
Security and Privacy

Threats and Tools to Protect Yourself

Notes for CSC 100 - The Beauty and Joy of Computing
The University of North Carolina at Greensboro

Reminders

For Monday, November 11

Due tomorrow (Tuesday) at 10:00am
Blown to Bits Reading Reflection - Chapter 5

Blown to Bits Discussion
Check discussion forum for prompts

Project
Progress reports due Friday (Nov. 15)

Warning: I'll be out of town the remainder of the week. If questions about any of this, email me!

Security Basics - What is security?

Commonly discussed in terms of three goals:

- **C**onfidentiality
Unauthorized people should not get information
Violation example: Thief gets your credit card number
 - **I**ntegrity
Unauthorized people should not modify information
Violation example: Thief changes "destination account" on a transfer
 - **A**vailability
Authorized people should be able to get information/services
Violation example: "Hactivist" knocks out a web server
-

Example of Security Attacks

Spamhaus Attack - Part 1

The New York Times Business Day
Technology

WORLD | U.S. | NY / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Published: March 30, 2013

How the Cyberattack on Spamhaus Unfolded

Spamhaus, a spam-prevention service based in Europe, was the victim of one of the largest known cyberattacks. The attackers tried to overwhelm Spamhaus's servers using what is known as a distributed denial of service attack. This technique harnessed the power of relatively few computers to generate as much as 300 gigabits a second of traffic — an attack so large it disrupted Internet service for millions of users in Europe. [Related: NYTimes](#)

Credit: New York Times, March 30, 2013

Example of Security Attacks

Spamhaus Attack - Part 2

The Initial Attack

1. The attackers send commands to about 1,000 computers under their control.
2. Each computer, pretending to be Spamhaus, sends requests for information to a type of Internet server called an open resolver. An estimated 100,000 resolvers are involved in the attack.
3. The resolvers respond with a much larger message than the initial request, amplifying the size of the attack.
4. Spamhaus cannot handle the amount of traffic and ceases to respond to legitimate traffic.

Question:
What security goal is violated?

The attackers amplified their assault by sending a relatively small command of a few bytes to the open resolvers which replied with a message that was 100 times larger than the initial request.

Credit: New York Times, March 30, 2013

Example of Security Attacks

LinkedIn Compromise



More than 6 million LinkedIn passwords stolen

By David Goldman @CNEMoney Tech June 7, 2012 8:34 AM ET

NEW YORK (CNNMoney) — Russian hackers released a giant list of passwords this week, and on Wednesday security researchers identified their likely source: business social networking site LinkedIn.

LinkedIn (LNKD) confirmed in a blog post late Wednesday afternoon that some of the stolen passwords correspond to LinkedIn accounts.

The company did not offer any information about how the passwords were stolen or the extent of the damage, but it said it is "continuing to investigate" the matter.

Dating site eHarmony also announced Wednesday that some of its users' passwords were stolen in the attack.

The 6.5 million leaked passwords were posted Monday on a Russian online forum, camouflaged with a common cryptographic code called SHA-1 hash. It's a format that's considered weak if added precautions aren't taken. Roughly half of the "hashed" passwords have already been decoded and posted online in human-readable text.

Question: What security goal is violated?

Example of Security Attacks

LinkedIn Compromise

WhatsApp Web site hijacked, shows pro-Palestinian message

A group called KDM5 Team claims credit for taking over the Web site of the popular messaging service, which is used to send billions of messages a day.

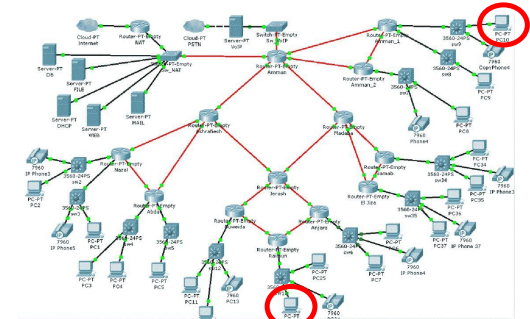


Question:
What security goal is violated?

Credit: screenshot by Stephen Skerfving (@SKR) on Twitter
The Web site of WhatsApp, a widely used messaging app, was hijacked Tuesday. The site showed a pro-Palestinian message at 2:40 a.m. PT Tuesday and was given the title "You Got Perked". A group called KDM5 Team claimed credit for the attack.
"Our Web site was hijacked for a small period of time, during which attackers redirected our Web site to another IP address," the company said in a statement. "We can confirm that no user data was lost or compromised. We are committed to user security and are working with our domain hosting vendor FastNet. Solutions on further investigation of this incident."
According to the Whois database, which can be used to see what numeric Internet Protocol (IP) address is assigned to a given Internet domain, the whatsapp.com IP address record was changed on Tuesday. Such a change, made through the Internet's Domain Name Service (DNS) system, is one way that users who typed in the whatsapp.com name would be redirected to a different Web site.

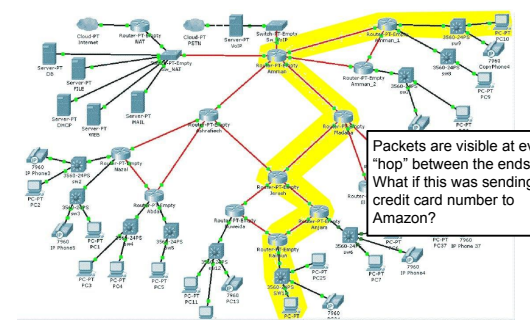
Protections

Eavesdropping problem: Consider Internet Communication



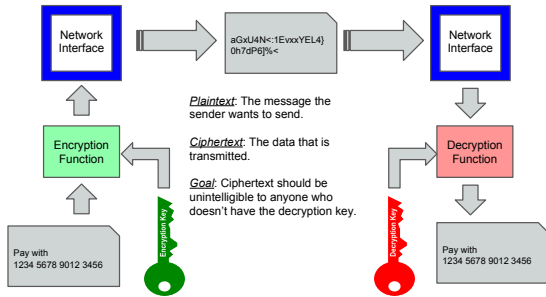
Protections

Eavesdropping problem: Consider Internet Communication



Protections

Cryptography to the Rescue! Encryption for Confidentiality



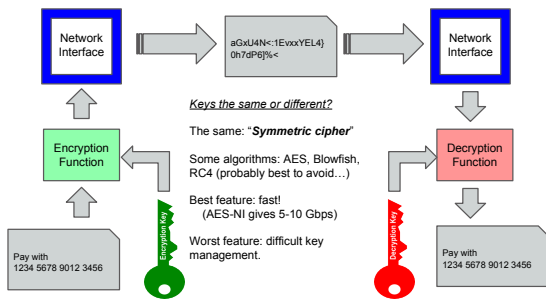
Plaintext: The message the sender wants to send.

Ciphertext: The data that is transmitted.

Goal: Ciphertext should be unintelligible to anyone who doesn't have the decryption key.

Protections

Cryptography to the Rescue! Encryption for Confidentiality



Keys the same or different?

The same: **"Symmetric cipher"**

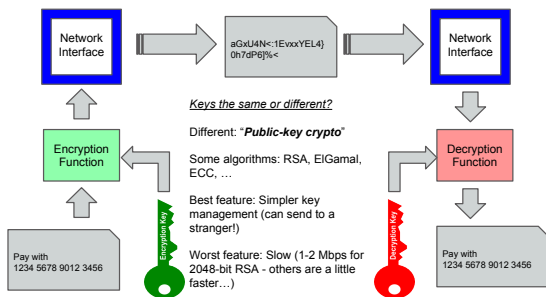
Some algorithms: AES, Blowfish, RC4 (probably best to avoid...)

Best feature: fast!
(AES-NI gives 5-10 Gbps)

Worst feature: difficult key management.

Protections

Cryptography to the Rescue! Encryption for Confidentiality



Keys the same or different?

Different: **"Public-key crypto"**

Some algorithms: RSA, ElGamal, ECC, ...

Best feature: Simpler key management (can send to a stranger!)

Worst feature: Slow (1-2 Mbps for 2048-bit RSA - others are a little faster...)

Protections

How big is a 128-bit (AES) key? To try all keys (brute force)...

2004 Estimate: \$100k machine breaks 56-bit DES key in 6 hours

What about a 128-bit key?

\$100k machine takes $>10^{18}$ years [the earth is $<10^{10}$ years old]

What if we spent \$100,000,000,000?

Would take $>10^{12}$ years

What about Moore's law saying that in 20 years machines will be about 16,000 times faster?

Would take $>10^8$ years

OK, what about in 40 years (machines 100 million times faster)?

Would still take $>30,000$ years

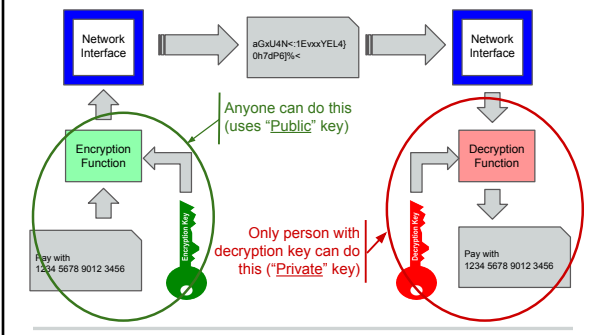
Do you really think Moore's law will last this long?

What about improvements in algorithms/cryptanalysis or super-duper quantum computers?

This could change everything...

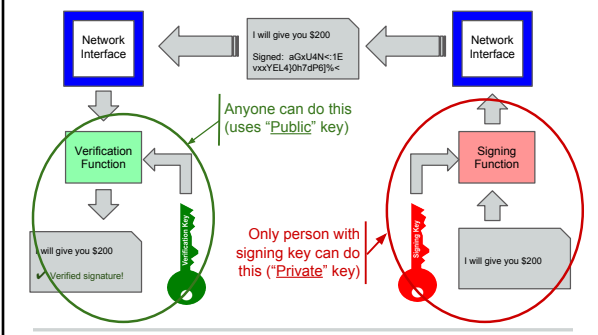
Protections

Cryptography to the Rescue! Signatures for Integrity



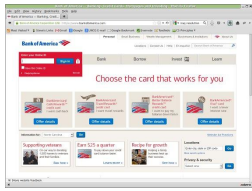
Protections

Cryptography to the Rescue! Signatures for Integrity



Protections

Verifying the origin of a web site

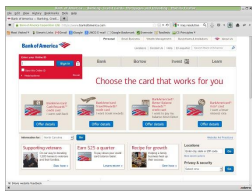


Signed by Bank of America Signing Key

Verify with Bank of America verification key

Protections

Verifying the origin of a web site



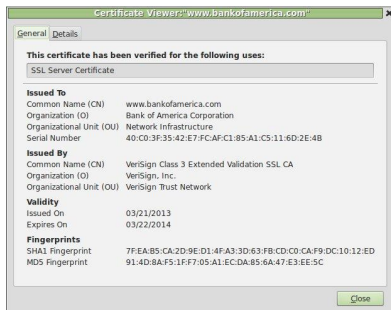
Signed by Bank of America Signing Key

Verify with Bank of America verification key

How do you know you have the right verification key?
It is signed (called a "certificate")! ... by a Certification Authority (CA)
A handful of trusted CA's built in to browser.

Protections

Viewing certificates



Protections - Tools

Crypto-enabled tools - Tools for e-mail and file protection

PGP: "Pretty Good Privacy"

- Originally created by Phil Zimmerman in 1991
- Interesting legal (export) and patent (RSA) problems at the time
 - Phil Zimmerman was under criminal investigation (no charges filed)
 - RSA Inc. allowed use of RSAREF library for non-commercial use (still other patent issues though)
- OpenPGP and then GPG (GnuPG) to avoid patent questions

Functionality:

- Supports encrypting and signing messages and/or files
 - Most direct use is for e-mail
 - People also use for encrypting files or protecting integrity (e.g., Linux software distribution)

Obtaining: GPG available from <http://www.gnupg.org/>

Protections - Tools

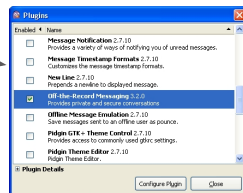
Crypto-enabled tools - Tools instant messaging

OTR (Off The Record)

- Encryption support for instant messaging protocols
- Designed by well-known and trusted people (Goldberg & Borisov)
- One design goal was *deniability*
- Forward secrecy: Archived communication secure even if long-term keys are later discovered
- Works as a plug-in for common IM software (like Pidgin)

For more information:

<https://otr.cypberpunks.ca/>

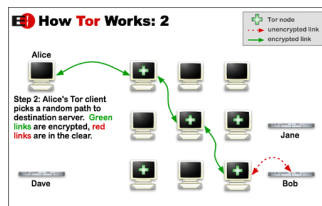


Protections - Tools

Crypto-enabled tools - Tools for anonymous Internet browsing

Tor: "The Onion Router"

- Traffic endpoints obscured using multiple hops and encryption
- Paths are randomized to obscure patterns
- For more information: <http://www.torproject.org>



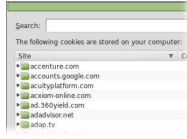
Privacy

“Privacy” is not the same as “Secrecy”

- Sometimes you willing give your information
- What happens to your information then?

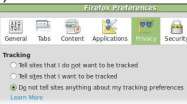
Cookies

- Information stored in browser
- Associated with specific domains/sites
- Sent along with web page requests
- ... including image/banner ad requests
- Information can include login credentials
- ... such as Facebook login (with your name!)



“Do Not Track” setting

- Recent initiative to indicate privacy prefs



Summary

Important things to know

Security goals: Confidentiality, Integrity, Availability

Encryption for confidentiality

- Terms: Plaintext, Ciphertext, Keys
- Symmetric cipher vs. Public-key encryption

Signatures for integrity

- Types of keys: Signing key, verification key
- Web site origin verification: Certificates, CAs

Tools

- PGP and GPG for encrypted email
- OTR for private chat
- Tor for anonymous communication
