Review of Security Foundations

- What is information security about?
  - Details on slides 2-3
- What are some terms that describe our concerns?
  - Details on slide 4
- What are the goals and key concepts of information security?
  - Details on slides 5-10
- Can we solve information security issues through better technology?
  - Details on slide 11

What is Information Security about?

- Society is increasingly more reliant on computers
- Placing trust on computer applications is a necessity
- But are all computer systems trustworthy?

- Trust is placing your confidence in something
- Trustworthiness is placing confidence correctly
  - Trust is belief that a system will operate in an expected manner with attacks causing minimal damage to system and users
  - Trustworthy systems **do** operate in an expected manner and resist damage from attacks

What is Information Security about?

(cont'd)

- Information security studies ways to make systems trustworthy
  - By assuring a computer system will behave reasonably even in the face of malicious attacks
- NIST Cybersecurity Framework
  - Lists five functions of information security
    1. Identify (system vulnerabilities)
    2. Protect (the system from attacks)
    3. Detect (attacks on the system if they occur)
    4. Respond (to attacks in a reasonable way)
    5. Recover (from attacks to cause minimal damage)
  - Each function contains outcomes and describes use of standards, guidelines and practices

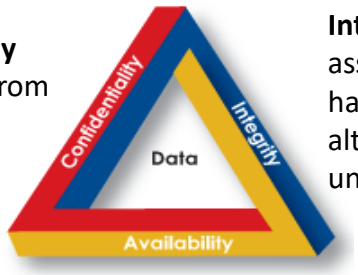
NIST Function #1: What to Identify?

- **Vulnerabilities**
  - Weaknesses in system that expose it to an attack
    - e.g. using non validated external data allows SQL injection attacks
- **Threats** or **attackers**
  - Adversaries who may exploit vulnerabilities
    - Includes unintentional blunders, hackers, disgruntled employees, organized crime, market competitors, foreign nations
    - Potential threats vary based on given system.
      - e.g., student record system is unlikely to be targeted by a foreign nation or organized crime
- ***Risk***
  - The expected damage from a security violation.
    - Includes likelihood of a vulnerability being exploited and cost of damage
      - e.g. web service may have vulnerability, but if it's not connected to network, risk is zero
- ***Attack vectors***
  - Describes how attacker could carry out an attack
    - e.g., malicious email attachment, SQL code injection, tricking human operator

Goals of Security

- C.I.A = Confidentiality, Integrity, Availability

Confidentiality
protect data from unauthorized disclosure



Integrity
assurance that data has not been altered in an unauthorized way

Availability
assurance that the data/service is accessible to those with access to it

Breaches of C.I.A

- Confidentiality Breach
  - Sensitive information reaches unauthorized persons
    - A student finds a file with test scores of all students in a class
    - A student's private discussions with counselor is revealed to an instructor
    - A student's records are released without obtaining student's permission
- Integrity Breach
  - Data is fraudulent or altered without authority
    - An email that looks like it is from your bank but in fact is a phishing attack
    - A request to transfer $100 from account is changed by attacker to $10,000
- Breaches of availability
  - Losing access to services
    - Not being able to access a web site if it is under a denial of service attack
    - A malicious attacker changes passwords of valid users, preventing them from accessing the service/site

Balancing C.I.A

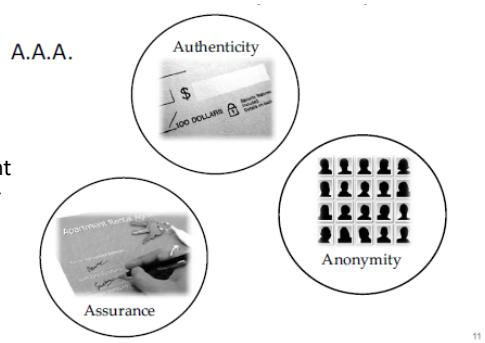
- C.I.A goals are at odds with one another and must be balanced
  - Increasing availability usually decreases confidentiality and integrity
- Example 1
  - Lockout a user's account after several failed password attempts
    - Policy compromises availability for confidentiality and data integrity
      - Suitable for some settings (e.g., email, bank accounts)
      - Not for others (e.g., medical records, military systems)
- Example 2
  - Allow users to do queries over a population (e.g. find average salary of Le Moyne Employees)
    - For integrity query results should be accurate
    - But queries over a small population can reveal salary of one person
      - Note: gender, date of birth, and zip code (i.e., well known attributes for an individual) together uniquely identify 99% of the people in Cambridge, Massachusetts

Perfect Security

- Since C.I.A goals are often at odds it is ***impossible*** to design systems with perfect security
- Our goal is to minimize risk and to be aware (as much as is possible) of the risks that remain

A.A.A – Security Concepts for trust

Authenticity
ability to determine that statements, policies, and permissions are genuine
- e.g. ATM card and a pin authenticates that you have right to make a withdrawal from your account



Assurance
how trust is managed
- Policies (i.e., behavioral expectations)
- Permissions (i.e., behaviors allowed by agents)
- Protections (i.e., mechanisms to enforce policies and permissions)

Anonymity
not possible to attribute certain records or transactions to any individual

How to Authenticate?

- Authenticate
  - Determine if statements, policies, and permissions are genuine
  - Authentication can be done based on
    - Something you know
      - e.g., PIN, a password, or mother's maiden name
    - Something you have
      - e.g., a driver's license, magnetic swipe card, car keys
    - Something you are
      - e.g., biometrics, e.g. fingerprints, retina scans, etc.

Cybersecurity is an Inter-disciplinary

- Information security requires more than just technical solutions
  - e.g., can technology alone solve social engineering attacks?
    - Spoofing someone's email address (phishing attacks)
    - Spoofing a bank's web-site
- Cybersecurity programs must also address
  - Policy choices
    - How quickly do we respond to a known vulnerability?
    - What data do we persistently store? Why? How? Duration?
    - How do we support attribution?
  - Ethical issues
    - Who should be notified of a data breach? How quickly?