Intro

Cybersecurity

Jeppe Stenstrup Lauridsen

September 9, 2021

1 Information

The exam is written, and there will be 2 assignments throughout the course. They will be completed after the lectures, so they are not to be completed from home.

2 Internet of Things

As everything is connected to the internet today, we need to have a clear concept for security when it comes to products.
So in order for one to create the tech of the future, one must understand all the risks that exists in the given tech.
A way to enforce these risks, an AI is typically implemented to run some tests whenever new features or changes are introduced, to validate that there are no "open doors" into the product.
It is important to note that **it is impossible to be 100% secure. No product/software is completely safe**.

3 Risks and defense mechanisms

3.1 The CIA-Triad

- Confidentiallity
  - Encryption
  - Access control
  - Auth
- Intetegrity
  - Checksum
- Availability
  - Backups

NOTE: TCP is not secure by default. It only handles data from A to B

4 Attack surfaces

- Search-bar
- Open port(s)
- USB-port(s)
- etc.

These are called **Attack Vectors** ($\sum$)

4.1 Vulnerabilities

The 4 main vulnerabilities are:

- Network
- Physical machines
- Software
- Humans

and the actors of the concepts are:

- Attacker
- Operator
- Designer

4.2 Attack types

4.2.1 Virus

Key: Self-replicating

4.2.2 Trojan

Key: Hidden begind a desired task

4.2.3 Spyware

Key: Monitoring, ie. a keylogger

4.2.4 Denial of Service

Key: Rendering a system unavailable to the general users

4.3 Protection

4.3.1 Firewall

A layer that filters internet traffic

4.3.2 Proxy

Disguises IPs

4.3.3 Intrusion detection

Monitoring for attacks

4.3.4 Intrusion prevention

Detection + conter meassures

4.3.5 Other meassures

- Penetration-testing
- Attacker POV
- Attack simulations

4.4 General attack steps

1. **Gather info**: IPs
2. Scan IPs
3. **Fingerprinting**: OS, version of OS, what browser, etc.

4. Identify vulnerabilities
5. Exploit said vulnerabilities
6. **If Attack-Simulation**: Fix the vulnerabilities