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**
- **• 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 successful leads using already known vulnerabilities**
        - **🤗 E.g. Microsoft had already patched the EternalBlue vulnerability that NSA developed before it was leaked to public. However, many systems still remained unpatched due to users not updating their systems. So the same vulnerability on**

unpatched systems were still successfuly exploited by first WannaCry ransomware that compromised hundreds of thousands computers, and then by NotPetya malware. 1

- **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:**
- **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**

i. **Create a breach e.g. through spear phishing**

ii. **Exploit inner system vulnerabilities**

iii. **Control of the system or its segments**

iv. **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.**
- **Categories include:**
    - **Command and control (C2) warfare**
    - **Intelligence-based warfare**
    - **Electronic warfare**
    - **Psychological warfare**
    - **Hacker warfare**
    - **Economic information warfare**
    - **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**