Principles of Information Security

Introduction

Cyber Security

- Cyber security is all about defending computing resources and data from malicious attacks.
- For effective security, we need physical protection, processes, protocols, tools, techniques, laws and regulation.
- Lack of effective security may lead to leak of sensitive information, financial losses, endanger lives, disruption of major infrastructures

Security Engineering

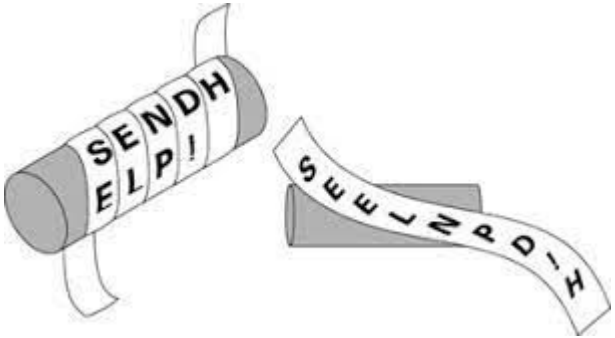
- Study of building secure systems that remain dependable in the face of malice, error, and mischance.
- Involves study of tools, processes, and methods needed to design, implement, and test secure systems.
- Requires knowledge of multiple disciplines such as Cryptography, psychology, laws and regulations, operations of organizations, etc.

Major Security Requirements (CIA Triad)

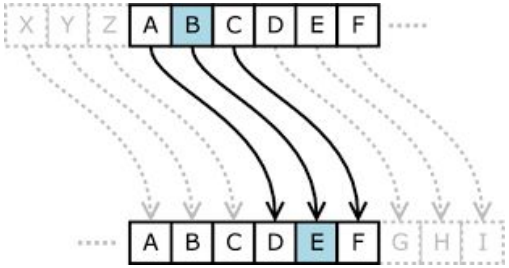
- **Confidentiality**: Concealing information.
- **Integrity**: Ensuring trustworthiness of the data or resource
- **Availability**: Ensuring that the services are available when required by the user.

Confidentiality

- **Confidentiality**: Concealing information.
  - Encryption and Access control help in achieving confidentiality
  - Secret message passing dates back to thousands of years

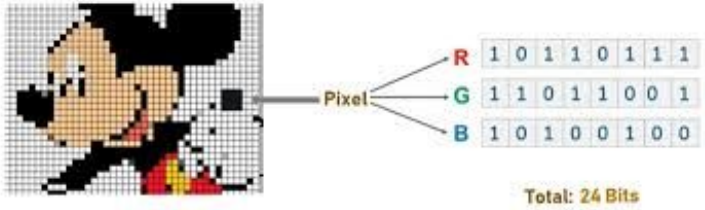


Transposition Cipher by Spartans
(Scytale cipher)



Substitution Cipher by Caesar

Confidentiality



We Entered the Lounge to Check Our Main Entrance

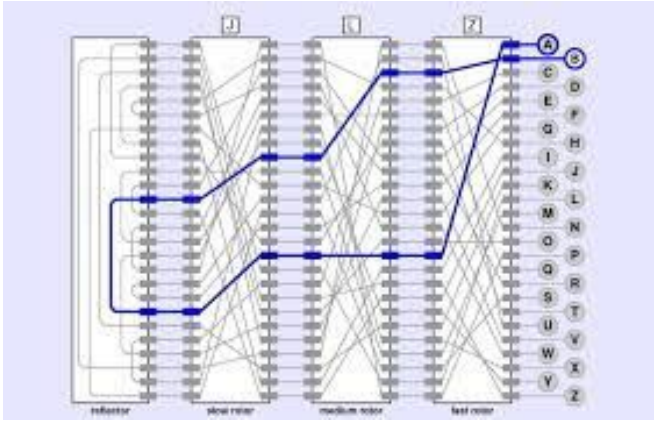
Image Steganography

Text Steganography

Enigma Machine

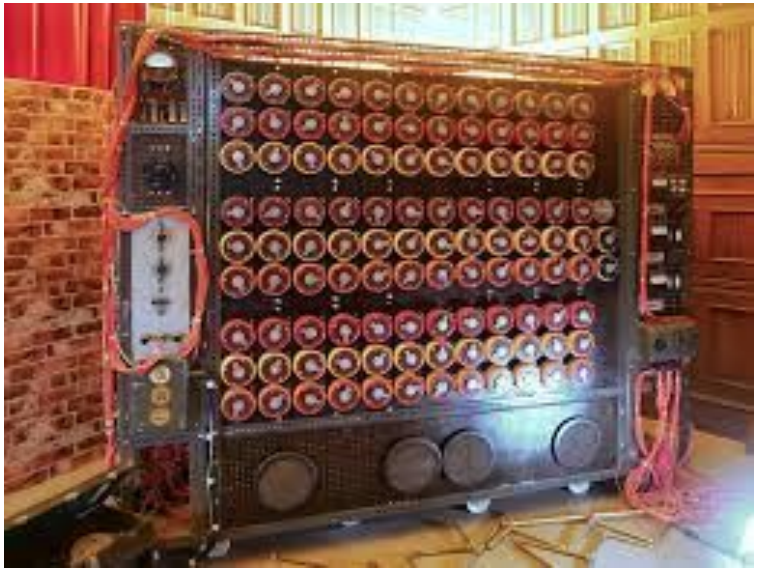
- Encryption machine used by the Germans in the World War 2.
- Resembled a typewriter. Pressing a letter key is would light up a bulb for another letter.
- Used three rotors, each rotated at different speeds
- Required an initial set up key
- On encrypting a letter, it never produced the same letter

Enigma Machine



The Bombe Machine

- A research center at Bletchley Park was set up to break the Enigma encryption
- Here, Alan Turing and his team developed a machine called the Bombe

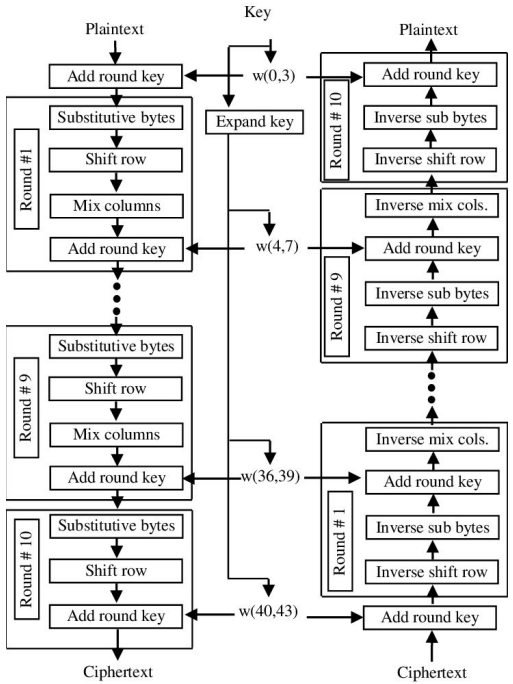


Confidentiality

- In today’s digitized world, a lot of sensitive information is stored in the digital form
- Online shopping, digital banking, digitisation of documents, digital communication
- The olden cryptography techniques are inadequate for today’s requirement

Confidentiality

- We use stronger cryptographic algorithms such as AES, RSA, Elliptic Curve Cryptography
- They are open algorithms
- In practical applications, longer keys are used so that it becomes computationally very expensive to crack the algorithm



https://www.researchgate.net/figure/Block-diagram-for-AES-encryption-and-decryption_fig1_324796235

Confidentiality

Access Control

- Access Control also plays an important role in providing confidentiality
- Access Control regulates access to resources
- Every access request for a resource goes through an access control module which decides whether to allow or deny the access based on predefined rules

Integrity

- **Source integrity:** Ensuring the identity of the source entity
- **Data integrity:** Ensuring that the data is not modified by a malicious entity
  - This can be done using hashing
  - Hash functions are one-way functions that help in detecting any changes made in a message

Availability

- **Availability:** Ensuring that the services are available when required by the user.
  - Unavailability of a service may cause financial loss, damage reputation of an organization, may even endanger lives
  - Denial of service (DoS), Distributed denial of services (DDoS), ransomware are common threats to availability

Other Major Requirements

- Non-repudiation: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
- Privacy: Protecting the personal information of individuals.

Vulnerability

- A weakness in a system which can lead to an unexpected, undesirable event compromising the security of a system.
- Vulnerability can be in any component of a system
  - Hardware
  - Operating system
  - System software
  - Application
  - Configuration
  - Protocol
  - Process
  - .....

Vulnerability Databases

- Common Vulnerabilities and Exposures (CVE), is a list of publicly disclosed computer security flaws.
- The database is maintained by the MITRE corporation
- Every new vulnerability is assigned a unique CVE ID number
- Contains brief descriptions of the vulnerabilities
- Helps in sharing data among tools, databases, and services

Vulnerability Databases

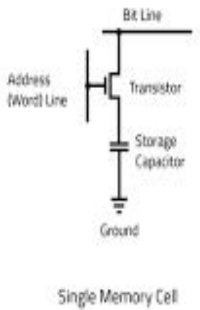
- To be categorized as a CVE vulnerability, a vulnerability must meet a certain criteria
  - **Independent of other issues:** You must be able to fix the vulnerability independently of other issues.
  - **Acknowledged by the vendor:** The vulnerability is known by the vendor and is acknowledged to cause a security risk.
  - **Is a proven risk:** The vulnerability is submitted with evidence of security impact that violates the security policies of the vendor.

OS Vulnerability

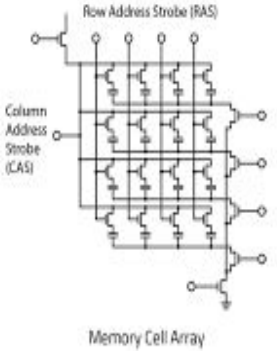
- Race Condition vulnerability of Dirty COW attack (CVE-2016-5195)
- Privilege escalation attack
- Provides write access to root files (local privilege escalation)
- Doesn’t check the completion of Copy-on-Write cycle before writing to a page in mmap()
- Can be exploited using two threads
    - One thread uses madvise to release a page
    - Other thread tries to write to a read-only page

Hardware Vulnerability

- Bit flip vulnerability in DRAM leading to Rowhammer attack(CVE-2020-10255)
- Discovered in 2014
- DRAMs use Capacitors to store data
- With the advancement in technology, the rows became dense
- Closer the two charged components, higher is the electromagnetic interference
- Continuous access of a row can toggle the nearby cells



Single Memory Cell



Memory Cell Array

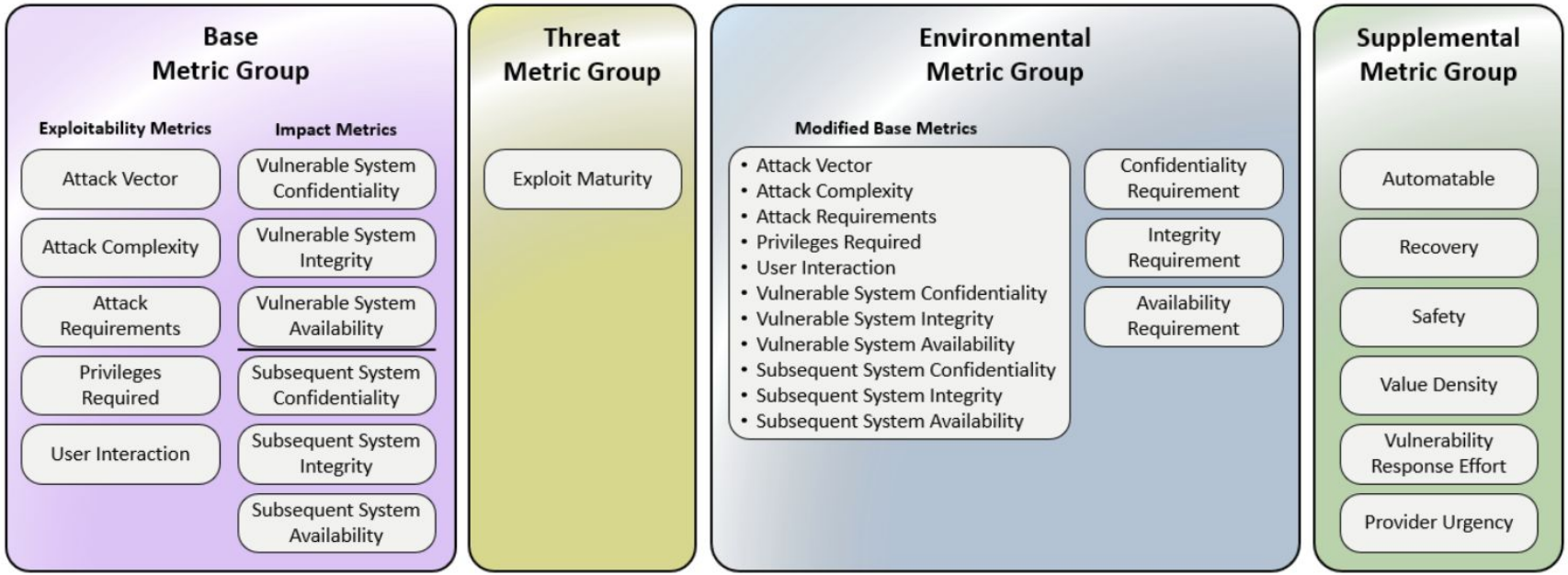
Hardware Vulnerability

- Countermeasure
    - Increase the refresh rates
    - Increase the access interval
    - Better error correction

Common Vulnerability Scoring System

- Common Vulnerability Scoring System (CVSS) is used to evaluate the threat level of a vulnerability.
- It provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.
- The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Common Vulnerability Scoring System



Some Common Attack Types

- **Piggybacking and Tailgating**

Some Common Attack Types

- **Social Engineering:** manipulation technique that exploits human error to gain private information, access, or valuables.
  Example: Phishing,Whaling, Vishing

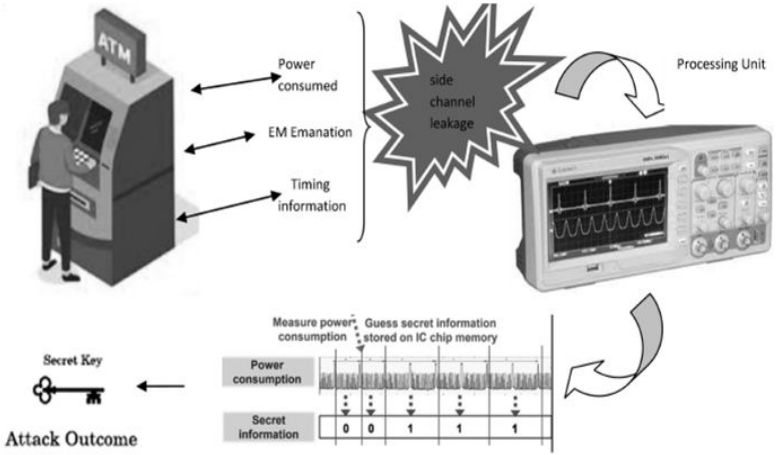
- **Malwares:** Malicious Softwares.
  Example: Spyware, Trojan-horse, Ransomware

Some Common Attack Types

- **Network Intrusion:** Attack on Network Resources, generally by exploiting vulnerabilities in network protocols.
  Example: Man-in-the-Middle Attack, Spoofing, DoS, DDoS
- **Code Injection Attacks:** injecting malicious code into a vulnerable applications.
  Example: SQL Injection, Cross-site Scripting (XSS)

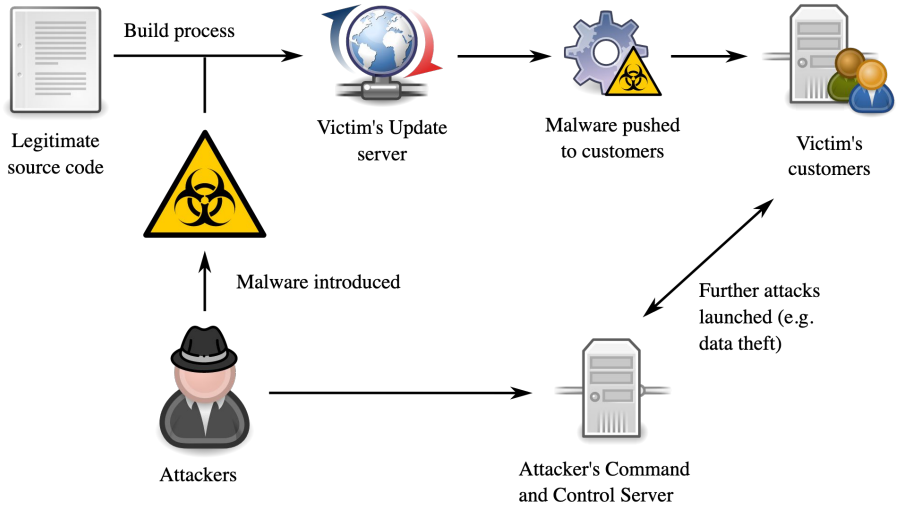
Some Common Attack Types

- **Side Channel Attacks:** attacks based on the implementation of a system (as opposed to attacks which are based on an algorithm/protocol) which is performed via channels or mediums that are created as a side effect of the main operation of the attacked system.
  Example: Cracking the encryption keys based on the time taken for encryption/decryption, Using heat generated by devices, number of memory accesses to extract sensitive data.



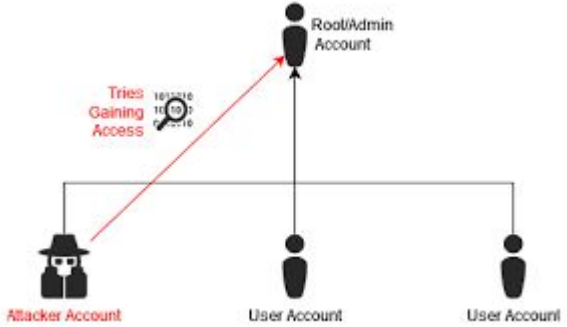
Some Common Attack Types

- **Supply Chain Attacks :** implanting malicious, whether code/hardware, into the manufacturing chain of a single product.



Some Common Attack Types

- **Privilege Escalation Attacks:** Attacker tries to gain higher privileges on the system/network. It can be of two types:
  - Vertical Privilege Escalation: Attacker tries to gain higher privileges with the current regular user account
  - Horizontal Privilege Escalation: Attacker tries to gain access to user account that has higher privileges



ATTA&CK Framework

- Stands for **A**dversarial **T**actics **T**echniques **&** **C**ommon **K**nowledge
- A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
- Can be used for development of threat models
- Uses the fact that the attackers generally use similar TTPs (Tactics, Techniques, and Procedures) and they are less likely to change frequently.

ATTA&CK Tactics

1. Reconnaissance: Adversaries gather information that they can use to plan future operations
2. Resource Development: The adversary tries to establish resources they can use to support operations. It consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting.
3. Initial Access: Consists of techniques that use various entry vectors to gain their initial foothold within a network.
4. Execution: Consists of techniques that result in adversary-controlled code running on a local or remote system.

ATTA&CK Tactics

5. Persistence: Consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
6. Privilege Escalation: Consists of techniques that adversaries use to gain higher-level permissions on a system or network.
7. Defense Evasion: Consists of techniques that adversaries use to avoid detection throughout their compromise.
8. Credential Access: Consists of techniques for stealing credentials like account names and passwords.

ATTA&CK Tactics

9. Discovery: Consists of techniques an adversary may use to gain knowledge about the system and internal network.
10. Lateral Movement: Consists of techniques that adversaries use to enter and control remote systems on a network.
11. Collection: Consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.
12. Command and Control: Consists of techniques that adversaries may use to communicate with systems under their control within a victim network.

ATTA&CK Tactics

13. Exfiltration: Consists of techniques that adversaries may use to steal data from your network.
14. Impact: Consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.

Threats and Threat Modeling

- A threat is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental (failure of a Storage Device).
- An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss. [NIST SP800-160]
- Threat modeling is a planned activity for identifying and assessing application threats and vulnerabilities.
- Threat modeling can be applied to a wide range of things, including software, applications, systems, networks, distributed systems, Internet of Things (IoT) devices, and business processes.

Threat Models

- A threat model is a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the lens of security.
- A threat model typically includes:
  - Description of the subject to be modeled
  - Assumptions that can be checked or challenged in the future as the threat landscape changes
  - Potential threats to the system
  - Actions that can be taken to mitigate each threat
  - A way of validating the model and threats, and verification of success of actions taken

Threat Factors

- Threat source: The origin of threat either internal or external.
- Threat agents: The agents that cause threats
- Threat motivation: The goal/motivation of attackers on a system which can be malicious or non-malicious
- Threat intention: The intent of the human who may cause the threat.
- Threats impacts: Threat impact is a security violation that results from a threat action. For example, Destruction of information, Corruption of information, Theft/ loss of information, Disclosure of information, denial of use, Elevation of privilege and Illegal usage.

Threat Agents

- Nation states—hostile countries can launch cyber attacks against local companies and institutions, aiming to interfere with communications, cause disorder, and inflict damage.
- Terrorist organizations—terrorists conduct cyber attacks aimed at destroying or abusing critical infrastructure, threaten national security, disrupt economies, and cause bodily harm to citizens.
- Criminal groups—organized groups of hackers aim to break into computing systems for economic benefit. These groups use phishing, spam, spyware and malware for extortion, theft of private information, and online scams.
- Hacktivists: An individual or a group that attacks a computing system for socially or politically motivated reason.

Threat Agents

- Individual Hackers—individual hackers target organizations using a variety of attack techniques. They are usually motivated by personal gain, revenge, financial gain, or political activity. Hackers often develop new threats, to advance their criminal ability and improve their personal standing in the hacker community.
- Malicious insiders—an employee who has legitimate access to company assets, and abuses their privileges to steal information or damage computing systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the target organization. They can also be outsiders who have compromised a privileged account and are impersonating its owner.

STRIDE Threat Model

- A threat model, created by Microsoft security researchers in 1999, which is meant to guide the discovery of threats in a system.
- Aims to ensure an app or system fulfills the CIA triad (confidentiality, integrity and availability).
- It is used to spot threats during the design phase of an app or system.
- The first step helps find potential threats using a proactive process. The design of the system forms the basis for spotting threats. The next steps include finding the risks inherent in the way the system has been implemented, and then taking actions to close gaps.

STRIDE Threats

	Type of Threat	What Was Violated	How Was It Violated?
S	Spoofing	Authentication	Impersonating something or someone known and trusted.
T	Tampering	Integrity	Modifying data on disk, memory, network, etc.,
R	Repudiation	Non-repudiation	Claim to not be responsible for an action
I	Information Disclosure	Confidentiality	Providing information to someone who is not authorized
D	Denial of Service (DoS)	Availability	Denying or obstructing access to resources required to provide service
E	Elevation of Privilege	Authorization	Allowing access to someone without proper authorization

References

1. How did the Enigma Machine work? https://www.youtube.com/watch?v=ybkkiGtJmkM
2. https://www.youtube.com/watch?v=d2NWPG2gB_A
3. https://www.youtube.com/watch?v=V4V2bpZlqx8
4. https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c01.pdf
5. http://apt.cs.manchester.ac.uk/projects/ARMOR/RowHammer/
6. https://www.youtube.com/watch?v=kEsshExn7aE
7. https://www.cve.org/CVERecord?id=CVE-2022-30190
8. https://www.youtube.com/watch?v=azX4y8WKysA
9. https://www.cvedetails.com/browse-by-date.php
10. https://www.first.org/cvss/calculator/4-0
11. https://www.cve.org/
12. https://owasp.org/www-community/Threat_Modeling
13. https://owasp.org/www-community/Threat_Modeling_Process
14. https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
15. https://www.sciencedirect.com/science/article/pii/S1877050914006528
16. https://attack.mitre.org/