Lecture 1 🌱

> **Class**: Security Modeling and Disaster Recovery Planning
>
> **Date**: 9.30AM , 10 Nov
>
> **Author**: Lasal Hettiarachchi

Key learnings:

- Security Principles
- Attack Vector
- Threat Modeling
- Security Control

Information

- Informations are assets (vulnerabilities of databases)
- Information in many forms
  - Printed paper
  - Electronicaly stored
  - Verbal
  - Transmited by post
- Our focus is on electronically stored or transmitted

Information Security

- Definition NIST(National instute of standars and systems):
- "The protection of information and information systems from **unauthorized access, use, disclosure, disruption, modification,** or destruction in order to provide **confidentiality, integrity, and availability**."
- Protection of data against unauthorized access
- To do this we have to protect 2 things
  - Information
  - Information systems (Networks)
- Information security is not just about stoping attacks
  - Business continuity : If attack sucessfull the business can continue to work
  - Minimize business risk
  - Maximize ROI
  - Maximize Business oppertunities

Information Security Terminology

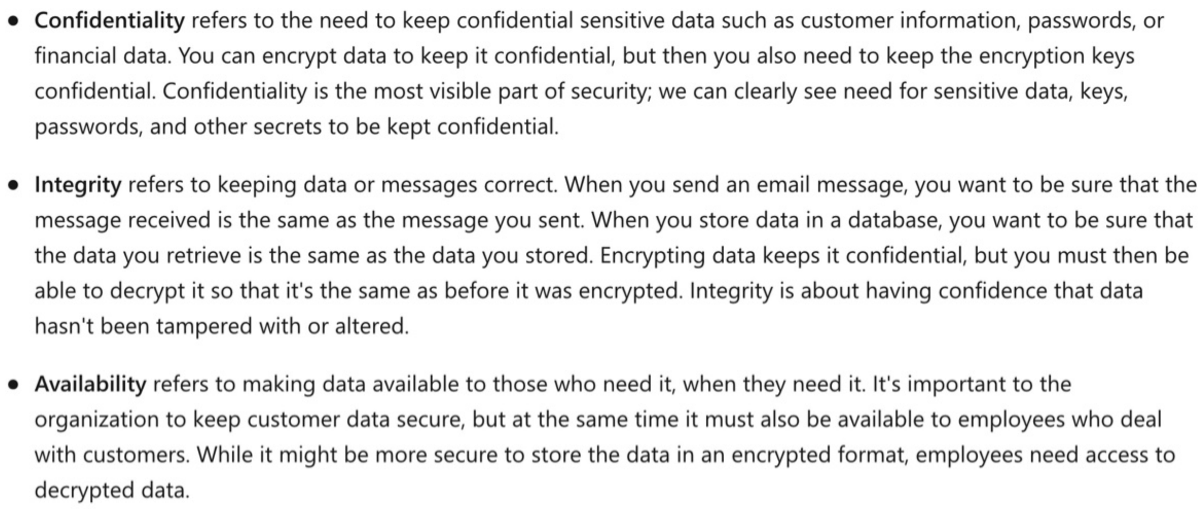
- System resource / Asset : Anything that has a value and needs to be safeguarded
- Vulnarability: Weakness in the system
  - week pw
  - using a cryptographic algorithm that has proven to be compromised
  - Unsafe network protocol
- Threat: Potential danger caused by the vulnerability
- Threat Agent/Attacker: Anyone who **tries** to use the vulnerability
- Risk: Likelihood of the agent taking advantage of the vulnerability corresponding to businesses impact
- Exposure: How much area is exposed by the vulnerability
- Countermeasures : Things done to mitigate vulnerability

Information Security Importance

- Since it keeps the assets secure which are essential for keepingg the business running
- IS can be expected to protect
  - Information assets
  - Mission critical applications and systems
  - Productivity - daily activities and operations
  - The privacy of individuals and their confidential information
  - The legal position of the organization by complying with laws and contracts
- Protect internet based app,web based , eccomerce , VOIP
- Causes of damage such as malicious code, computer hacking and DoS attacks have become more common more ambitious and increasingly sophisticated.
- Information security is important to both public and private sector businesses, and to protect critical infrastructures

Information Security principles

- Information Security Principals



- **Confidentiality** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data. You can encrypt data to keep it confidential, but then you also need to keep the encryption keys confidential. Confidentiality is the most visible part of security; we can clearly see need for sensitive data, keys, passwords, and other secrets to be kept confidential.
- **Integrity** refers to keeping data or messages correct. When you send an email message, you want to be sure that the message received is the same as the message you sent. When you store data in a database, you want to be sure that the data you retrieve is the same as the data you stored. Encrypting data keeps it confidential, but you must then be able to decrypt it so that it's the same as before it was encrypted. Integrity is about having confidence that data hasn't been tampered with or altered.
- **Availability** refers to making data available to those who need it, when they need it. It's important to the organization to keep customer data secure, but at the same time it must also be available to employees who deal with customers. While it might be more secure to store the data in an encrypted format, employees need access to decrypted data.

    - Confidentiality: Only authorized parties can view the Information . Assurance that information is not disclosed to unauthorised individuals, programs or processes.
        - Only the specific student and the admin can view the student marks(Other students cannot)
        - mechanisms to ensure confidentiality :
            - Encryption
            - Transmission protocols
            - database views
            - controlled traffic flow
            - Logical and physical access control (Biomentrics)
    - Integrity : Ensures the information is correct / not tampred with. Integritty can be changed intentionally or accidentally(hardware or human error).
        - Students cannot change the marks
        - mechanisms: Hashing mechanisms to have digital signature
    - Availability : Information is available when required
        - Student marks should be available
        - Mechanism:
            - Backups
    - (CIA triad)

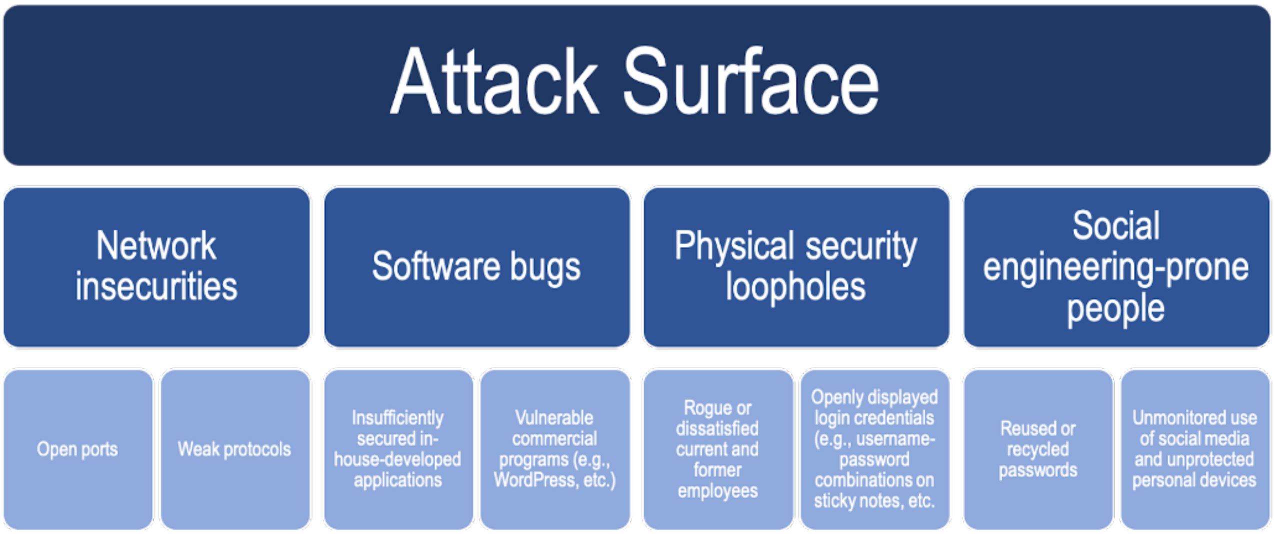
User Security principles

- In addition to IS principles there are user Security principles to do with users.
    - Authentication : Users are who they claim to be
        - Login system
    - Non-repudiation : Systems where there are multiple users are communicating with one another

- The actions performed by the using can be traced back to the user. User cannot deny an activity that they are **authorized** to do

Threat modeling

- Process of analysing system to identify threat agents, risks , counter messures, impacts etc.
- Understand the system environment to better comprehend what they are trying to protect and the mitigations and what risks are most eminent
- Different people have different approaches.
    - Costs more to develop secure software (Security guys say needs to be more secure, managers need low cost)
- Cyber threat analysis:
    - Process that evaluates internal and external threats and vulnerabilities and matches them against real-world attacks
- Attack vector: Direction from which the attack originated
    - Visualising the attacks hapenning
    - 3 main things in the attack vector
        - Source: attacker
        - Vulnerability
        - Impact / Malicious content
        - ex: An attacker looking to steal my bank account and use the unpatched windows on my PC to install a keylogger
            - attacker: trying to steal the money
            - vulnerability : Unpatched windows(not allowing to install trojan)
            - payload : Keylogger
- Attack surface: All possible attack vectors on a system. Combination of all system and asset vulnerabilities .
    - This has 4 main catagories
        - Network insecrities
            - Open ports
            - Weak protocols
        - **Software bugs**
            - Insufficiently secured inhouse-developed applications
            - Vulnerable commercial programs (e.g.WordPress, etc.)
        - Physical security loopholes
            - Former employee
            - Openly displayed login credentials
            - Server rooms not being properly secured
        - Social engineering prone people
            - Reused passwords
            - Unmonitored use of social media and unprotected devices


Attack Surface
Network insecurities
Software bugs
Physical security loopholes
Social engineering-prone people
Open ports
Weak protocols
Insufficiently secured in-house-developed applications
Vulnerable commercial programs (e.g., WordPress, etc.)
Rogue or dissatisfied current and former employees
Openly displayed login credentials (e.g., username-password combinations on sticky notes, etc.
Reused or recycled passwords
Unmonitored use of social media and unprotected personal devices

- Security is not an after thought

Threat modeling Techniques

- This can be done at design, Implementation or testing stage
- Some take a quantitative or a qualitative approach
- goal: Develop a formal process while identifying, documenting, and mitigating security threats.

CVSS

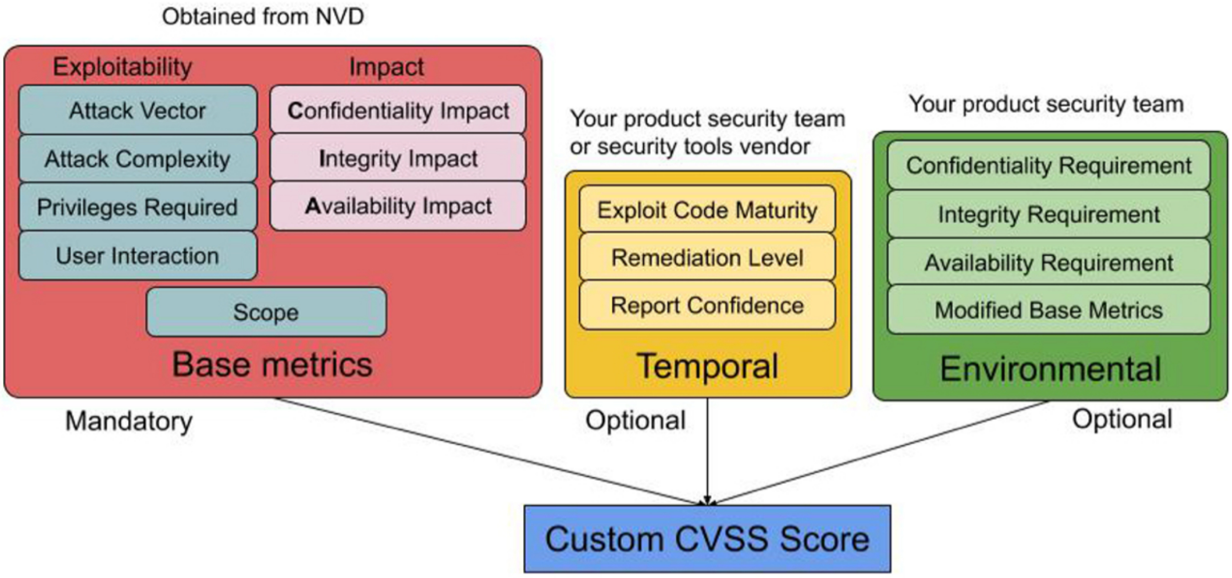
(Mostly used for software)

- Common vulnerability scoring system
- Capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.
- The numerical score can be translated into a qualitative representation (such as low, medium, high, and critical)
- Helps organizations properly assess and prioritize their vulnerability management processes.

CVSS 3.1

Environmental: Customize the base score to meet the company requirement

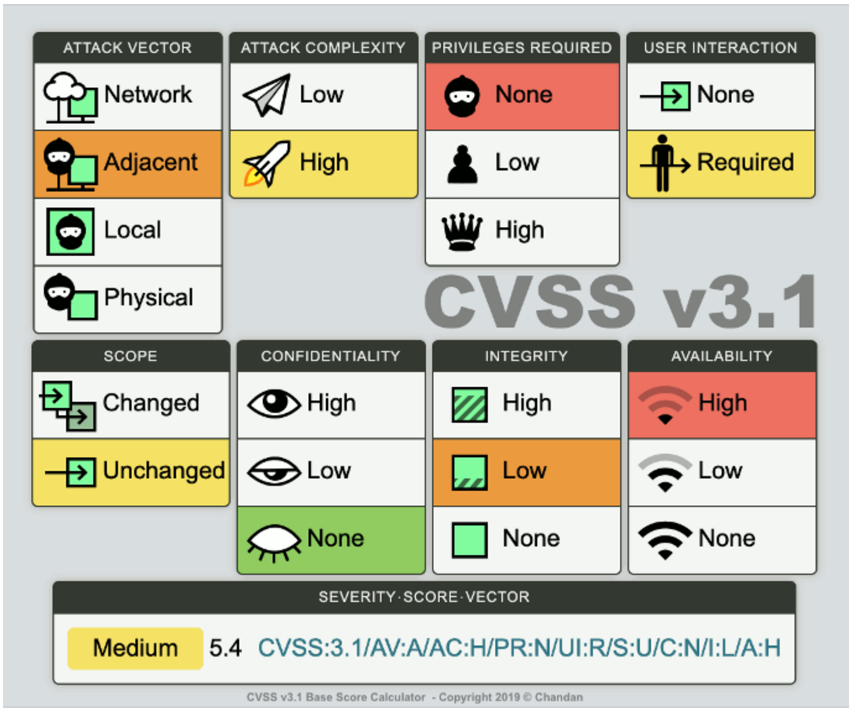
Temporal: Overtime how this is chaning



Demo 1.05.00

Attack Metrics

Expolitability: How easy is to use the vulnerability



ATTACK VECTOR	ATTACK COMPLEXITY	PRIVILEGES REQUIRED	USER INTERACTION
Network	Low	None	None
Adjacent	High	Low	Required
Local		High	
Physical			

CVSS v3.1

SCOPE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Changed	High	High	High
Unchanged	Low	Low	Low
	None	None	None

SEVERITY·SCORE·VECTOR

Medium 5.4 CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:H

CVSS v3.1 Base Score Calculator - Copyright 2019 © Chandan

Attack Vector

Physical : Need physical device access

Local: LAN

Adjacent : Need to be in an adjacent network

Network : Internet

Attack Complexity

Low

High

Privilages

None

Low

High

User interation

none: like a worm can spread through the system without user intreaction

need: needs click

Scope changed (Use first attack to mount more attacks**)**

changed

Unchanged

If scope can be changed threat goes up

Security control

- how to mitigate the vulnerabilities identified
- Access contol can be implemented in many layers: Organization, Network, individual systems
- 3 main types controls to mitigate the threats possed by a vulnerability
  - Technical Security
    - Biomentric
    - Encryption
    - VPN
    - Firewalls
    - Antivirus
  - Physical
    - Actual hardware: biometrics to enter the server room
    - CEOs laptop harddrive is encrypted and cannot be used without giving the password
  - Administrative
    - Use of policies, practices and procedures
      - Effective hiring practices
      - Pre-employment background checks
      - Controlled termination processes: All access is removed after employees resign
      - Security awareness: Employees are aware of security practices

Resources:

Common Vulnerability Scoring System Version 3.0 Calculator
https://www.first.org/cvss/calculator/3.0
https://www.first.org/cvss/calculator/3.0

Describe the Zero Trust model - Training
Describe the Zero Trust model
https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/4-describe-zero-trust-model