CPSC 467: Cryptography and Computer Security

Michael J. Fischer

Lecture 1
August 27, 2014
Protecting Information

Information security
Security principles
Crypto as a security tool

Highlights from Syllabus
Protecting Information
Information Security

*Protecting information* is a major challenge in the digital world.

Massive compromises of confidential data are disclosed almost daily.

- Identity theft.
- Industrial espionage.
- Cyberwarfare.
- Major web sites taken down by denial-of-service attacks.
- Massive government surveillance.
- Massive harvesting of personal data by large internet companies such as Google and Facebook.
Threat examples

Some risks and possible countermeasures:

- Eavesdropping on private conversations: encryption.
- Unauthorized use of a computer: passwords, physical security.
- Unwanted email: spam filters.
- Unintentional data corruption: checksums and backups.
- Denial of service: redundancy, isolation.
- Breach of contract: nonrepudiable signatures.
- Malicious data corruption: backups, access controls, cryptographic hash functions.
- Disclosure of confidential data: access controls, encryption, physical 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.
Banking example

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?
Information security principles

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

How well does this capture

- privacy?
- secrecy?
- authenticity?
- trustworthiness?
- non-repudiation?
- accountability?
- deniability?
- auditability?
- authorization?
- possession?
- utility?
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.
Highlights from Syllabus
Expectations

Read the syllabus! Some highlights:

- Pay attention to policies on plagiarism, submitting your work, and electronics in class.
- Teaching assistant is Ewa Syta.
- The midterm and final exam are both scheduled. Keep those dates clear.
- You will use the Zoo for both programming and homework submissions.
- Do problem set 0!

Also, class attendance and class participation is required. See me if you have to miss class.