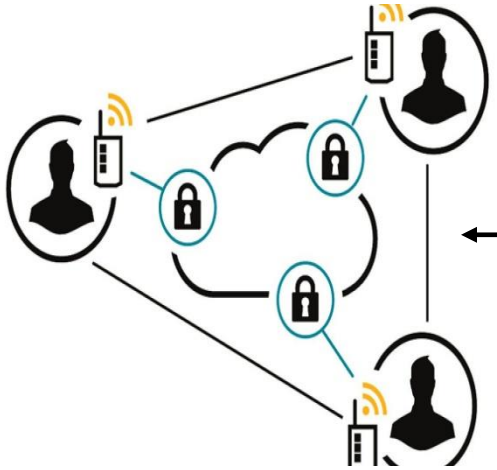
Threats

- A *threat* is an object, person, or other entity that represents a constant danger to an *asset*
- *Management must be informed* of the various kinds of threats facing the organization
- By examining each *threat category* in turn, management effectively protects its information through *policy, education and training, and technology controls*

Threat Modeling

Threat Modeling

- Theoretical use cases considered to identify potential threats.



attack

- Microsoft STRIDE
  - S: **Spoofing** of identity
  - T: **Tampering** with data
  - R: **Repudiation**
  - I: **Information** disclosure
  - D: **Denial** of service
  - E: **Elevation** of privilege

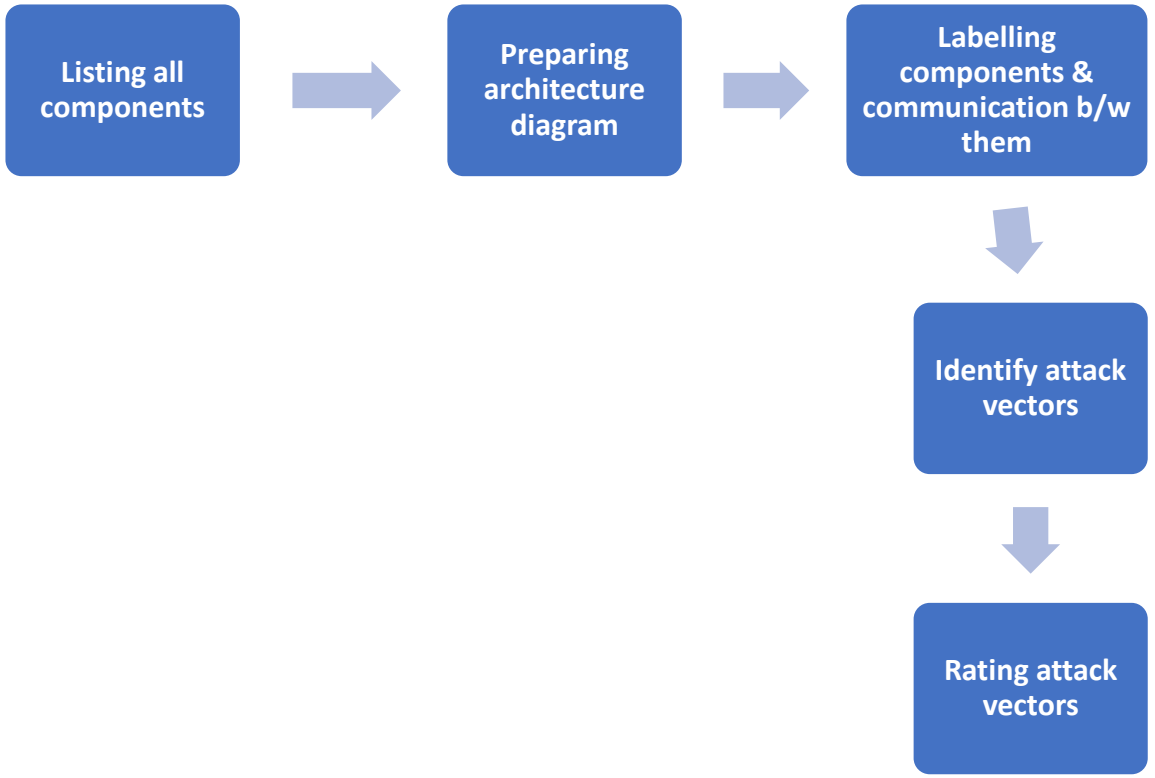
Six categories of security threats

- Requires realization of Assets and Vulnerabilities

Attack Surface Mapping

- Attack surfaces are *different points that an unauthorized user can employ to compromise* a system/ network/ solution.
- Each attack surface has its *associated risk, likelihood and impact*.
- Source of input maybe *HW, SW/FW, Communication*
- Example: mapping out all entry points an attacker can abuse in IoT device.
- Involves creating an *architecture diagram*
  - Tests performed based on priority
  - Priority = ease of exploitation * impact of exploitation

Attack Surface Mapping Process



Threats to Information Security

TABLE 2-1 Threats to Information Security[4]

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Attacks

- An attack is the *deliberate act that exploits a vulnerability*

- It is accomplished by a *threat-agent* to damage or steal an organization's *information or physical asset*
  - *A vulnerability is an identified weakness* of a controlled system whose controls are not present or are no longer effective

  - An *exploit is a technique to compromise a system*

  - An *attack* is then *the use of an exploit* to achieve the compromise of a controlled system

Some classes of attacks

- phishing (~ fishing):
- “dear Internet banking user, please fill in the attached module and return it to us ASAP according to the privacy law 675 …”

- psychological pressure:
- “help me, otherwise I’ll be in trouble …”
- “do it, or I’ll report it to your boss …”
- showing acquaintance with the company’s procedures, habits and personnel helps in gaining trust and make the target lower his defenses

Some classes of attacks

- Back Doors
  - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource
- Password Crack
  - Attempting to reverse calculate a password
  - Brute Force
  - The application of computing and network resources to try every possible combination of options of a password
  - Dictionary
  - The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses

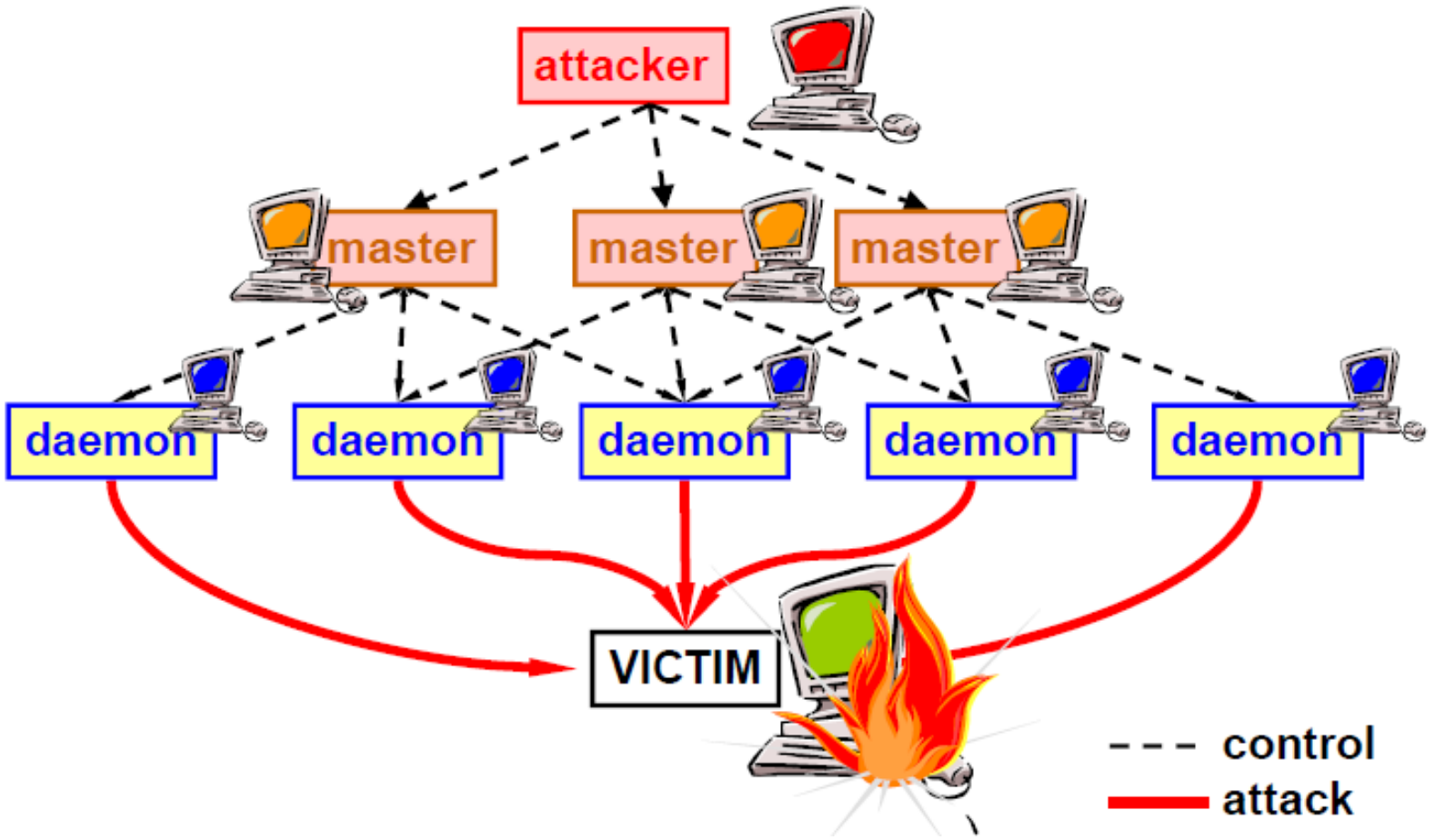
Some classes of attacks

- IP spoofing / shadow server
  - someone takes the place of a (legitimate) host
- Packet sniffing
  - passwords and/or sensitive data are read by (unauthorized) third parties
- Connection hijacking / data spoofing
  - data inserted / modified during their transmission
- Denial-of-service (distributed DoS)
  - the functionality of a service is limited or disrupted (e.g. ping bombing)

Distributed Denial of Service

- Software for DoS installed on many nodes (named daemon, zombie or malbot) to create a *Botnet*
- *Daemons* remotely controlled by a master (often via encrypted channels) and have auto-updating feature
- Effect of the base DoS attack *multiplied* by the *number of daemons*

Distributed Denial of Service



Basic Problems

- *Networks are insecure*: (most) communications are made in clear
- LANs operate in *broadcast*

- Geographical connections are *NOT* made through *end-to-end dedicated lines* but:
  - through *shared lines*
  - through third-party routers
  - *weak user authentication* (normally password-based)

- There is *no server authentication*
- Software contains many *bugs*!

Basic Problems

- Low problem understanding (i.e., *no awareness*)
- *Mistakes by human beings* (especially when overloaded, stressed, …)
- Human beings have a *natural tendency to trust*
- Complex interfaces / architectures *can mislead the user* and lead to *erroneous behaviors*
- *Performance decrease* due to the application of security (i.e., tradeoff)
- Ask for the (involuntary) user's participation to the attack action
- Usually *naive users* are targeted (e.g. "do immediately change your password with the following one, because your PC is under attack") ...
- But *experienced users* are targeted too (e.g. by copying an authentic mail but changing its attachment or URL)

Roots of Insecurity

- “Defensive strategies are reactionary”
- “Thousands - perhaps millions - of systems with weak security are connected to the Internet”
- “The explosion in use of the Internet is straining our scarce technical talent. The average level of system administrators has decreased dramatically in the last 5 years”
- “Increasingly complex software is being written by programmers who have no training in writing secure code”
- “Attacks and attack tools transcend geography and national boundaries”
- “The difficulty of criminal investigation of cybercrime coupled with the complexity of international law means that prosecution of computer crime is unlikely”

ICT Security

- ICT (*Information and Communication Technologies*) refers to *technologies that provide access to information through telecommunications*.
- ICT *security* is the set of *products, services, organization rules and individual behaviors* that protect the ICT system of a company.

- Three main components of any system are:
  - *Hardware*
  - *OS and applications*
  - *Communication*

  - Cloud - (Optional)

Glossary – 1

- *Phishing is a type of cyberattack that uses fraudulent emails, text messages, phone calls or websites to trick people into sharing sensitive data, downloading malware or otherwise exposing themselves to cybercrime.*
  - Source: What is Phishing? | IBM

Glossary – 2

- *A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions. This attack can be used to change the authoring information of actions executed by a malicious user in order to log wrong data to log files. Its usage can be extended to general data manipulation in the name of others, in a similar manner as spoofing mail messages. If this attack takes place, the data stored on log files can be considered invalid or misleading.*
  - Source: Repudiation Attack | OWASP Foundation

Glossary – 3

- An **attack vector** is a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities. Hackers use numerous attack vectors to launch attacks that take advantage of system weaknesses, cause a data breach, or steal **login credentials**. Such methods include sharing malware and viruses, malicious email attachments and web links, pop-up windows, and instant messages that involve the attacker duping an employee or individual user.
  - Source: What is an Attack Vector? Types & How to Avoid Them (fortinet.com)

Glossary – 4

- **An exploit** (in its noun form) is a segment of code or a program that maliciously takes advantage of vulnerabilities or security flaws in software or hardware to infiltrate and initiate a denial-of-service (**DoS) attack** or install malware, such as **spyware**, **ransomware**, **Trojan horses**, **worms**, or viruses. So the exploit is not the malware itself but is used to deliver the malware. To exploit (in its verb form) is to successfully carry out such an attack.
  - Source: Exploit in Computer Security | Fortinet