Lecture 1 Course Overview

Data and Network Security (University of Canterbury)

Lecture 1: Course Overview

What is cybersecurity?

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity, availability, and confidentiality** of information system resources including hardware software firmware info/data and telecommunications.
    - Computer security - security of single computer
    - Cyber security - security of multiple computers

Security terminology

- Threat
    - represents potential security harm to an asset
- Attack
    - threat that’s carried out and if successful leads to violation of security
    - targets integrity, confidentiality and availability of system
- Threat agent
    - carrying out the attack is referred to as an attacker
- Countermeasure
    - any means taken to deal with a security attack (prevention, detection/recovery)
- Residual level of risk to the assets
    - represented by vulnerabilities possibly exploited by attackers

Assets

- Hardware
    - computer systems and other data processing, data storage and data communication devices
- Software
    - operating system, system utilities and applications

- Data (what we'll focus on)
    - files and databases, as well as security related data (password files)
- Communication facilities and networks
    - local and wide area network communication links, bridges, routers, etc.
- Need to protect all layers

Vulnerabilities

A computer system or network can be:

- Leaky
    - gives access to information through network while it shouldn't (confidentiality vulnerability)
    - we want to protect data from unauthorised access
- Corrupted
    - it does the wrong thing or gives wrong answers (integrity vulnerability)
    - when you send message you want to make sure the receiver receives original message, not modified in transit
- Unavailable
    - becomes impossible to use it or impractical (availability vulnerability)
    - server flooded with requests to access webpage but too many requests makes server busy so you can't access it

Passive attacks

- DOES NOT alter information and resources in the system
    - E.g you have a code behind your system to work, then it doesn't modify the code.
- It may be hard to detect but easy to prevent
- Eavesdropping (interception)
    - attacker directly accesses sensitive data traveling between authorised source and destination
- Traffic analysis (inference)

    - attacker gains information from observing the amount of traffic between source and destination

Active attacks

- DOES alter information and resources in the system
- may be hard to prevent but easy to detect and recover
- Masquerade
    - attacker claims to be a different entity
- Modification of messages (falsification)
    - attacker changes messages during transmission
        - don't change source info of message just body
- Distributed denial of service (misappropriation)
    - attacker prevents legitimate users from accessing resources
        - server flooded with fake requests for accessing webpage then normal user can’t access

Inside attacks

- initiated by an entity INSIDE the security perimeter
    - e.g belongs to the UC network with credentials, user and password so you can try attack UC system.
- authorization to access system resources but use of them in a malicious way
- Exposure
    - attacker intentionally releases sensitive information to an outsider
    - project with industry partners, ask you to sign a form to keep results from project secret but you would disclose everything
- Falsification
    - attacker alters or replaces valid data or introduces false data into a file or database
    - teacher has control over our marks so can be a malicious person to try destroy your marks

Outside attacks

- initiated from OUTSIDE the perimeter by an unauthorised or illegitimate user of the system
    - not a user/student of UC
- Obstruction
    - the attacker disables communication links or alters communication control information
- Intrusion
    - the attacker gains unauthorised access to sensitive data by overcoming the access control projections

Security functional requirements

- Information security management needs to:
    1. Identify threats
    2. Classify all threats according to likelihood and severity
    3. Apply security controls based on cost benefit analysis
- Countermeasures to vulnerabilities and threats compromise of:
    1. Computer security technical measures (e.g. access control, authentication, system protection)
    2. Management measures (e.g. awareness and training)
    3. Both (e.g configuration management)

What is information security?