CPSC 467: Cryptography and Computer Security

Michael J. Fischer

Lecture 2
September 1, 2017

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

Course Overview

Security Principles

Confidentiality

Integrity

Availability

Crypto as a security tool

Threats

Who are the Attackers?

Course Overview

Course modules

1. Security properties: Interests of various parties, motivation and capabilities of adversaries, knowledgable and provability.
2. Classical cryptography: Simple algorithms, information leakage, stream and block ciphers, DES, AES, message authentication codes.
3. Public key cryptography: 2-key systems, pseudorandom numbers, cryptographic hash functions, digital signatures.
4. Crypto toolbox: Multiparty protocols such as contract signing, oblivious transfer, zero-knowledge proofs, bit commitment, secret-splitting, and coin flipping.
5. Real-world applications such as SSH, SSL, WPA, encrypted email, PGP/GPG, bitcoin, etc.

Computer science, mathematics and cryptography

Cryptography cuts across both computer science and mathematics.

Computer science: Cryptography underlies much security software. The algorithms must be implemented correctly and efficiently.

Mathematics: Mathematics underlies both algorithms and their security analysis.

Many cryptographic primitives are based on:

- Number theoretic problems such as factoring and discrete log;
- Algebraic properties of structures such as elliptic curves.

Some useful mathematics

Cryptography cuts across traditional areas of mathematics. Some topcs relevant to cryptography:

- Probability and statistics.
- Coding theory.
- Complexity theory.
- Number theory.
- Algebra.

We will draw from pure mathematics to provide insight for how algorithms work and why they are believed secure. No specific prior knowledge of any of these areas is expected. The relevant mathematical facts will be presented as needed.

Organization

The main body of the course is organized around *cryptographic primitives*. For each one:

- What can be done with it? Study of cryptographic algorithms and protocols.
- What are its properties? Modeling and analysis. Requires complexity theory, probability theory, and statistics.
- How does it work? Requires some mathematics, particularly number theory and algebra.
- How is it implemented? Requires attention to detail, especially to prevent accidental leak of secret information.

What this course is not

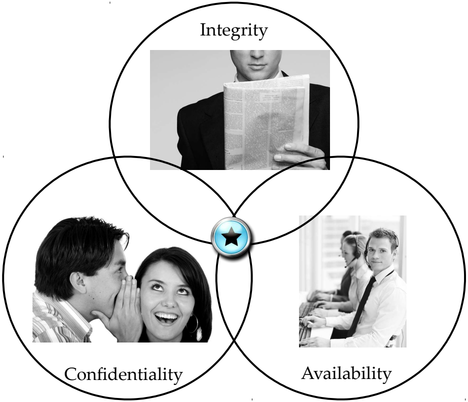
This course is broad rather than deep.

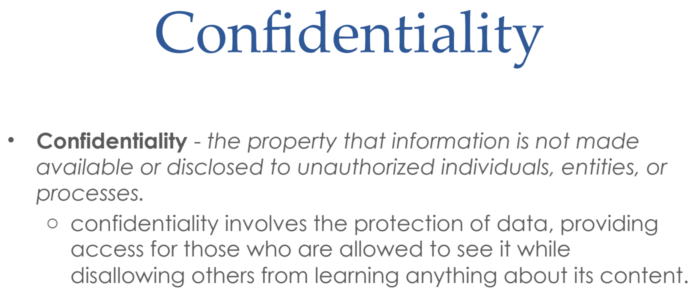
- Only enough mathematics to understand algorithmes such as AES, RSA, ElGamal, and elliptic curves will be presented.
- It will only briefly touch on cryptanalysis, the flip side of cryptography.
- It will not go deeply into real-world security protocols.
- It will not talk about security mechanisms for computer and network devices and applications such as firewalls, operating system access controls, detecting software security holes, or dealing with web security vulnerabilities.

Security Principles

Information security principles

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



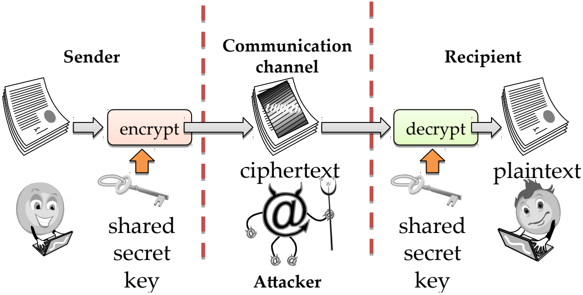


Confidentiality

- **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

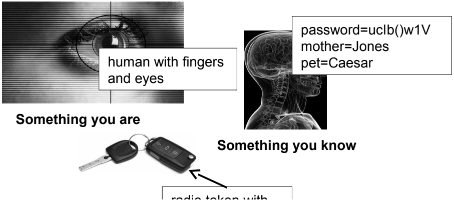


Tools for Confidentiality

- **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.

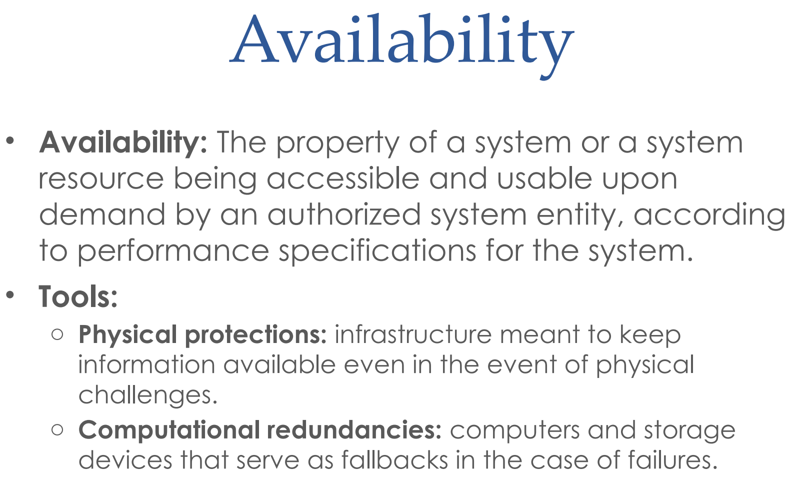
Tools for Confidentiality

- **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.

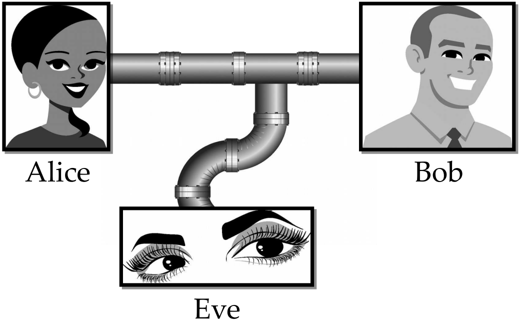
Threats

Threat examples 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.

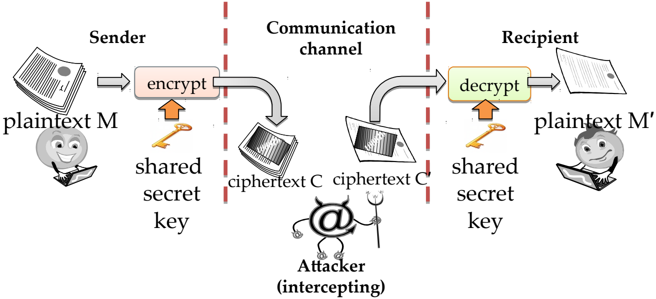
Threats and Attacks

- **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel.



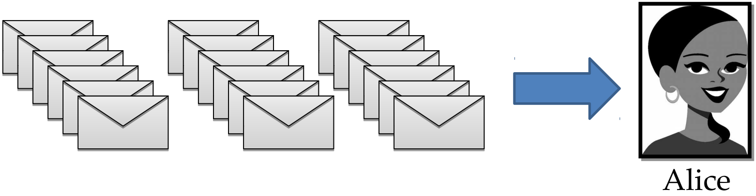
Threats and Attacks

- **Alteration:** unauthorized modification of information.
  - **Example:** the **man-in-the-middle attack**, where a network stream is intercepted, modified, and retransmitted.



Threats and Attacks

- **Denial-of-service:** the interruption or degradation of a data service or information access.
  - **Example:** email **spam**, to the degree that it is meant to simply fill up a mail queue and slow down an email server.



Threats and Attacks

- **Masquerading:** the fabrication of information that is purported to be from someone who is not actually the author.

"From: Alice"
(really is from Eve)

Threats and Attacks

- **Repudiation:** the denial of a commitment or data receipt.
  - This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.

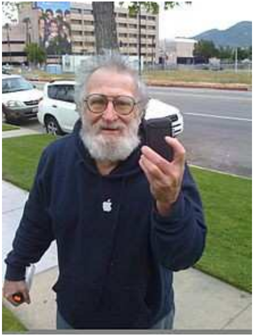
Public domain image from http://commons.wikimedia.org/wiki/File:Plastic_eraser.jpeg

Threats and Attacks

- **Correlation** and **traceback:** the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information.

Bob

Who are the Attackers?



John “Captain Crunch” Draper

Phreaking

Targets:
AT&T phone system

Escapades:

> 2600Hz Cap’n Crunch whistle
> Blue box
> Worked at Apple, taught Wozniak and Jobs

I don’t do that. I don’t do that anymore at all. And if I do it, I do it for one reason and one reason only. I’m learning about a system. The phone company is a System. A computer is a System, do you understand? If I do what I do, it is only to explore a system. Computers, systems, that’s my bag. The phone company is nothing but a computer.
— Secrets of the Little Blue Box, Ron Rosenbaum, Esquire Magazine (October 1971)

Read more: http://en.wikipedia.org/wiki/John_Draper

Kevin “Condor” Mitnik

Free LA bus rides, breaking into corporate systems

Made off with:
> 1 year prison, 3 years supervision
> Consulting career
> Book deal

Read more: http://en.wikipedia.org/wiki/Kevin_Mitnick

Julian “Mendax” Assange

Hacker in early 90’s

Targets:
> Nortel
> USAF 7th Command
> Wikileaks

Made off with:
> Free stay at Ecuadorian embassy

Read more: http://en.wikipedia.org/wiki/Julian_Paul_Assange

Albert “soupnazi” Gonzalez

Committed various electronic crimes while also a FBI/USSS informant

Targets:
Heartland Payment Systems, TJX, others

Made off with:
> 130,000,000 credit card numbers
> $2mil in cash
> 15-20 years in jail

Read more: http://en.wikipedia.org/wiki/Albert_Gonzalez

Russian Business Network

St. Petersburg Internet hosting company involved in numerous criminal activities

Started as legitimate ISP (2006)
Hosts malware, spammers, phishing sites
Alleged operator of Storm botnet
Accused of involvement in DoS on Estonia

Makes off with:
> Supposedly ~$150mil per year

Read more: http://en.wikipedia.org/wiki/Russian_Business_Network

People's Liberation Army Unit 61398

Widely accused of participating in attacks against Falun Gong websites, US companies

Google said China originated attacks in Operation Aurora

Great Firewall of China

Makes off with:
> Allegedly, lots of intellectual property
> Strict control over Internet usage

Read more: http://en.wikipedia.org/wiki/Operation_Aurora

US (and Israeli) governments

Widely accused of developing Stuxnet worm that attacked and temporarily disabled Iranian nuclear reactors

Makes off with:
> Slowed down nuclear reactors
> First use of "cyberweapons" targeting physical damage

Read more:
http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all

Edward Snowden

Former NSA contractor. Whistleblower on USA mass surveillance and cyber Espionage

Makes off with:
> 10s of 1000s of NSA documents
> Criminal charges in USA
> Several prizes
> Life in Russia

Read more:
http://en.wikipedia.org/wiki/Edward_Snowden

North Korea's Bureau 121

North Korean leader Kim Jong Un at the Sci-Tech Complex, in this undated photo released by North Korea's Korean Central News Agency (KCNA), October 28, 2015.Reuters/KCNA

Bureau 121 is a North Korean cyberwarfare agency, which is part of the Reconnaissance General Bureau of North Korea's military. According to American authorities, the General Bureau of Reconnaissance (also termed Reconnaissance General Bureau) manages clandestine operations and has six bureaus. Cyber operations are thought to be a cost-effective way for North Korea to maintain an asymmetric military option, as well as a means to gather intelligence; its primary intelligence targets are South Korea, Japan, and the United States. Bureau 121 was created in 1998.

Read more: https://en.wikipedia.org/wiki/Bureau_121