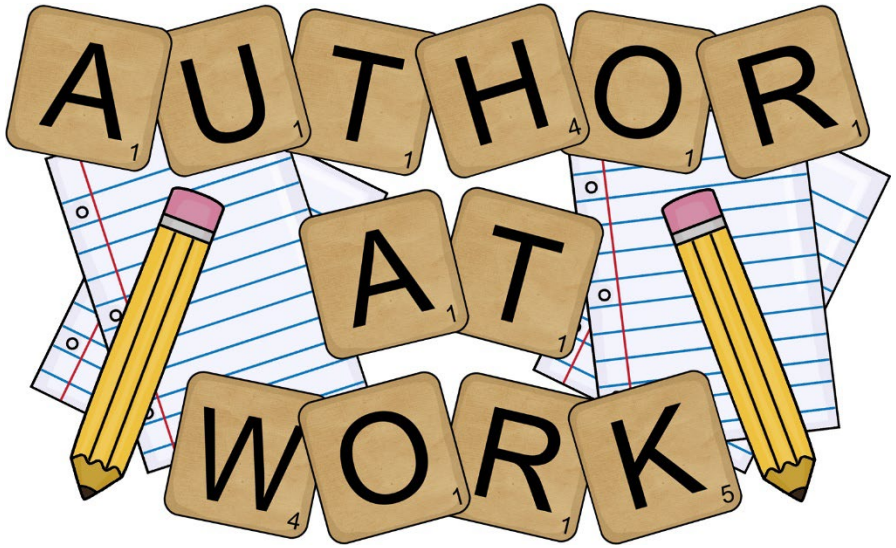
01-Introduction to Security

Acknowledgement

The slides & lab handouts used in this course contain information and ideas of exercises that were adapted/compiled from several resources.

Major resources used:

- The course textbook (CompTia Security+ Guide to Network Security Fundamentals by Mark Ciampa).
- Material used in similar previous course offerings created by Nalin Wijesinghe, Abdullatif Shikfa, Robert Ford, and others.
- Security courses by Cisco Networking Academy. https://www.netacad.com/courses/cybersecurity

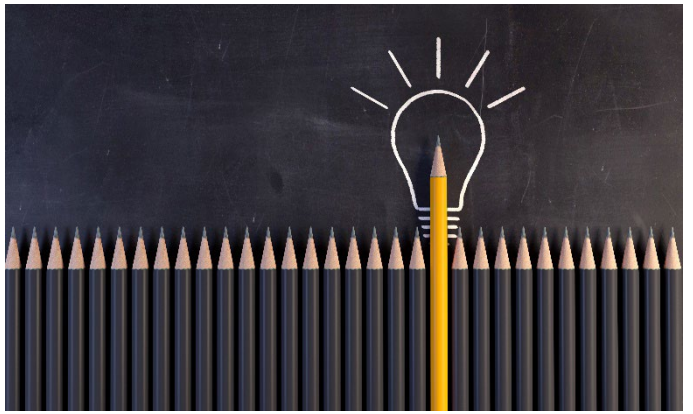


Lecture Attendance

- Lecture attendance is recorded by the card reader at the theater's door.
- You must tap your card for your attendance to be recorded.
  - You only need to tap your card at the beginning of the lecture, there is no need to tap it again when you leave.
  - Do not tap your card too early, any record before 5 minutes of the lecture start will not be taken into consideration.
  - If you are more than 10 minutes late, you will be recorded absent.
- Attendance is now managed by the centralized attendance office, do not email the instructor to apologize for not attending or asking to be excused.
- The only case you must contact your instructor is if you miss an assessment (face to face, not by email).
  - Note that your recoded absence won't be changed, but you will be informed on how your grade will be accommodated if such accommodation is possible.

Learning Objectives

- Define information security.
- Realize the key objectives of security.
- Explain what is meant by the CIA triad (confidentiality, integrity, and availability).
- Identify the states of data.
- Describe cybersecurity countermeasures.
- Explain security trade-offs.



World of Computers

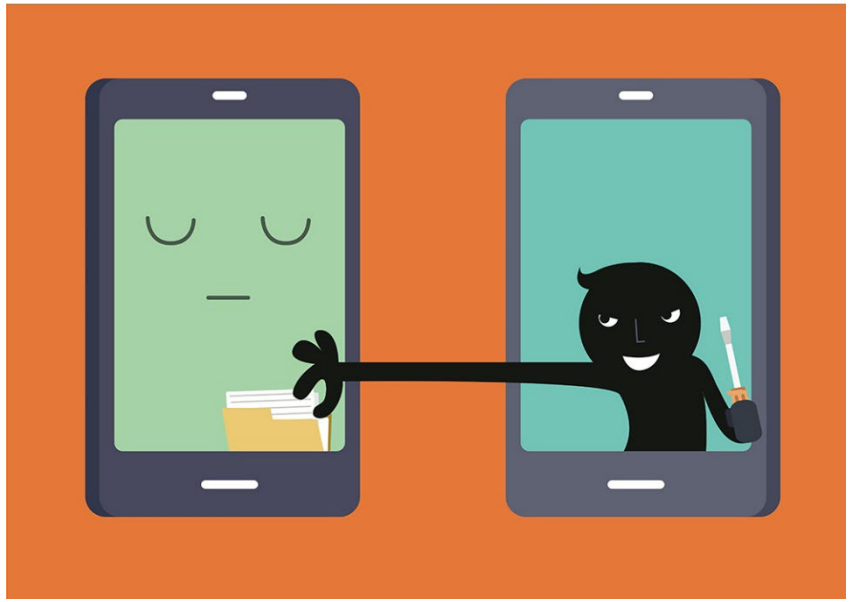
Computers today are ubiquitous. We depend on them to perform several tasks in our daily life such as:

- Study and education.
- Online shopping.
- Online Banking.
- Play games.
- Communicate with others (emails, chat, video conferences).
- Monitor and operate IoT devices in smart homes.
- etc.

Discussion

What are the threats associated with a malicious actor accessing the following sources of information?

- Laptop of a student taking courses in UDST.
- Personal accounts on social media.
- Personal identification data like social security numbers, Qatar IDs, date of birth, or home address.
- Computers and educational records in an educational institute.
- Servers in a data center such as Amazon or Google.
- Medical records in a health care organization.
- Employment information or records in an organization.
- Financial information or records.



Technology and Security

Convenient usage of technology poses major security risks:

- Your money could be transferred/stolen if attackers could access your bank account.
- You may face troubles if attackers could access your private information (e.g., personal photos, private emails/chats).
- A company/institute could suffer damage to its reputation and lose millions of dollars if its database containing proprietary information was breached.
- Large scale damages could also be caused, for example:
  - Power off the electricity grid.
  - Cancel flights/ground the planes of an airline company, etc.

Defining Security

The goal of security is to be free from danger (whether from natural disasters, attackers invading your networks, vandalism, loss, or misuse).

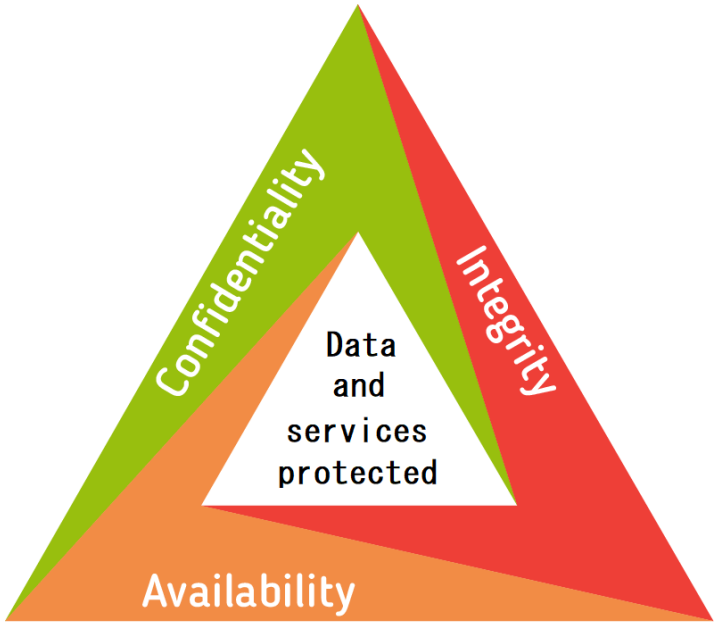
This goal is almost impossible to be fully achieved, but measures (steps) can be taken to protect our digital assets.

Information security is a term that describes the tasks of securing digital information, whether it is:

- Manipulated by a microprocessor (such as on a personal computer).
- Preserved on a storage device (such as a hard drive or USB flash drive).
- Transmitted over a network (such as a local area network or the Internet).

The CIA Triad

- Information security is intended to protect information that provides value to people and enterprises.
- There are three types of information protection (often called the CIA Triad):
  - Confidentiality
  - Integrity
  - Availability
- If one of the above principles is breached in an information system, the system becomes unsecure.
- The three principles provide focus and enable cybersecurity specialists to prioritize actions in protecting the cyber world.



Confidentiality

- Confidentiality refers to protecting the data from those who are not authorized to view it. In other words, keeping data secret.
- Your bank card PIN and your password to log in to your D2L account are considered confidential data and no one should know them.
- Organizations collect a large amount of data and much of this data is not sensitive, like names and telephone numbers.
- Other data collected, though, should be kept secret:
  - Data protected from unauthorized access to safeguard an individual or an organization (e.g., credit card number). It should never be disclosed.

Confidentiality

- Confidentiality can be compromised in several ways:
  - You may lose your laptop which contains sensitive data (files), and somebody finds it.
  - A person could look over your shoulder while you are entering a password.
  - An attacker could penetrate the system of an organization and access its database.
- Methods used to ensure confidentiality include data encryption, authentication, and access control.

Integrity

- Integrity, also called quality, is the accuracy, consistency, and trustworthiness of data during its entire life cycle.
- It refers to the ability to prevent people from altering your data in an unauthorized or undesirable manner.
  - Imagine you request your bank to send 100 QAR to your mother, but an attacker modifies the request so that it becomes 10000 QAR to his own account.
- To maintain integrity, you must prevent unauthorized access and have the ability to reverse unwanted changes.
  - Operating systems assign different permissions (read, write, execute) to each file to prevent unauthorized changes.
  - Other systems and applications provide the ability to roll back or revert to an earlier version.

Availability

- Availability refers to the ability to access data whenever needed.
- Availability could be lost due to:
  - Power failure.
  - Malfunction of an operating system, application, or the network.
  - Denial of service attack (DOS) on a system; an attacker sends a larger number of fake requests to slow or shut down a server preventing it from responding to other legit requests.
- Methods used to ensure availability include:
  - System redundancy.
  - System backups.
  - Equipment maintenance.
  - Plans in place to recover quickly from unforeseen disasters.

Question

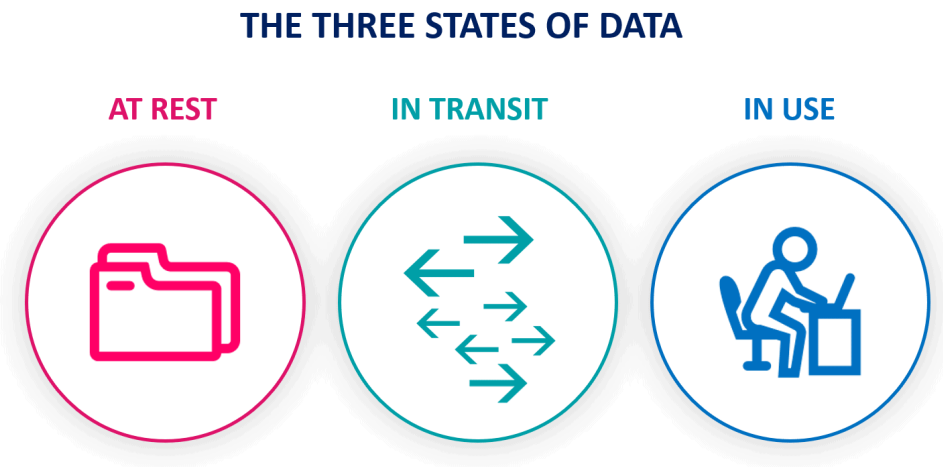
- A student loses her smart phone which contains her pictures without hijab. Since the phone is not protected with a screen lock, the person who finds the phone checks the pictures on the phone and recognizes the owner before returning the phone to her. What pillar of the CIA triad was breached?
  - Confidentiality.
  - Integrity.
  - Availability.
  - Picture viewing.

Question

- A student loses her USB drive which contains a set of files that are all password protected. What can be said about such incident?
  - The confidentiality was compromised since the student is not confident that she can find the USB.
  - The integrity was compromised since the student must create new files but cannot remember the exact content.
  - The availability was compromised since the student doesn't have access to the files anymore.
  - The convenience was compromised since the student must make a trip to buy a new USB drive.
  - The useability was compromised since the USB drive is not useable anymore.

Sates of Data

- Data has three possible states:
  - Data at rest or in storage.
  - Data in transit or in motion.
  - Data in process.
- Data must be protected in all states.

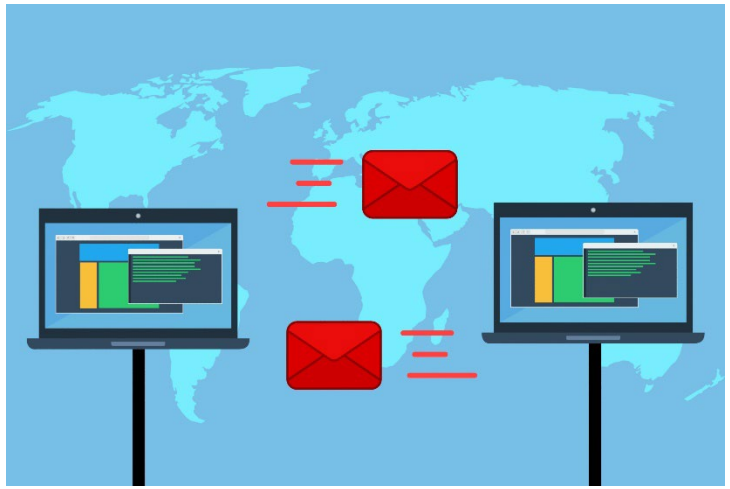


Data at Rest

- Data at rest means that a type of storage device retains the data when no user or process is using it.
- Direct-attached storage (DAS) is storage connected to a computer. A hard drive or USB flash drive is an example of direct-attached storage.
- Storage could also be centralized on the network using technologies such as:
  - Redundant array of independent disks (RAID).
  - A network attached storage (NAS).
  - A storage area network (SAN).

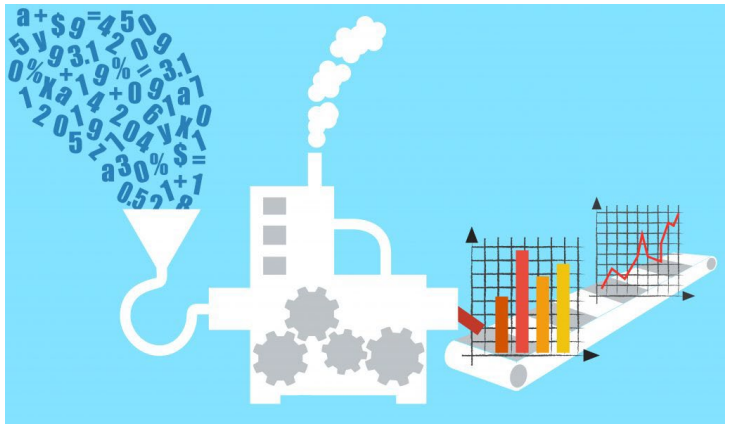
Data in Transit

- Data in transit refers to data being sent from one device to another, mostly over a wired or a wireless network.
- Data in transit could be:
  - Data collected and submitted via a web form.
  - A file, email, or a text message.
  - Data collected from sensors and sent for processing.



Data in Process

- Data in process refers to data being currently used and processed by a user or a process.
- Data in use could be:
  - A file being edited by a user.
  - Information collected from a user and currently processed by a web server.

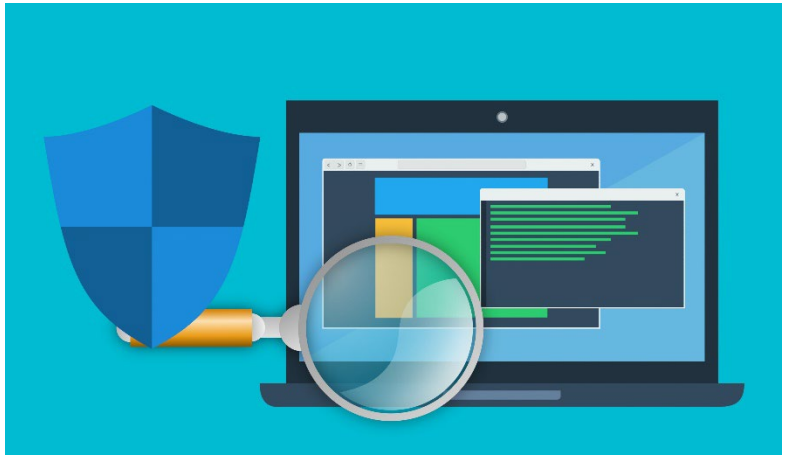


Cybersecurity Countermeasures

- Cybersecurity countermeasures define the types of actions used to protect the cyber world.
- There are several countermeasures that can be used to provide security, categorized in:
  - Security products and technologies.
  - Policies and procedures.
  - Human training and education.

Technologies

- Technologies used to counteract security threats could be:
  - Software technologies such as antivirus, antimalware.
  - Hardware technologies such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS).
  - Network technologies such as virtual private networking (VPN), Network access control (NAC), Wireless access point security.
  - Cloud based technologies.



Policies and Procedures

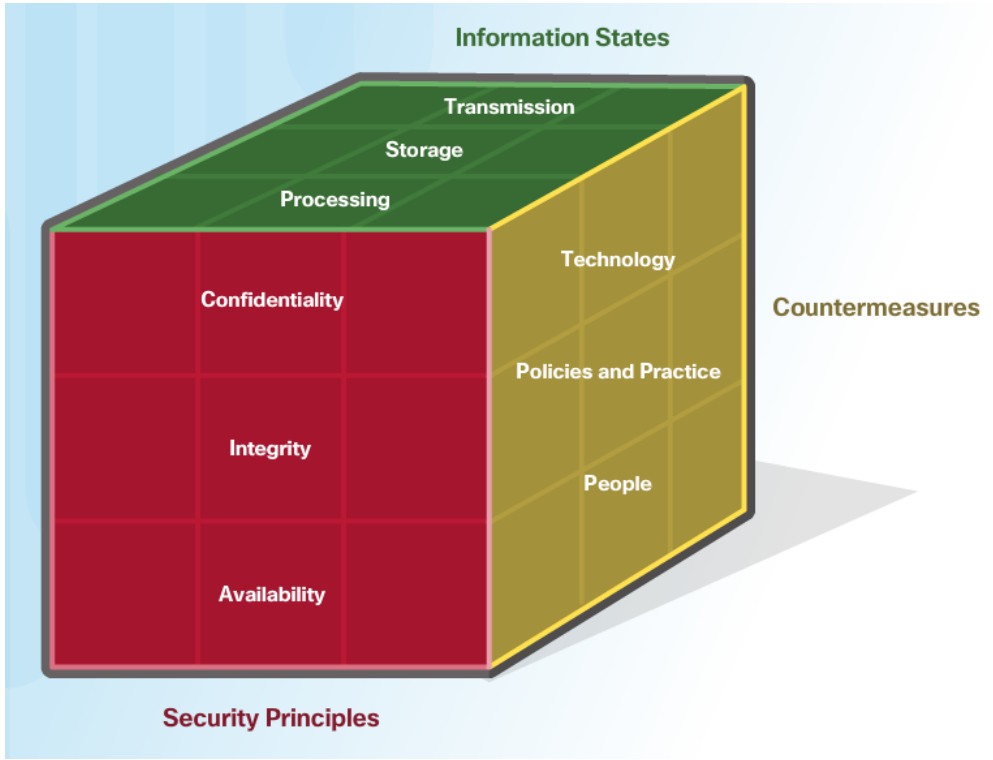
- A security policy is a set of security objectives that includes rules of behavior for users and processes.
- Standards help an IT staff maintain consistency in operating the network.
- Guidelines are a list of suggestions on how to do things more efficiently and securely.
- Procedure documents include implementation details that usually contain step-by-step instructions and graphics (e.g., operation and configuration manuals).

Human Training and Education

- Humans play a very important role in securing systems.
- An employee/user may not be purposefully malicious but just unaware of what the proper procedures are.
- There are several ways to implement a formal training program:
  - Make security awareness training a part of the employee's onboarding process.
  - Tie security awareness to job requirements or performance evaluations.
  - Conduct in-person training sessions.
  - Complete online courses.
- Security awareness should be an ongoing process since new threats and techniques are always on the horizon.

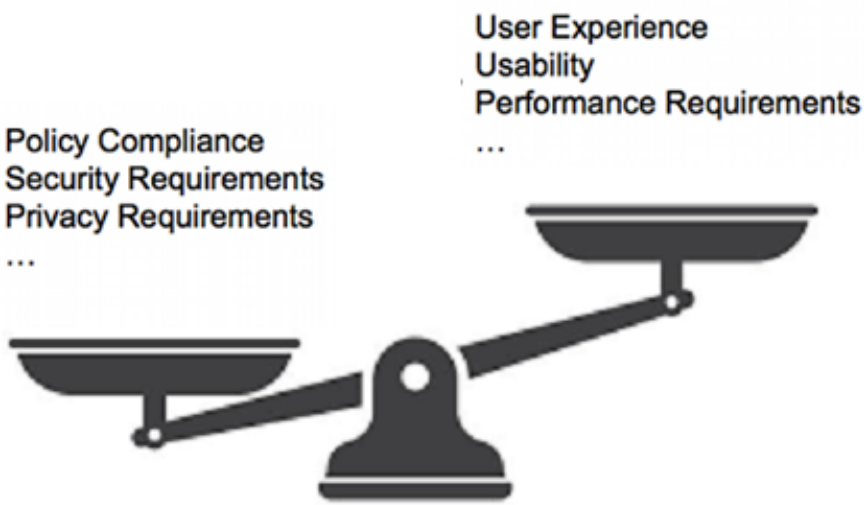
The Cybersecurity Cube

- Protection is achieved through a process that combines three entities:
  - The CIA triad.
  - The states of data.
  - Security countermeasures.
- The cybersecurity cube ties all aspects of security together.
- Thus, information security is ensuring the confidentiality, integrity, and availability of information by using countermeasures to protect data in all its states.



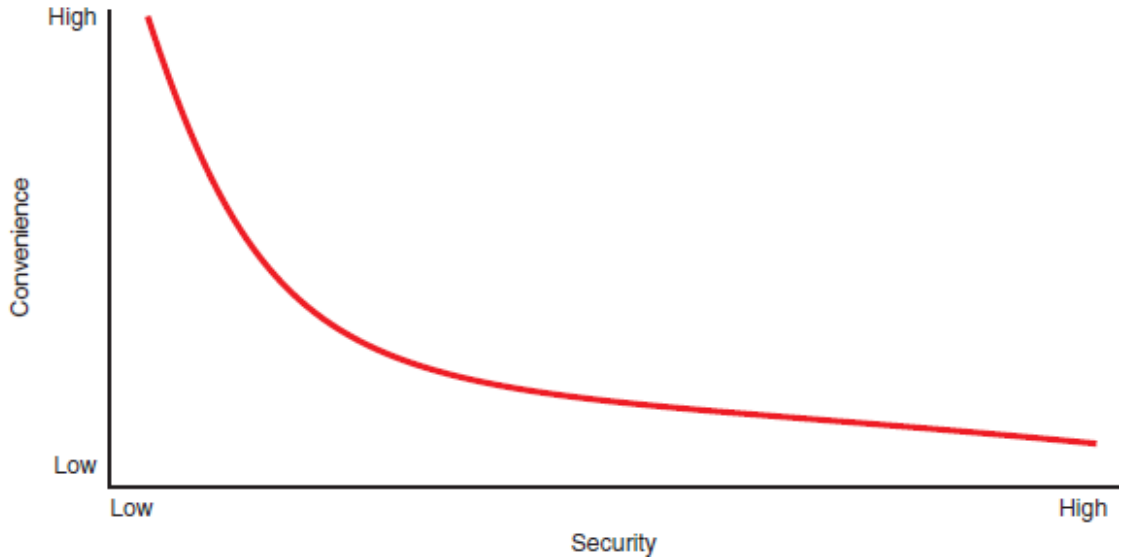
Security Tradeoffs

- Security is never 100% perfect,
  - the only secure system is one that's isolated and shut down
  - but such a system is neither usable, nor productive.
- Security is always a trade-off between competing interests:
  - especially security vs. convenience, usability, and performance,
  - and don't forget the cost.
- Often, security needs to be good enough under limited conditions
  - if the cost of security is significantly higher than the resulting harm, it is more cost-effective to just fix any resulting damage.



Security Tradeoffs

- Examples
  - A computer without a password is usable, but not very secure.
  - A computer that logs the user off every minute and requires a sixty-character long password, finger swipe, and face scan to log back in is more secure, but inconvenient to use and lowers productivity.
  - Would you build a castle and hire armed guards to save your mom's cake recipe?



The End

End of Slide Set