CSC 519 Information Security

LECTURE 1: Introduction

Dr. Esam A. Alwagait
alwagait@ksu.edu.sa

Introduction

- Instructor: Esam A. Alwagait
- Communication by email alwagait@ksu.edu.sa
- Class time: Wednesday 4-7
- Studying material
  - Slide notes
  - Any other references linked to inside the class notes

Grading policy (tentative)

- Midterm exam (30%)
- Final exam (40%)
- Assignments (20%)
- Topic research (10%)

- NOTE: the student will be denied final exam if he exceeds 25% absence rate (university policy)

Plagiarism and academic offenses

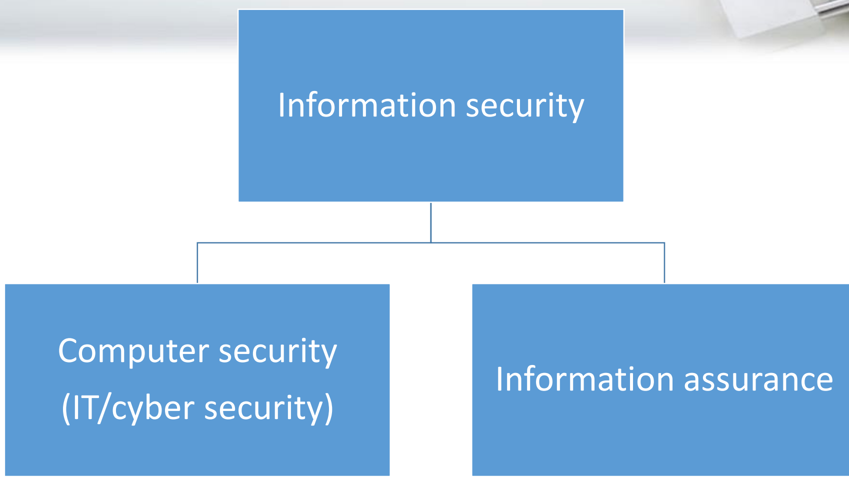
- Applies to both text and code
- Exchanging ideas is encouraged, sharing code or text is prohibited
- Common mistakes
  - Copy code from Internet
  - Sharing assignments

Ethics

- In this course you will learn about some concepts of security vulnerabilities and attacks
- This knowledge is essential for protecting systems!
- You are not to use such information to break into (or even test!) systems without the explicit consent of the owner
- So, it must be used in an ethical manner

Course goals

- Identify security and privacy issues in/related to
  - Programs and applications
  - OSs
  - Networks
  - DBs
  - Processes
  - People!
- Learn how to evaluate security posture of a system
- Learn how to design and build more protective systems



Module1:
What is a computing system

- A collection of
  - Hardware
  - Software
  - Storage media
  - Data, and
  - People

  that an organization uses to perform computing tasks
- A computer-based system has three separate but valuable components
  - HW,
  - SW, and
  - data

CSC 519 Information Security

What is information security?

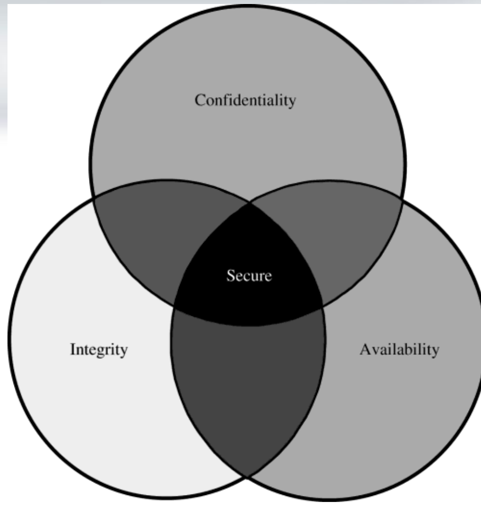
- The practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction [Title 44 US Code 3542 Definitions]
- Information security is defined as the preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved [ISO/IEC 17799:2005]
- Information system security is a system characteristic and a set of mechanisms that span the system both logically and physically. The five security goals are integrity, availability, confidentiality, accountability, and assurance [NIST 800-30]
- It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)

What does “secure” mean?

- Confidentiality
  - ensures that computer-related assets are accessed only by authorized parties
- Integrity
  - assets can be modified only by authorized parties or only in authorized ways
- Availability
  - assets are accessible to authorized parties at appropriate times
- Extended properties/qualities
  - Accountability
    - The requirement that actions of an entity may be traced uniquely to that entity
  - non-repudiation
    - A service that provides proof of the integrity and origin of data
  - Authenticity
    - ensure that the data, transactions, communications or documents (electronic or physical) are genuine

[NIST Special Publication 800-33, at 3; ISO/IEC 7498-2]

Secure computing systems have all these three properties



Relationship Between Confidentiality, Integrity, and Availability.

What is privacy?

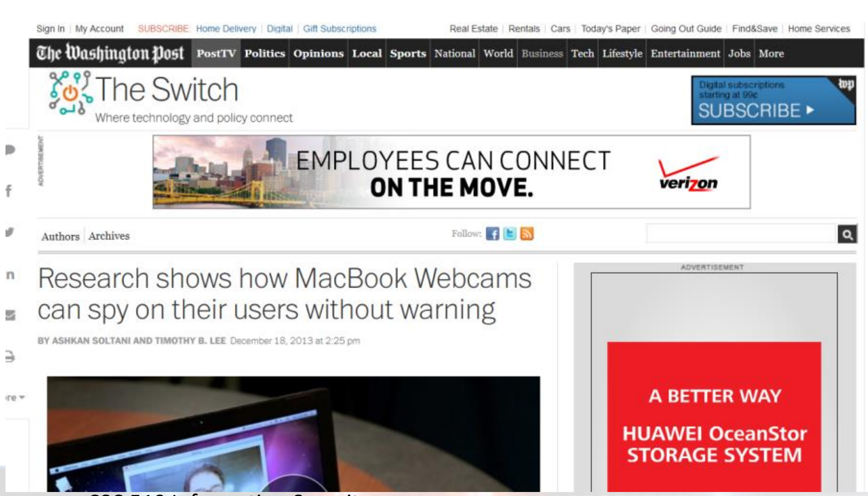
- A simple definition
  - informational self-determination
- This means that you get to control information about you
- Control what?
  - Who gets to see it
  - Who gets to use it
  - What they can use it for
  - Who they can give it to
  - etc.

Security vs. Privacy

- Are they opposing forces to each other?
- Security is about the practices and processes that are in place to ensure data isn't being used or accessed by unauthorized individuals or parties
  - basically protection!
- Privacy is about the appropriate use of data
  - Governance and use!
  - Viewed very differently in different cultures!
- Security is necessary but not sufficient for addressing privacy
  - Example?
    - an online advertising company that has near perfect security but shares the information it tracks about consumers with third parties without consent!

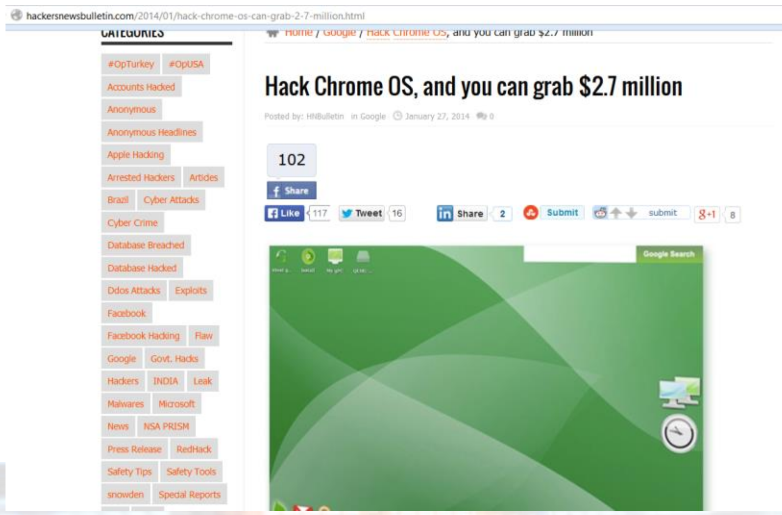
Few stories...

- Where is the problem?
  - Program
  - Physical
  - DB
  - Networks
  - OS
  - administrative
  - Social eng.
  - Privacy
  - economics



Few stories...

- Where is the problem?
  - Program
  - Physical
  - DB
  - Networks
  - OS
  - administrative
  - Social eng.
  - Privacy
  - economics

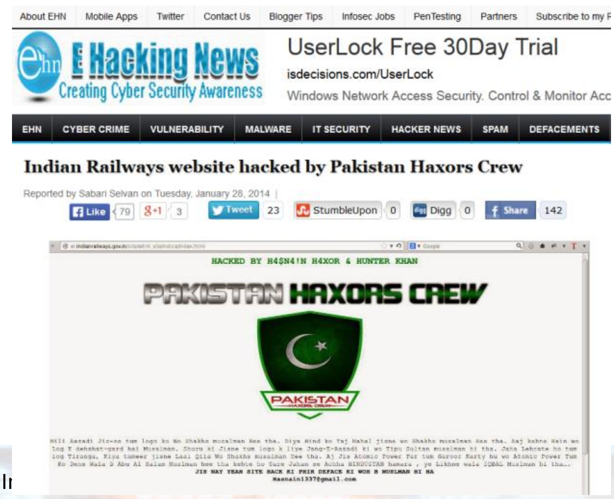


Few stories...

- Where is the problem?
  - Program
  - Physical
  - DB
  - Networks
  - OS
  - administrative
  - Social eng.
  - Privacy
  - economics

Few stories…

- Where is the problem?
  - Program
  - Physical
  - DB
  - Networks
  - OS
  - administrative
  - Social eng.
  - Privacy
  - economics



CSC 519 I

Other issues?

- Where is the problem?
  - Program
  - Physical
  - DB
  - Networks
  - OS
  - administrative
  - Social eng.
  - Privacy
  - Economics
- How about
  - Scale?
  - Target?
  - Adversaries?
  - Incentives?
  - Tools?

CSC 519 Information Security

Websites Hacked!

JUNIPER NETWORKS

Adobe

monster
Your calling is calling

F-SECURE

Google

symantec.

Microsoft

YAHOO!

KASPERSKY ANTI-VIRUS

CSC 519 Information Security

Saudi websites Hacked!

الوطن
al-watan

KING FAISAL UNIVERSITY

المملكة العربية السعودية
القناة الأولى

بنك الرياض
riyad bank

samba سامبا

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

صحاري نت
Sahara Net

العربية

Al Rajhi Bank مصرف الراجحي

الإخبارية

وزارة التعليم العالي
Ministry of Higher Education

اول نت
AwalNet

وزارة العدل

المملكة العربية السعودية
مرور منطقة الرياض

الاتصالات المتكاملة
INTEGRATED TELECOM
Your way to the future

إمارة المنطقة الشرقية

ARREYADI
الرياضي

SACM

samc
الجمعية السعودية للإعلام والإتصال

MAS ماس

مركز المعلومات والأبحاث السياحية

Who are the adversaries?

- Computer criminals
  - Amateurs
  - Script kiddies
  - Hackers
  - Crackers
  - Organized crime and professional criminals
  - Cyber warriors
  - …
- Remember!
  - One approach to prevention or moderation is to understand who commits these crimes and why

Key security principles

- For attacker?
  - Principle of Easiest Penetration
  - “A system is only as strong as its weakest link”
  - The attacker will always look for the easiest entrance!
- For defender?
  - Principle of Adequate Protection
  - “Security is economics”
  - Don’t spend SR100,000 to protect a system that only cause SR1000 in damage!

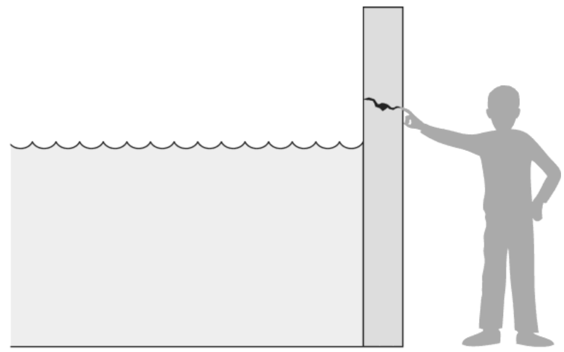
- To build secure systems, we need to think like attackers!

Terminology

- **Assets** are things we want to protect, such as
  - HW
  - SW
  - Data
- A **vulnerability** is a weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm
  - A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access

Terminology

- **A threat** to a computing system is a set of circumstances that has the potential to cause loss or harm
  - Revealing users' personal files to the public
- **Attack** is an action which exploits a vulnerability
  - Compromising file server's authentication in an attempt to access/modify users' data
- **Control** is an action, device, procedure, or technique that removes or reduces a vulnerability
- **Relationship**
  - A threat is blocked by control of a vulnerability to prevent an attack



Pfleeger/Pfleeger Fig. 01-01

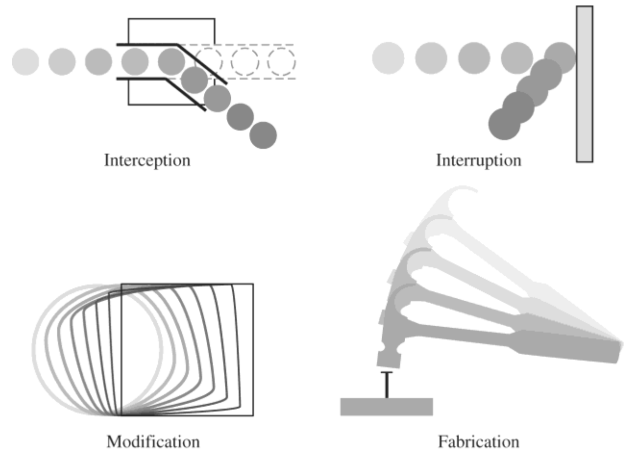
Threats, Controls, and Vulnerabilities.

Method, Opportunity, and Motive

- A malicious attacker must have three things:
  - *Method*
    - the skills, knowledge, tools, and other things with which to be able to pull off the attack
  - *Opportunity*
    - the time and access to accomplish the attack
  - *Motive*
    - a reason to want to perform this attack against this system

Terminology

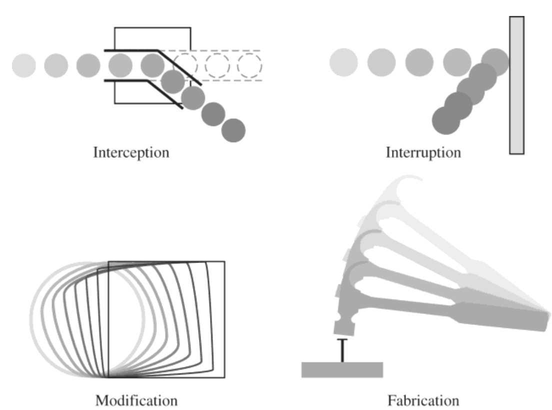
- Are all **threats** of the same type?
- An **interception** means that some unauthorized party has gained access to an asset.
  - The outside party can be a person, a program, or a computing system.
  - Examples of this type of failure are illegal copying of program or data files, or wiretapping to obtain data in a network



Pfleeger/Pfleeger Fig. 01-02

Terminology

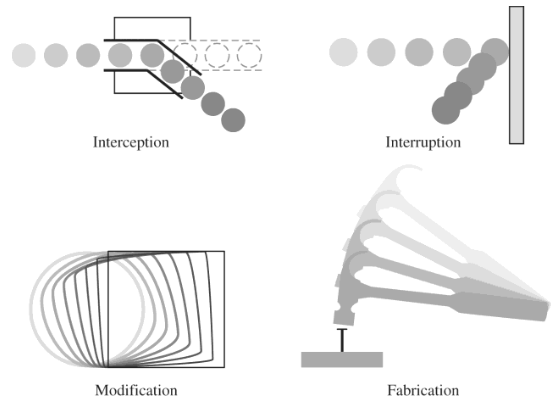
- Are all threats of the same type?
- In an **interruption**, an asset of the system becomes lost, unavailable, or unusable.
  - An example is malicious destruction of a hardware device, erasure of a program or data file,
  - Malfunction of an operating system file manager so that it cannot find a particular disk file



Pfleeger/Pfleeger Fig. 01-02

Terminology

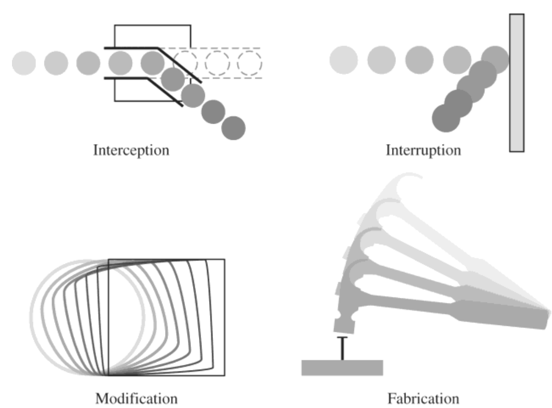
- Are all threats of the same type?
- If an unauthorized party not only accesses but tampers with an asset, the threat is a **modification**.
  - For example, someone might change the values in a database, alter a program so that it performs an additional computation,
  - modify data being transmitted electronically



Pfleeger/Pfleeger Fig. 01-02

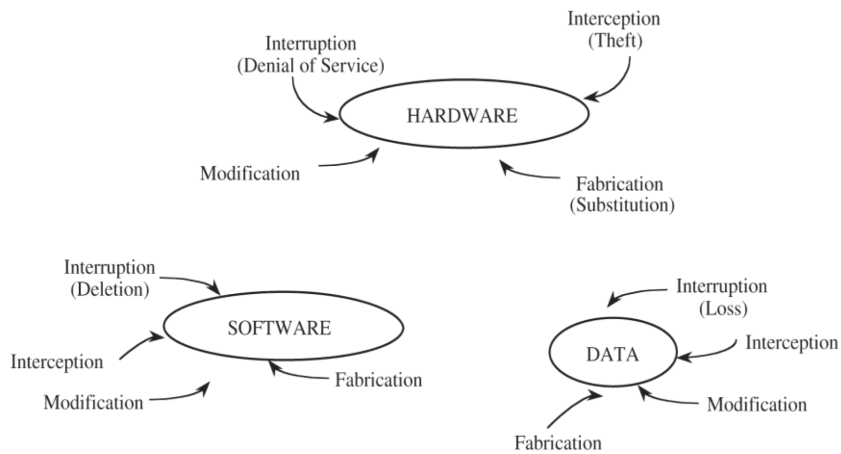
Terminology

- Are all threats of the same type?
- an unauthorized party might create a **fabrication** of counterfeit objects on a computing system.
  - The intruder may insert spurious transactions to a network communication system or add records to an existing database.
  - Sometimes these additions can be detected as forgeries, but if skillfully done, they are virtually indistinguishable from the real thing



Pfleeger/Pfleeger Fig. 01-02

- When designing a system, we need to specify the threat model:
  - **Set** of threats we are defending
  - **Whom** do we want to stop from doing **what**?



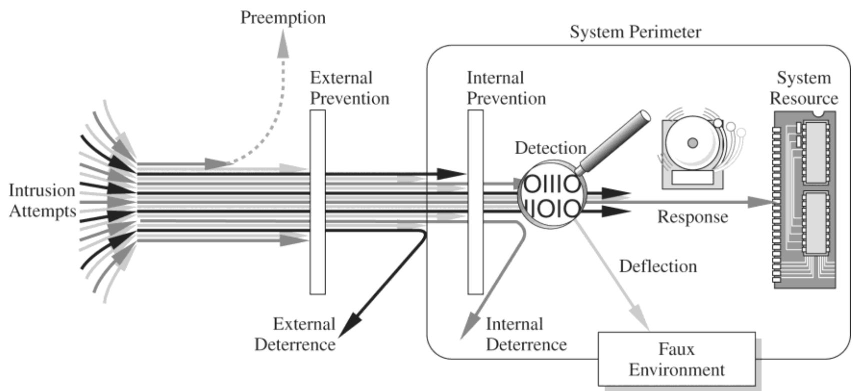
Vulnerabilities of Computing Systems

Methods of defense against threats

- ***prevent*** it, by blocking the attack or closing the vulnerability
- ***deter*** it, by making the attack harder but not impossible
- ***deflect*** it, by making another target more attractive (or this one less so)
- ***detect*** it, either as it happens or some time after the fact
- ***recover*** from its effects (mitigate the effects of the attack)

Multiple controls?

- ***Defense in depth:***
- *Often, we deploy many controls to defend against the same threat*



Pfleeger/Pfleeger Fig. 01-06

Examples of defense

- Threat: your house may get broken in
- How to defend it?
  - Prevent it: can you absolutely prevent it?
  - Deter it: use proper keys, proper doors
  - Deflect it: put a sign that you have an alarm!
  - Detect it: use alarm/CCTV systems
  - Recover: insurance

Examples of computer defense

- Cryptography
  - Protecting data by making it unreadable to an attacker
  - Authenticating users with digital signatures
  - Authenticating transactions with cryptographic protocols
  - Ensuring the integrity of data at rest and communication

Examples of computer defense

- Software controls
  - Passwords
  - Operating systems separate users' data and actions from each other
  - Antivirus tools
  - Structured development tools and methodology to enforce quality of source code
  - Software firewalls

Examples of computer defense

- Hardware controls
  - Fingerprint readers
  - Smart tokens/cards
  - Circuit boards that control access to storage media
  - Firewalls
  - Intrusion detection/prevention systems
  - Threat prevention systems

Examples of computer defense

- Physical controls
  - Protection of physical access and hardware itself:
  - Locks
  - Guards
  - Doors

Examples of computer defense

- Policies and procedures (non-technical means of protection):
  - Not allowing users to install wireless access points
  - Password rules
  - Employee recruitment procedures

Recap

- What is the goal of this course?
- What is security?
- What is privacy?
- Key security principles
- Who are the adversaries?
- What do we mean by assets, vulnerabilities, threats, attacks, controls
- Types of threats
- Methods of defense