COMP-4670: Security & Privacy

Lyndon Renaud

Lecture 1: Security and Privacy

Computer security is the protection of computer hardware, software, and data. It assesses how assets may be harmed and how to counter or at least mitigate the harm.

Why Security and Privacy?

Security and privacy is necessary for data communication between two or more parties. It allows for the storing and exchange of sensitive information. Applications of security is system security are:

- system security
- secure computation
- system protection

Computer Intrusion Characteristics

Any system is most vulnerable at its weakest point

Principle of Easiest Penetration

- an **intruder** must be expected to use *any available means of penetration*
- the **penetration**:
  - may not necessarily be by *the most obvious means*
  - is not necessarily the one against which *the most solid defense* has been installed
  - does not have to be *the way we want the attacker to behave*

All possible means of penetration must be considered **repeatedly** and whenever the **system and its security change**

Analyze a System from a Security Perspective

Vulnerabilities: *weakness* in a security system
Threats: set of *circumstances* that has the *potential to cause loss or harm*
Attacks: *harm or loss committed* by a person or system who exploit a vulnerability
Controls:

- ways to *address committed, or possible attacks*
- ways to *protect systems*
- could be *actions, devices, procedures, or techniques* that *remove or reduce vulnerabilities*

A **threat** is blocked by **control** and **vulnerability**

Threats

Interception: unauthorized access to an asset by a party
Interruption: an asset of the system becomes lost, unavailable, or unusable
Modification: unauthorized changes to data or systems
Fabrication: insert counterfeit objects to the system

Attack Method, Opportunity, and Motive

A malicious attacker must have:

- **Method**: skills, knowledge, and tools
- **Opportunity**: time and access
- **Motive**: reason to want to perform an attack

Security Triad (3 Goals of Security)

- **Confidentiality**
  - assets are accessed only by authorized parties
  - access means reading, printing, or simply knowing that a particular asset exists
- **Integrity**
  - assets can be modified only by authorized parties or only in authorized ways
  - modification includes writing, changing, changing status, deleting, creating
- **Availability**
  - assets are accessible to authorized parties at appropriate times

Aspects' Issues

Table 1: Aspect Issues

Confidentiality	Integrity
• who determines the access authorization for users? • what is the limit of any access? • what is the user's obligation?	• authorized actions • separation and protection of resources • error detection and correction

Table 2: Aspect Issues cont.

Availability
• timely response to requests • fair resource allocation • fault tolerance • easy use of services • concurrency issues – simultaneous access – deadlock management – exclusive access

Vulnerabilities

- **Hardware vulnerabilities**: adding, changing or removing devices, data traffic interception, physical attacks, theft, DOS attack
- **Software vulnerabilities**: software deletion, modification, theft
- **Data vulnerabilities**: data must be protected only until they lose their value
    - **confidentiality**: prevents unauthorized disclosure of a data item
    - **integrity**: prevents unauthorized modification
    - **availability**: prevents denial of authorized access
- **Networks**: collection of hardware software and data, security issues are multiplied
    - lack of physical proximity
    - use of insecure shared media
    - inability to identify remote users
- **Access**
    - stealing computer time to do general-purpose computing
    - malicious access to computing systems to destroy software or data
    - unauthorized access may deny service to legitimate user
- **Key People**: People can be weak points in security. Trouble can arise if only one person knows how to use or maintain a particular program or system

Methods of Defense

Prevent it: block the attack or close the vulnerability
Deter it: make the attack harder but not impossible
Deflect it: make another target more attractive
Mitigate it: make the attack's impact less sever
Detect it: either has it happens or some time after the fact
Recover it: recover from the effects of an attack

Controls

What are we protecting? How does the cost of protection compare with the risk of loss? How difficult would it be for an intruder?

- **Physical**: using something tangible
    - walls, fences, locks, guards, etc.
- **Procedural** or **Administrative**: using a command or agreement
    - contracts, laws, regulations
- **Technical**: using technology
    - passwords, network protocols, encryption, firewalls
- **Data Encryption**: process of data scrambling
    - cleartext (plaintext)
    - ciphertext (enciphered text)
    - encryption key
    - can address confidentiality, integrity, and availabilty
    - Issues: performance degradation, weak encryption
- **Data Anonymization**
    - sampling, anonymizing, randomizing, supressing

Software Controls

Internal Program Controls: access limitation in a database management program
Operating system and network system controls: limitations enforced by OS or network to protect users from each other
Independent control programs: application programs such as password checkers, intrusion detection utilities, or virus

scanners
Development controls: quality standards to design, code, test, and maintain software programs

Hardware Controls

- hardware or smart card implementations of encryption
- locks or cables for limiting access and deterring theft
- firewalls, intrusion detection systems, etc.

Effectiveness of Controls

- awareness of problem, likelihood to use
- controls must be used and used properly to be effective. They must be **efficient**, **easy to use**, and **appropriate**
- **overlapping controls**: layered defense such as file locking
- **periodic review**: few controls are permantently effective w/o reconsidering and making improvements

Principle of the weakest link:

> Security can be no stronger than its weakest link. Two controls are not always better than one, and could be even worse.