CPSC 467: Cryptography and Security

Michael J. Fischer

Lecture 2
September 3, 2020

Slide credits: Mariana Raykova, Tom Ristenpart, Stefano Tessaro, as well as the teaching slides for *Introduction to Security* by Goodrich, Tamassia

Real-World Security

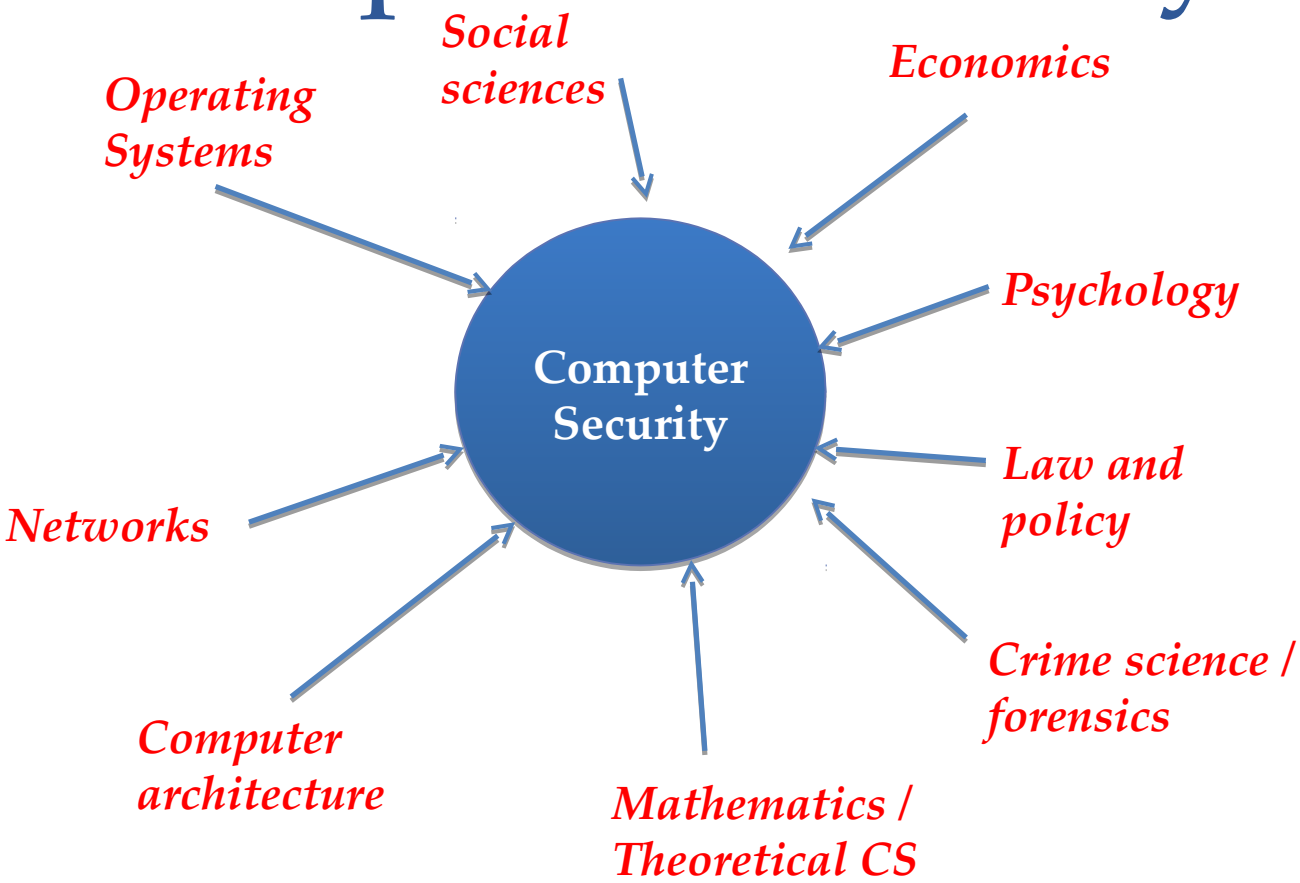
Security Principles

- Confidentiality
- Integrity
- Availability
- Crypto as a security tool

Real-World Security

The Digital Landscape

Computer Security



How is security achieved in the real world?

- **Prevention:** Physical barriers, access controls, encryption, firewalls, human awareness, etc.
- **Detection:** Audits, checks and balances.
- **Legal means:** Laws, patents, trademarks, copyrights, sanctions against wrongdoers.
- **Concealment:** Camouflage, steganography.

Different stakeholders have differing interests

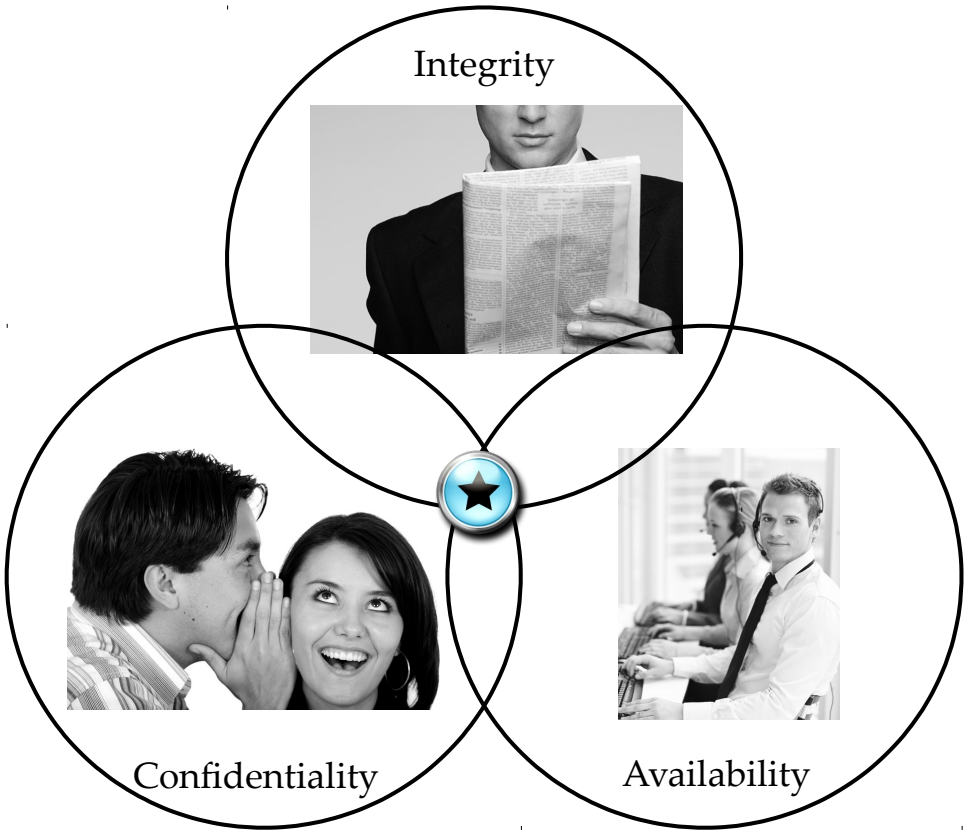
Consider an on-line banking web site.

- What are the interests of the customer?
- What are the interests of the bank?
- What are the interests of possible intruders?
- Can the bank trust the customer? Why or why not?
- Can the customer trust the bank? Why or why not?

Security Principles

Information security principles

The CIA triad (Confidentiality, Integrity, and Availability) captures many of the goals of information security.

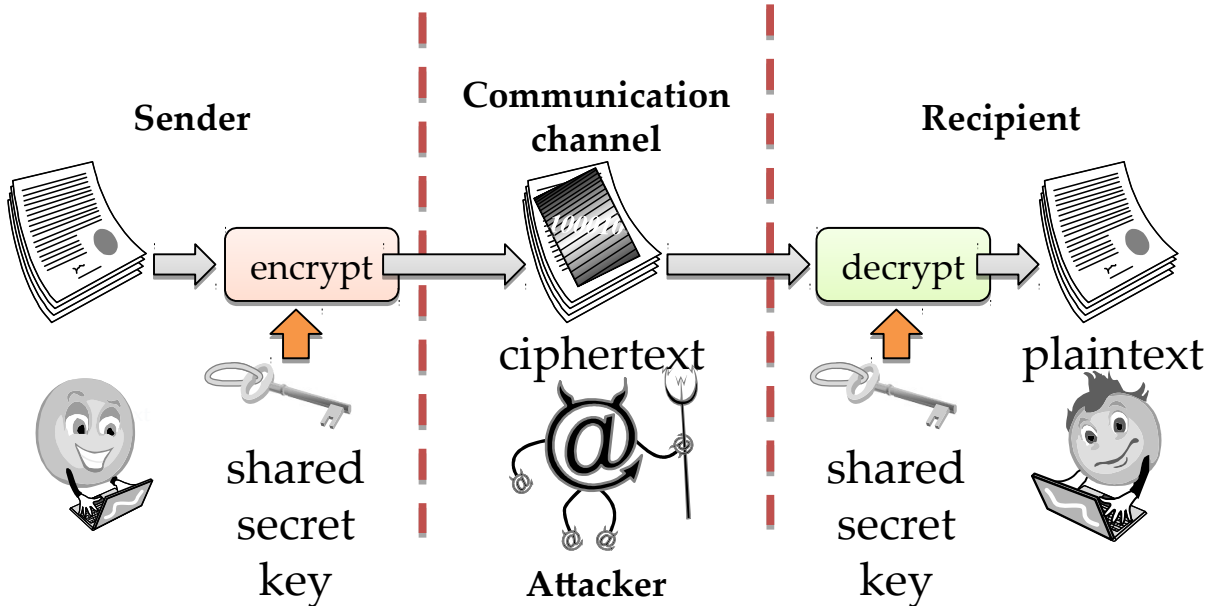


Confidentiality

- **Confidentiality** - *the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.*
  - confidentiality involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.

Tools for Confidentiality

- **Encryption:** the transformation of information in encoded/hidden form that can be open only using some secret (key) information

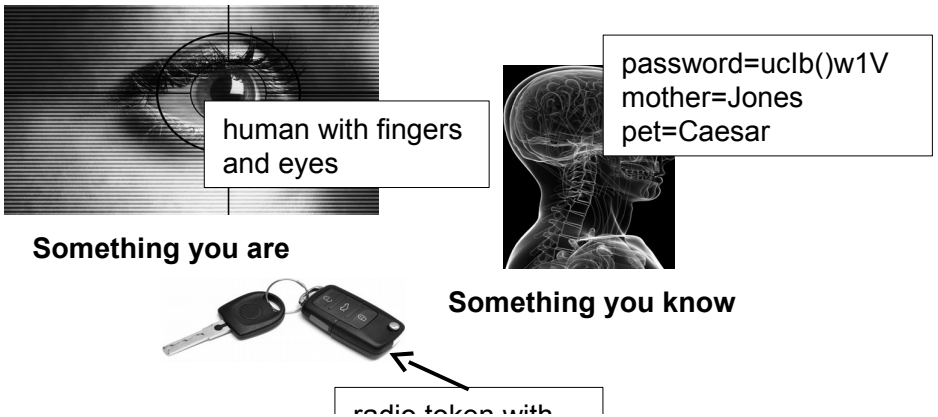


Tools for Confidentiality

- **Access control:** rules and policies that limit access to confidential information to those people and/or systems with a "need to know."
  - This need to know may be determined by identity, such as a person's name or a computer's serial number, or by a role that a person has, such as being a manager or a computer security specialist.

Tools for Confidentiality

- **Authentication:** the determination of the identity or role that someone has. Usually based on a combination of
  - something the person has (like a smart card or a radio key fob storing secret keys),
  - something the person knows (like a password),
  - something the person is (like a human with a fingerprint).



Integrity

- **Integrity:** The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
- **Tools:**
  - **Backups:** the periodic archiving of data.
  - **Checksums:** the computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
  - **Data correcting codes:** methods for storing data in such a way that small changes can be easily detected and automatically corrected.

Availability

- **Availability:** The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.
- **Tools:**
  - **Physical protections:** infrastructure meant to keep information available even in the event of physical challenges.
  - **Computational redundancies:** computers and storage devices that serve as fallbacks in the case of failures.

Principles of risk management

No such thing as absolute security.

Security goal: optimize tradeoff between cost of security measures and losses from security breaches.

Security risks can be lowered by

- Reducing exposure to attack.
- Reducing number of vulnerabilities.
- Reducing value to the attacker of a successful attack.
- Increasing the cost of a successful attack.
- Increasing the penalty for a failed attempt.

What does this have to do with cryptography?

Cryptography is an important tool for achieving information security.

Cryptography is to information security as locks are to personal security.

- Both are clever mechanisms that can be analyzed in isolation.
- Both can be effective when used in suitable contexts.
- Both comprise only a small part of the security picture.

Some applications of cryptography

- Secret message transmission over an insecure channel.
- Remote authentication.
- Verifying integrity and authenticity of data: digital signatures.
- Privacy-preserving computation.
- Contract signing.
- Protection of data at rest.