Information Security

Week 1

Muhammad Taseer ul Islam

taseerulislam@hotmail.com

Department of Computer Sciences

Federal Urdu University of Arts, Science and Technology, Islamabad

SECURITY CONCEPTS

6

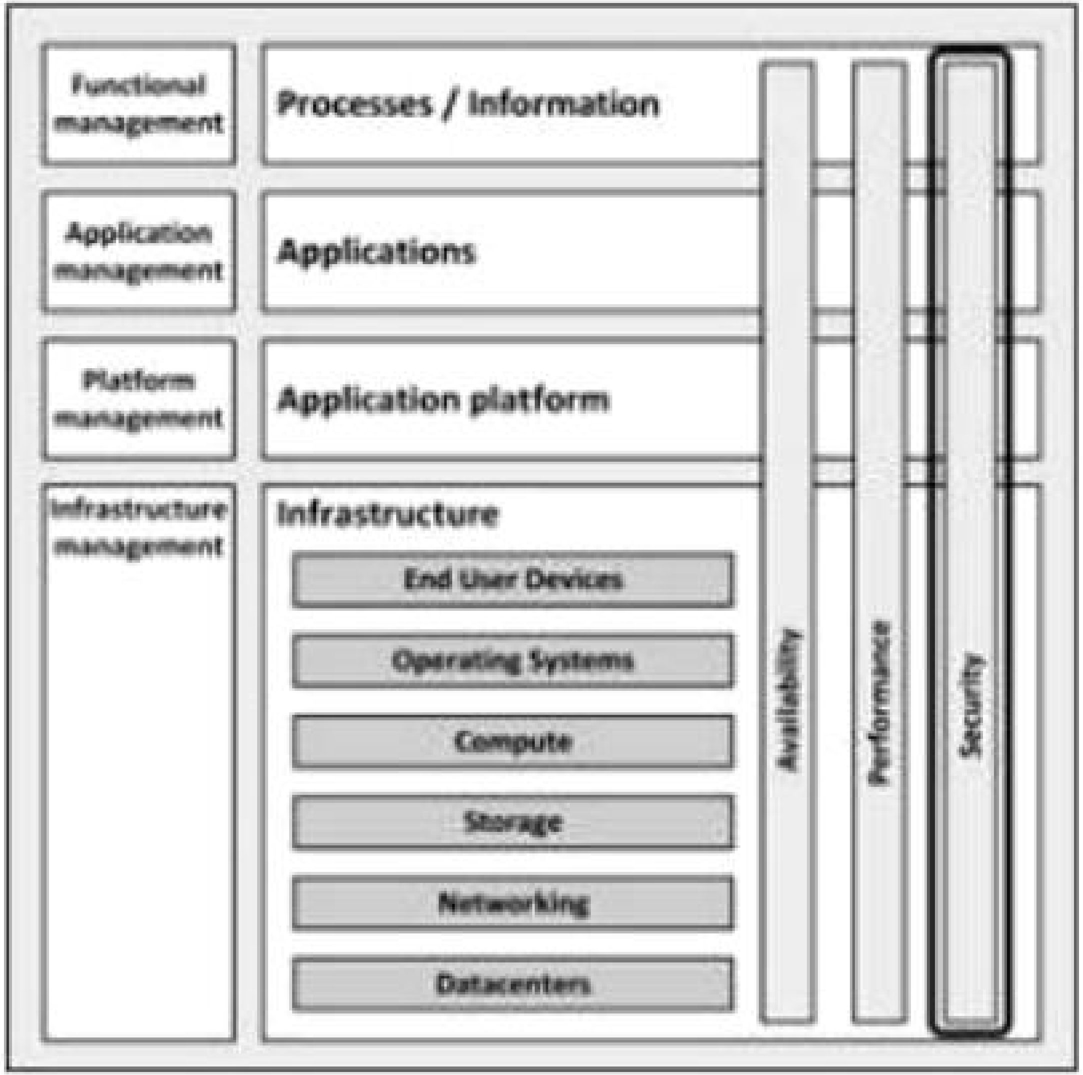


Figure 21: Security in the infrastructure model

✓ N

6.1 Introduction

- Creating secure IT systems is more important than ever.
- Year after year IT gets more complex, more business processes rely on it, and attacks are getting more sophisticated.
- In general, information systems security can be defined as the combination of availability, confidentiality, and integrity, focused on the recognition and resistance of attacks.

6.1 Introduction

- Computer crimes use some form of gaining control over – in the context of this book – IT infrastructures.
- There are various reasons for committing crime against IT infrastructures:
  - Personal exposure and prestige.
  - Creating damage to organizations
  - Financial gain.
  - Terrorism.
  - Warfare.

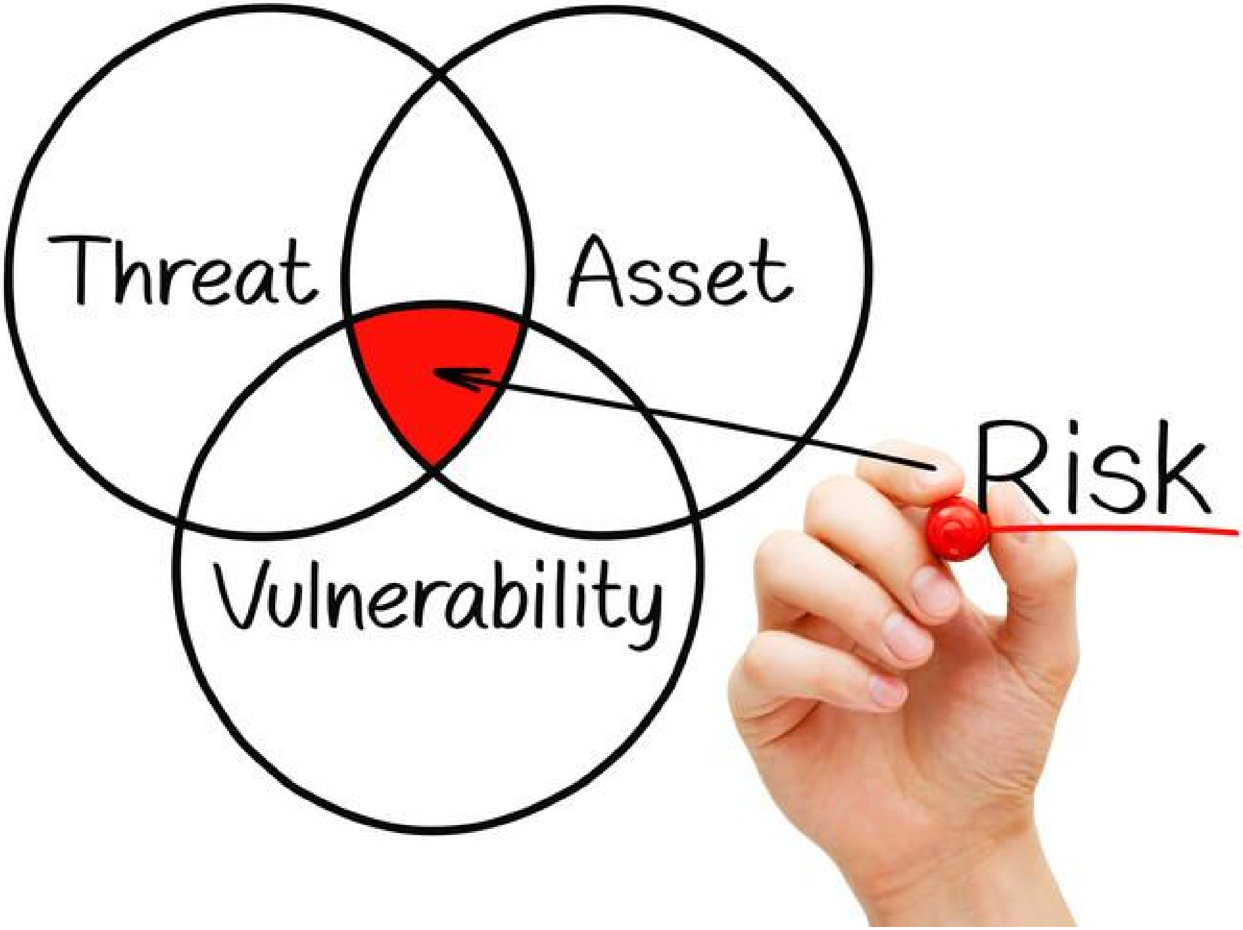
6.2 Risk management

- Managing security is all about managing risks.
- If there are no risks, we don't need any security controls.
- The effort we put in securing the infrastructure should therefore be directly related to the risk at hand.
- ***Risk management*** is the process of determining an acceptable level of risk, assessing the current level of risk, taking steps to reduce risk to the acceptable level, and maintaining that level.

6.2 Risk management

- A ***risk list*** can be used to quantify risks.
- Such a list can be compiled in a ***Business Impact Analysis (BIA)*** workshop with all relevant stakeholders.
- A risk list contains the following parts:
  - ***Asset name:*** the component that needs to be protected.
  - ***Vulnerability:*** a weakness, process or physical exposure that makes the asset susceptible to exploits.
  - ***Exploit:*** a way to use one or more vulnerabilities to attack an asset.

6.2 Risk management



V N

6.2 Risk management

- ***Probability:***

  For example:

  - 5: Frequent
  - 4: Likely
  - 3: Occasional
  - 2: Seldom
  - 1: Unlikely

- ***Impact:***
  - For example:

    Risk = Probability **x** Impact.
  - 4: Catastrophic:
  - 3: Critical:
  - 2: Moderate:
  - 1: Negligible:

6.2 Risk management

- Controls mitigate these risks.
- For example, a control for the risk of laptops with sensitive data getting stolen is to encrypt the hard disk to make the data unreadable for anyone but the owner.
- Controls can be designed and implemented based on the identified severity of the risk in the risk list.

6.2.1 RISK RESPONSE

- For each risk, the risk response must be decided upon by senior management.
- There four risk responses:

  1. ***Acceptance*** of the risk –
     for instance, the risk could be accepted if the risk is very unlikely to happen and the costs of the damage imposed by exploitation of the risk is low and the cost of mitigating the risk is high.

N ✓

6.2.1 RISK RESPONSE

- There four risk responses:

2. ***Avoidance*** of the risk –
   do not perform actions that impose risk (for instance, don’t host your own website or e-mail server).
3. ***Transfer*** of the risk –
   for instance transfer the risk to an insurance company (if it happens, the insurance company will pay for the damage).

N V

6.2.1 Risk response

- There four risk responses:
  4. ***Mitigation*** of the risk and accepting the residual risk. Some ways of doing this are:
     - Design for minimum risk.
     - Incorporate safety devices.
     - Provide warning devices.
     - Implement training and procedures.

✓ N

6.2.2 Exploits

- Information can be stolen in many ways. Here are some of the more common exploits related to infrastructure:
  - Key loggers
  - Network sniffers
  - Data on backup tapes PCs or disks can get into the wrong hands.
  - Corrupt or dissatisfied staff
  - End users are led to a malicious website that steals information (also known as phishing).

✓ N

6.2.3 Security controls

- Three core goals of security:
  - **C**onfidentiality,
  - **I**ntegrity, and
  - **A**vailability of information.
- Security controls must address at least one of these.

✓ iN

6.2.3 Security controls

1. ***Confidentiality*** prevents the intentional or unintentional unauthorized disclosure of data..
2. ***Integrity*** ensures that:
   - No modifications to data are made by unauthorized staff or processes.
   - Unauthorized modifications to data are not made by authorized staff or processes.
   - Data is consistent.
3. ***Availability*** ensures the reliable and timely access to data or IT resources by the appropriate staff

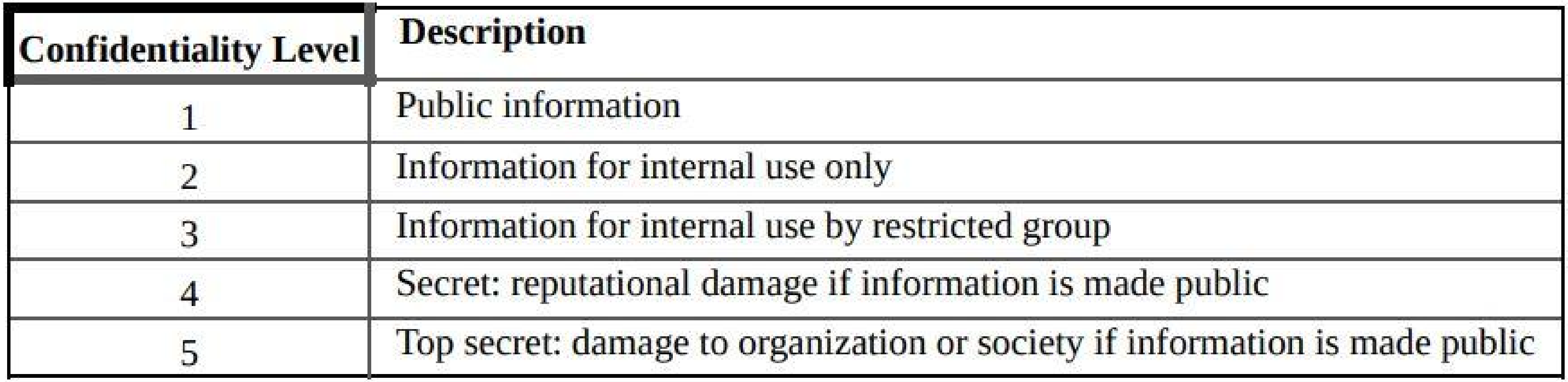
N ✓

6.2.3 Security controls

- Information can be classified based on CIA levels, typically between one and five.
- An example of a set of CIA levels is given in the tables.

✓ N

6.2.3 Security controls

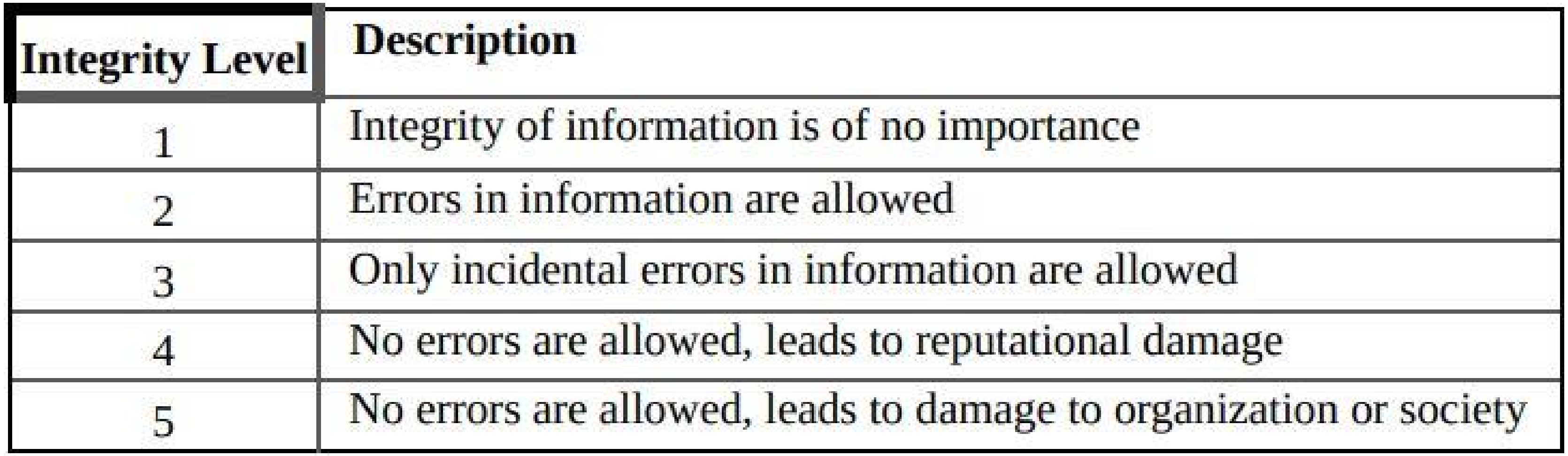


Confidentiality Level	Description
1	Public information
2	Information for internal use only
3	Information for internal use by restricted group
4	Secret: reputational damage if information is made public
5	Top secret: damage to organization or society if information is made public

Table 10: Confidentiality levels

✓ N

6.2.3 Security controls

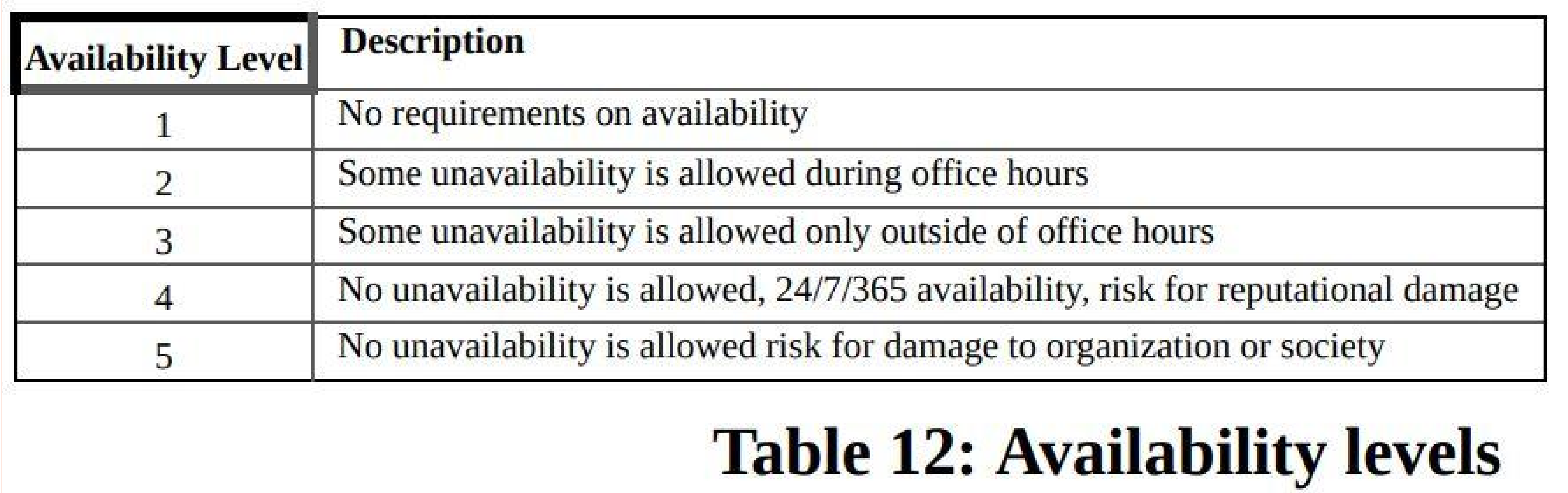


Integrity Level	Description
1	Integrity of information is of no importance
2	Errors in information are allowed
3	Only incidental errors in information are allowed
4	No errors are allowed, leads to reputational damage
5	No errors are allowed, leads to damage to organization or society

Table 11: Integrity levels

V N

6.2.3 Security controls



Availability Level	Description
1	No requirements on availability
2	Some unavailability is allowed during office hours
3	Some unavailability is allowed only outside of office hours
4	No unavailability is allowed, 24/7/365 availability, risk for reputational damage
5	No unavailability is allowed risk for damage to organization or society

Table 12: Availability levels

6.2.3 Security controls

- For each application or data set the CIA classification should be determined.
- For instance, for a mail server the CIA criteria can be classified as:
  - C = 3: Information for internal use by restricted group.
  - I = 3: Only incidental errors in information are allowed.
  - A = 3: Some unavailability is allowed only outside of office hours.

6.2.3 Security controls

- Based on the CIA classification and the risk list, controls can be implemented to mitigate the identified risks.
- A sample list of CIA based infrastructure specific controls is provided in book.
- Table 13: Example of CIA based controls

✓

6.2.4 Attack vectors

- 6.2.4.1 Malicious code
- 6.2.4.2 Denial of service attack
- 6.2.4.3 Social engineering
- 6.2.4.4 Phishing
- 6.2.4.5 Baiting

6.2.4 Attack vectors

- **6.2.4.1 Malicious code**
- Malicious code are applications that, when activated, can cause network and server overload, steal data and passwords, or erase data.
  - **Worms** are self-replicating programs that spread from one computer to another, leaving infections as they travel.
  - **Virus** is a self-replicating program fragment that attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels.

WannaCry:
In 2017, the WannaCry ransomware attack affected many organizations worldwide.
It affected organizations in over 150 countries.
It spread quickly through a vulnerability in Microsoft Windows systems.
The attack encrypted files on infected computers and demanded ransom payments in Bitcoin.

6.2.4 Attack vectors

6.2.4.1 Malicious code

- **Trojan Horse** appears to be useful software but will actually do damage once installed or run on your computer. Trojan horses can be used to deliver viruses or worms.

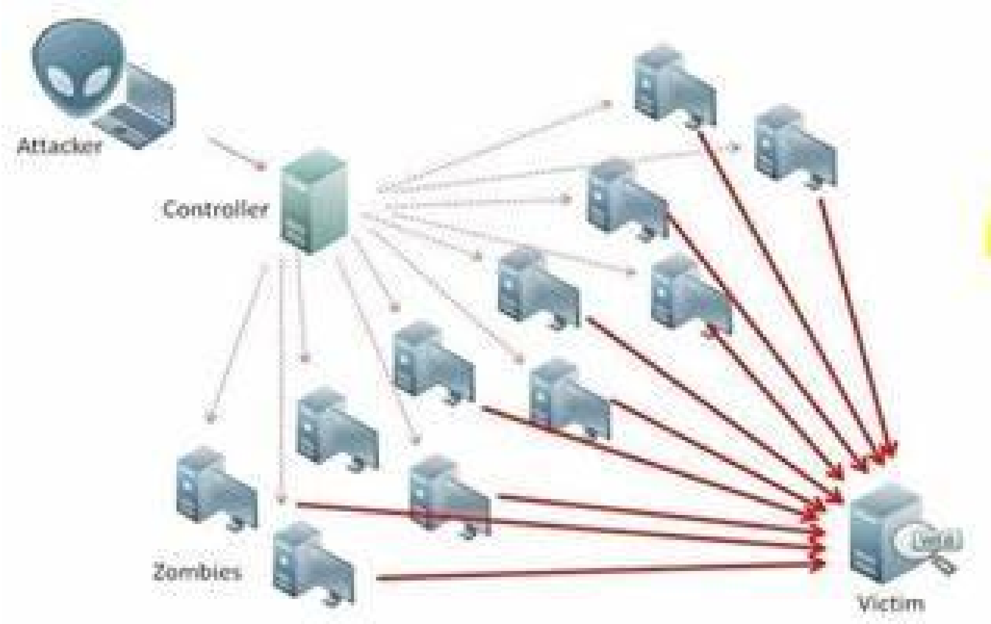
6.2.4 Attack vectors

- **6.2.4.2 Denial of service attack**
- A Denial of Service (DoS) attack is an attempt to overload an infrastructure to cause disruption of a service.
- This overload can lead to downtime of a system, disabling an organization to do its business.
- high load → the server needs to process,
- requests fill up the request queues, → the server either crashes, or performs so slow

GitHub (2018):
GitHub was hit by a massive DDoS attack in 2018.
Users worldwide faced disruptions accessing GitHub.
Attackers misused Memcached servers to amplify the attack.
Response: GitHub implemented measures to mitigate the attack.

6.2.4 Attack vectors

- **6.2.4.2 Denial of service attack**
- Because usually one attacking computer alone has insufficient power or bandwidth available to bring down a server, most of the time a ***Distributed Denial of Service (DDoS)*** attack is used.
- In this case the attacker uses many computers to overload the server.



6.2.4 Attack vectors

- **6.2.4.2 Denial of service attack**
- Some preventive measures to a DDos attack are:
  - ***Split*** business and public resources
  - ***Move*** all public facing resources to an external cloud provider
  - ***Setup*** automatic scalability
  - ***Limit*** bandwidth for certain traffic –maximum number of calls per second on ports 53 (DNS) and 123 (NTP)
  - Lower the ***Time to Live (TTL)*** of the DNS records

6.2.4 Attack vectors

- **6.2.4.2 Denial of service attack**
- Some preventive measures to a DDos attack are:
  - ~~Lower the ***Time to Live (TTL)*** of the DNS records~~
  - ~~Setup monitoring for early detection on:~~
    - ~~Traffic volume~~
    - ~~Source and number of requests~~
    - ~~Transaction latency~~

✓

6.2.4 Attack vectors

- **6.2.4.2 Denial of service attack**
- When a DDoS attack actually occurs, some actions could be:
- Immediately inform your internet provider and ask for help
- Run a script to terminate all connections coming from the same source IP address if >10
- Change to an alternative server (with another IP)
- Scale-out the public facing environment under attack
- Reroute or drop suspected traffic

6.2.4 Attack vectors

- **6.2.4.2 Denial of service attack**
- More recent attacks show an alternative DDoS attack, called ***Low & Slow***,
- where a website is used in a normal way (low key), but at an extremely slow pace.
- In this type of attack, legitimate data is sent to a web server (using a HTTP POST command),
- but only one byte at a time,
- with a long wait time between the bytes.
- The web server keeps on waiting for bytes, while keeping a channel occupied and busy.

6.2.4 Attack vectors

- **6.2.4.3 Social engineering**
- In social engineering,
  social skills are used
  to manipulate people
  to obtain information,
  such as passwords or other sensitive information,
  which can be used in an attack.

Ubiquiti Networks (2016):s
In 2016, Ubiquiti Networks, a tech company, was tricked.
Criminals pretended to be the CEO in emails to employees.
They asked workers to send a lot of money to fake accounts.
The company lost around $46.7 million in this scam.

6.2.4 Attack vectors

- **6.2.4.4 Phishing**
- Phishing is a technique of obtaining sensitive information.
- Typically, the phisher
  sends an e-mail
  that appears to come from a legitimate source,
  like a bank or credit card company,
  requesting "verification" of information.

Facebook Phishing Attack (2020):
Cybercriminals launched a phishing attack targeting Facebook users in 2020. They sent messages with a link to a fake Facebook login page, claiming that the recipient's account was compromised and needed immediate verification. Unsuspecting users who entered their credentials on the fake page had their accounts hijacked.

6.2.4 Attack vectors

- **6.2.4.5 Baiting**

Example:
Iran's nuclear program

- Baiting uses ***physical media***, like an USB flash drive, and relies on the curiosity of people to find out what is on it.
- For instance, an attacker leaves a malware infected USB flash drive in some location where it will be easily found, like the elevator or the parking lot of an organization it wants to attack.
- some employee picks up the device.
- put into an organization owned PC,
- malicious software is installed automatically

6.2.4 Attack vectors

- **6.2.4.5 Baiting**
- The effect of this kind of attack can largely be mitigated by switching off the "auto-run" feature on all organization PCs.

Any Questions?