Introduction to Information Security Principles

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?
  - i.e., Do all computer systems deserve our trust?
- 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
  - Describes five functions of information security

1.	Identify	(system vulnerabilities, risks)
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: 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 grades are 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

What is Information Security about?

(cont'd)

- Information security is a process
  - It is never done! Always trying to improve
- How does this relate to the NIST Cybersecurity Framework?
  - Some examples …
    - Identify a vulnerability, adjust system to protect it
    - Detect an attack, respond and recover
    - Detect an attack, identify attack vector, adjust system to protect it

5

Cybersecurity is Inter-disciplinary

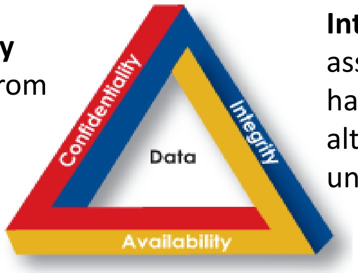
- Information security requires more than just technical knowledge and solutions
  - E.g., Can technology alone solve social engineering attacks?
    - Spoofing someone's email address (phishing attacks)
    - spoofing a bank's web-site
- How does this relate to the NIST Cybersecurity Framework?
  - Some examples
    - Identify a risk, change a company policy (e.g., long-term retention of data)
    - Detect an attack
      - What is company's ethical responsibility for contacting affected individuals?
      - What is company's legal responsibility for notifying the public?
      - What is the economic impact to the company's suppliers/partners?
    - Detect an email phishing attack, modify education strategy of employees

6

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

- Integrity Breach

  Data is fraudulent or altered without authority

- Breaches of availability

  Losing access to services

Which security goal is violated?

1. A student’s private discussions with counselor is revealed to a teacher. C
2. A malicious attacker changes the passwords of valid users, preventing them from accessing the site. A
3. A request to transfer $100 from account is changed by attacker to $10,000. I
4. An email that looks like it is from your bank but in fact is a phishing attack I
5. A student’s records are released without obtaining student’s permission. C
6. Not being able to access a web site if it is under a denial of service attack A

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.**
  - Good for confidentiality and data integrity, bad for availability
  - Is this a good security policy?
    - Yes for some settings (e.g., email)
    - No for others (e.g., medical records systems)

Balancing C.I.A

(cont'd)

- **C.I.A goals are at odds with one another and must be balanced**
  - Increasing availability usually decreases confidentiality and integrity
- **Example 2: Allow users to do queries over a population (e.g. find the average salary of Le Moyne Employees)**
  - Good for availability and integrity, bad for confidentiality
  - Queries over a small population can reveal good estimates of salary of one person

Group Discussion

(Balancing CIA)

- How are security goals C.I.A being traded off below?
  - Students are only informed of the average grade of a homework assignment only if more than 10 students submitted it.

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*

GRANTLAND®
2506
BUT HOW CAN YOU BE SURE NO ONE ELSE CAN ACCESS MY COMPUTER FILES?
BECAUSE I ERASED THEM AND RE-FORMATTED YOUR HARD DRIVE.
YOU IDIOT! NOW I CAN'T GET INTO THEM EITHER!
EVERYTHING'S A TRADEOFF, MIKE, EVERYTHING'S A TRADEOFF.
COPYRIGHT GRANTLAND May not be reproduced.

Security Concepts that Support Trust (A.A.A.Nr)

- 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)
- Authenticity
  - Ability to determine that statements, policies, and permissions are genuine
    - e.g. ATM card and pin authenticates that you have right to make a withdrawal from your account
- Anonymity
  - Not possible to attribute certain records or transactions to any individual
- Non-repudiation
  - Someone cannot deny something
    - i.e., a user should be responsible for their actions and should not be able to deny what they have done

How to Authenticate?

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

Breaches in A.A.A.Nr

- In each scenario describe which concept authentication, assurance and anonymity is breached .
  1. An individual under 21 uses a fake ID to get into a bar and buy alcohol.
  2. A wait staff takes a customer's order. When the order is ready, the customer's name is called and they must walk over to the bar to pick up their order.
  3. An individual under 21 goes into a bar and is asked to wear a green band to indicate that they are not allowed to purchase alcohol. The bar is crowded and the bartender misses the green band and allows the individual to purchase alcohol.

Class Discussions

(Cybersecurity is inter-disciplinary)

- You work at a software company and discover a new vulnerability in an application that is already deployed. Should this be disclosed?
  – What are some ethical reasons to disclose?
  – What are some ethical reasons not to disclose?
- San Bernardino case: FBI had iPhone of suspected shooter
  – FBI could not access data on device (it's data was encrypted)
  – Apple did not want to help FBI (by disabling its password policy)
    - i.e., after 10 unsuccessful password attempts the device is locked
  – What arguments are in favor of the FBI?
  – What arguments are in favor of Apple's position?