CPSC 467: Cryptography and Security

Michael J. Fischer

Lecture 3
September 8, 2020

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

Threats

Who are the Attackers?

Analyzing Confidentiality of Cryptosystems

- Secret ballot elections
- Information protection

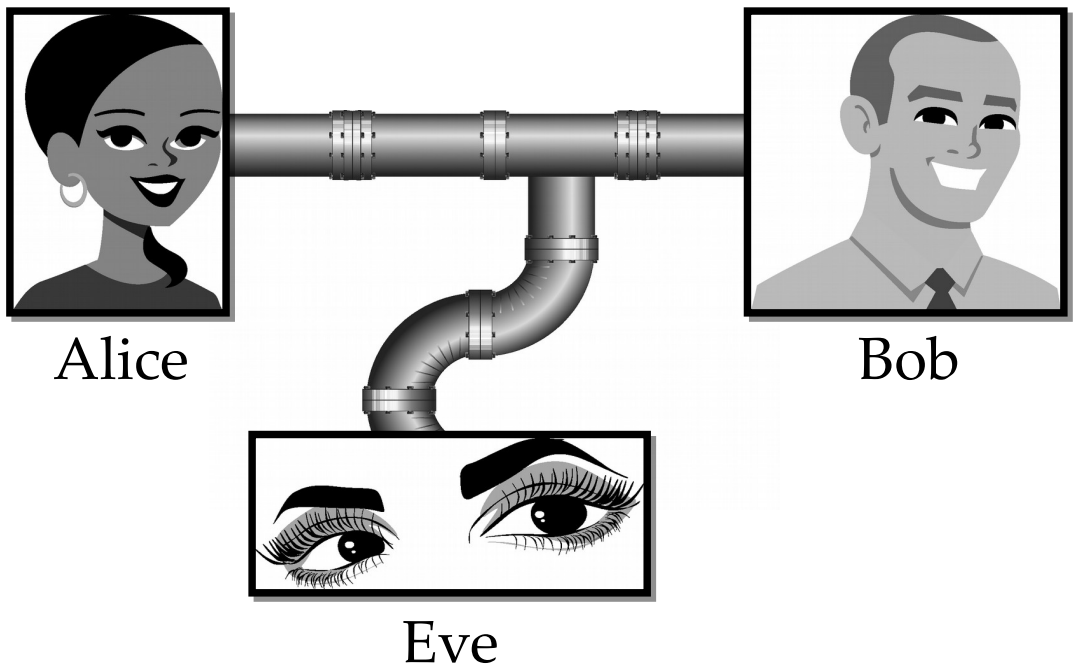
Threats

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.

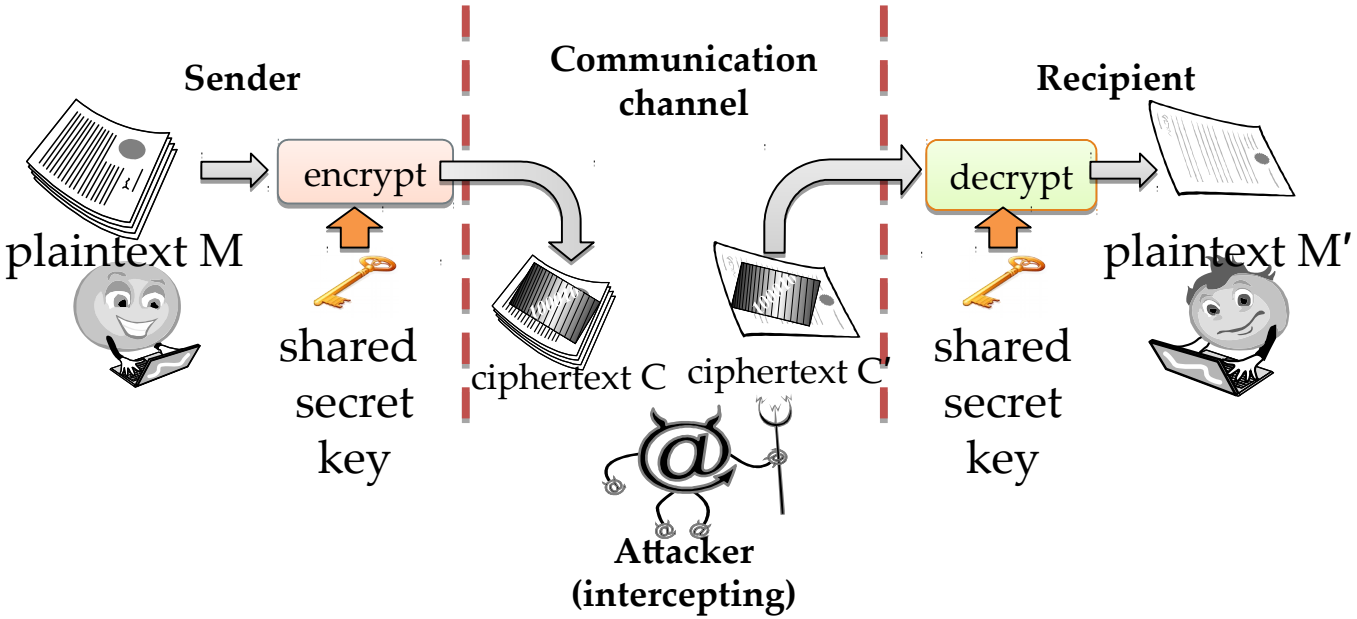
Threats and Attacks

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



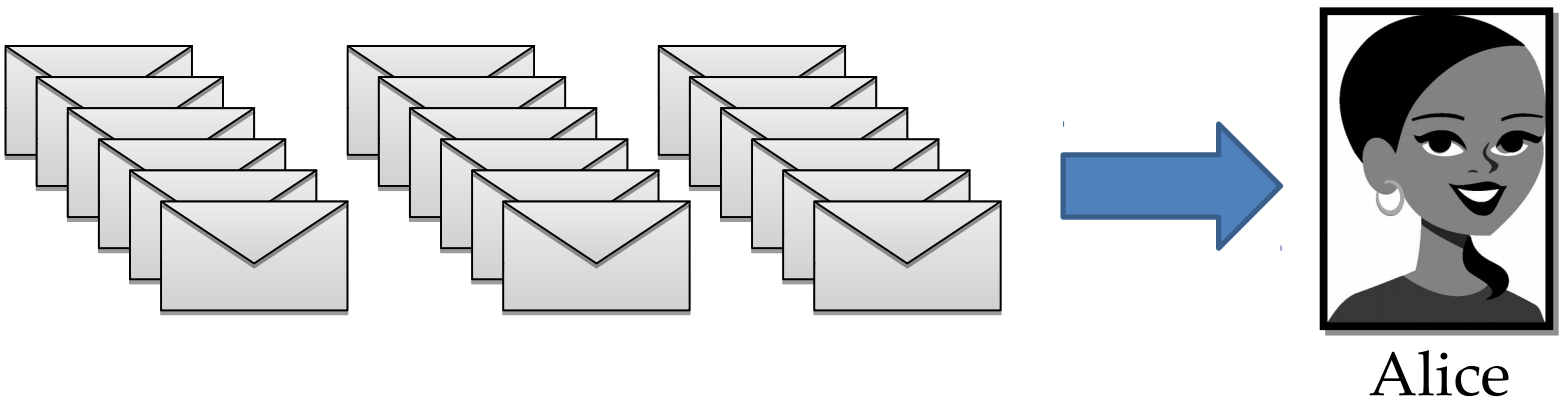
Threats and Attacks

- **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.



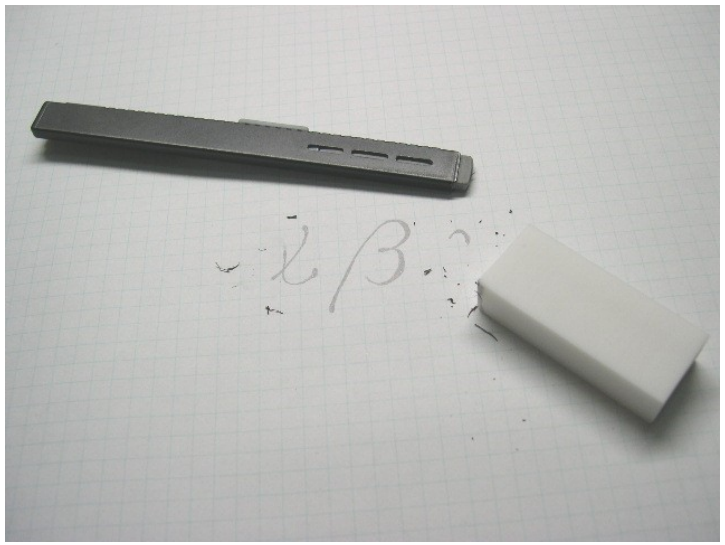
Threats and Attacks

- **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

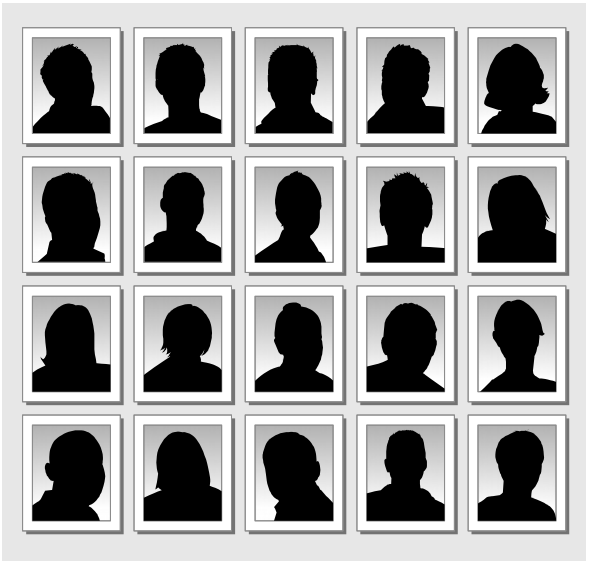
- **Repudiation:** the denial of a commitment or data receipt.
  - This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.



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

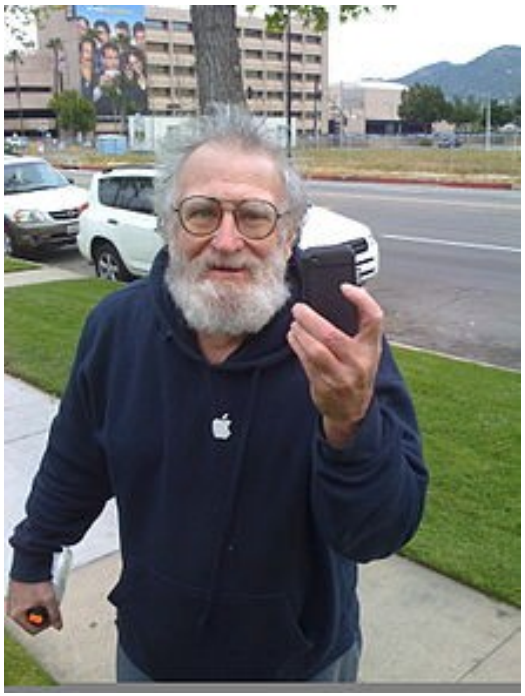
Threats and Attacks

- **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

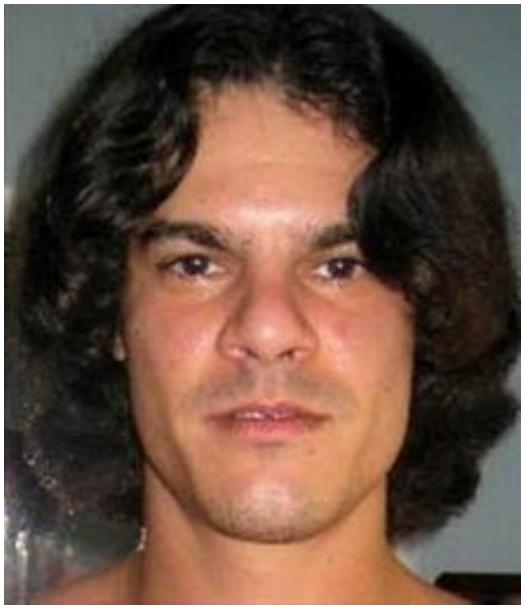
Julian "Mendax" Assange

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 cyber-warfare 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

Analyzing Confidentiality of Cryptosystems

Election example

What does *confidentiality* mean in a secret-ballot election?

Some proposed definitions:

1. Nobody knows if I voted.
2. Nobody knows how I voted.
3. Nobody gets any information about how I voted other than what could be inferred from the election returns.

Why might these properties be important?

What is the difference between 2 and 3?

Confidentiality and information

Information is central to the notion of *confidentiality*.

Information is what is to be protected; not its representation by data.

Often, ciphertext (the encrypted message) is public data that nonetheless hides secret information.

The adversary generally has some prior knowledge about the secret.

Confidentiality protection means limiting the amount of new information that the adversary can acquire, given reasonable assumptions about the adversary's prior knowledge and capabilities.

What is new information?

New information is anything that Eve learns from the ciphertext that she didn't know before.

Here are some things that she might learn:

1. The ciphertext of the message is `EXB JXQ`.
2. The length of the message is 6.
3. The third letter of the message is either `e` or `y`.
4. The message is either `hae mat` or `buy gun`.
5. The message is `buy gun`.
6. The encryption key is 3.

Questions for protecting each kind of information:

- How important is it to protect?
- How hard is it to protect?

What if Eve only sometimes succeeds?

Eve might only succeed on certain runs of the protocol.

For example, suppose Eve already knows that `EXB JXQ` means `buy gun`. Then without any knowledge of the key or even the kind of cryptosystem in use, if she sees `EXB JXQ`, she knows what it means.

Is this a serious security breach? Why or why not?

What are you assuming about the likelihood of different messages?

What if Eve knows the message in advance?

Suppose she knows *in advance* that the message is `buy gun` but *does not* know the ciphertext.

When she sees the ciphertext `EXB JXQ`, she can immediately output the decryption `buy gun`.

Does this mean that she has broken the cryptosystem?

Does this mean that she has deciphered the message?

Can she convince Fred that her decryption is correct?

Does this matter?

Imperfect attacks

Eve does not always have to succeed to do damage.

Weak keys Eve might succeed in reading messages encrypted using certain "weak" keys.

Partial information Eve might discover some information about m by narrowing down the set of possibilities but still not know which is correct.
Example: In many cryptosystems, she always learns the length of m.

Randomized algorithms Eve might use a randomized attack algorithm that succeeds with some small probability.

What kinds of compromise are acceptable?

How much protection is needed?

A naive claim of confidentiality: **Eve can't find the key.**

This definition is both too strong and too weak.

Too strong We can't always prevent Eve from finding the key.

- She can guess the key at random and will sometimes be right.
- She can try all possible keys, given enough time.

Too weak The goal of a cryptosystem is to keep information confidential. A system in which Eve can decrypt Alice's messages is totally insecure, whether or not she learns the key.

Can you think of a situation where Eve could decrypt messages but not find the key?

A more nuanced approach

Some compromises of decreasing difficulty for Eve:

Complete break Eve can find the key.

- Can read all messages between Alice and Bob.
- Can send valid encrypted messages to Bob.

Complete message recovery Eve can decrypt all messages.

- Can read all messages between Alice and Bob.
- Cannot encrypt her own messages to fool Bob.

Selected message recovery Eve can decrypt some subset of possible messages.