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

Reminders for November 12

Blown to Bits

Chapter 6: Start reading - reflection due Wed., 11/19

Project

Should be working on coding (assistance in Lab on Friday)
Progress report due Friday (Nov. 14) at 5:00

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. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Published: March 30, 2013

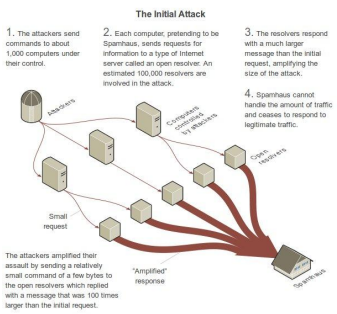
How the Cyberattack on Spamhaus Unfolded

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 Article »

Credit: New York Times, March 30, 2013

Example of Security Attacks

Spamhaus Attack - Part 2



Question:

What security goal is violated?

Credit: New York Times, March 30, 2013

Example of Security Attacks

Home Depot Compromise

Home Depot confirms months-long hack

By Jose Pagliery @Jose_Pagliery September 9, 2014: 7:10 AM ET
NEW YORK (CNNMoney)

Home Depot on Monday confirmed that hackers indeed broke into its payment systems -- maybe as far back as April.

Home Depot (HD)'s hack might be even bigger than Target (TGT)'s was last year. In Target's case, hackers slipped in for three weeks and grabbed 40 million debit and credit cards. Hackers remained in Home Depot's computers -- unnoticed -- for about five months.

Hackers stole debit and credit card data from shoppers in the United States and Canada. The question now is how many millions of shoppers are affected.

Home Depot said it's still investigating the breach, but said there's still "no evidence" debit card PINs were exposed.

But noted Internet fraud expert Brian Krebs, who first reported the Home Depot breach a week ago, wrote early Tuesday that there's a sharp increase in recent days in fraudulent

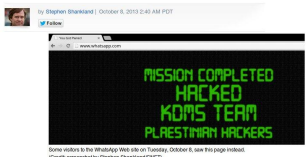
Question: What security goal is violated?

Example of Security Attacks

WhatsApp Compromise

WhatsApp Web site hijacked, shows pro-Palestinian message

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



Some visitors to the WhatsApp Web site on Tuesday, October 8, saw this page instead. (Credit: screenshot by Stephen Shankland/CNET)

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 Pwned." A group called KDMS 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 Network Solutions on further investigation of this incident."

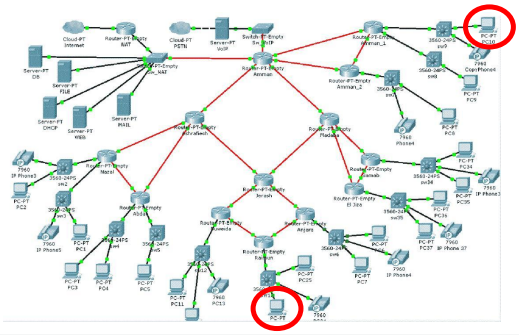
According to the Whois database, which can be used to see what numeric Internet Protocol (IP) address is assigned to a given Internet domain, the whatsapp.com IP address record was changed on Tuesday. Such a change, made through the Internet's Domain Name Service (DNS) system, is one way that users who typed in the whatsapp.com name would be redirected to a different Web site.

Question:

What security goal is violated?

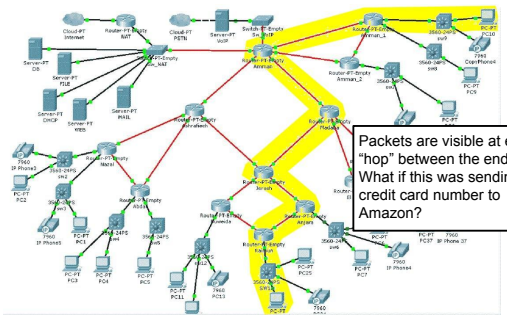
Protections

Eavesdropping problem: Consider Internet Communication



Protections

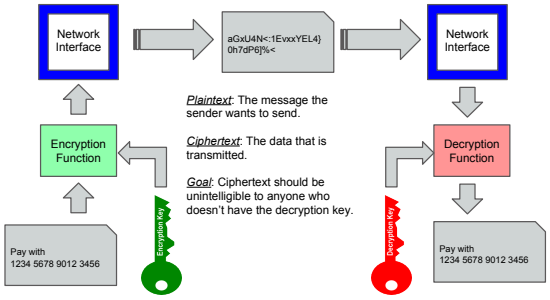
Eavesdropping problem: Consider Internet Communication



Packets are visible at every "hop" between the ends. What if this was sending a credit card number to Amazon?

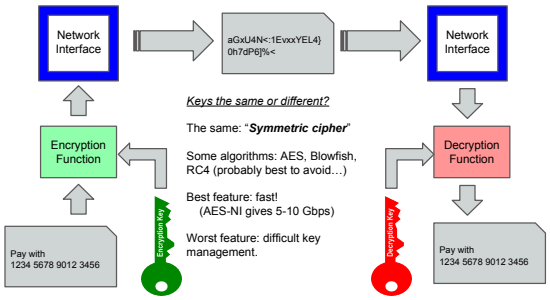
Protections

Cryptography to the Rescue! Encryption for Confidentiality



Protections

Cryptography to the Rescue! Encryption for Confidentiality



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

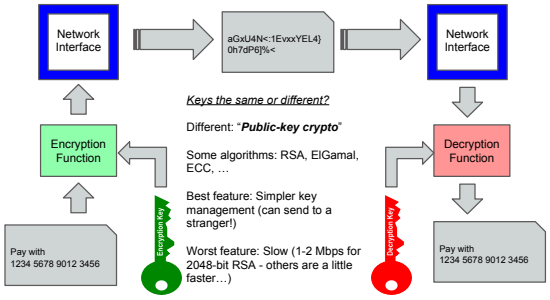
Do you really think Moore's law will last this long?

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

This could change everything....

Protections

Cryptography to the Rescue! 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

Research in Public Key Crypto Was Revolutionary!

MIT Team Wins Turing Award

Goldwasser and Micali revolutionized cryptography

By Abby Abazorius on April 23, 2013

Shafi Goldwasser and Silvio Micali, along with Ronald Rivest, lead the Information and Computer Security Group at CSAIL.

On June 15, EECS professor Shafi Goldwasser and engineering professor Silvio Micali will receive the A. M. Turing Award for their pioneering work in cryptography and complexity theory. The two developed new mechanisms for encrypting and securing information, which are widely applicable today in communication protocols, Internet transactions, and cloud computing. They also

New ways of thinking about security.

Important part: Taking a computational view, based on reductions.

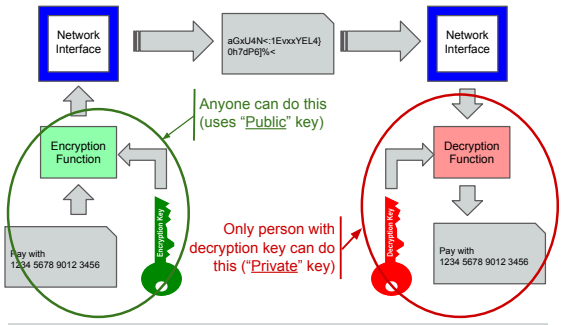
Example: "If Algorithm A can get any information out of a ciphertext, then we can use that to efficiently solve Problem B (which we believe is computationally difficult)."

Logical Contrapositive: "If it is impossible to efficiently solve Problem B then there is no way any algorithm can get any information out of a ciphertext."

"Problem B" might be "factoring large integers."

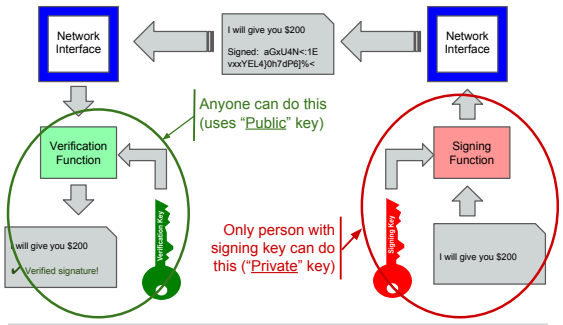
Protections

Cryptography to the Rescue! Signatures for Integrity



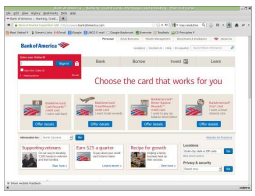
Protections

Cryptography to the Rescue! Signatures for Integrity



Protections

Verifying the origin of a web site

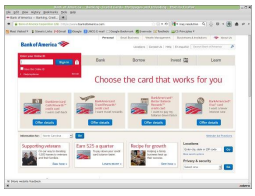


Signed by Bank of America Signing Key

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

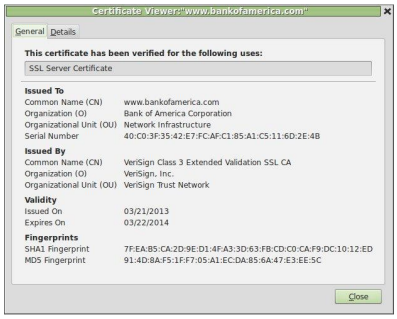
How do you know you have the right verification key?

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 used 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)

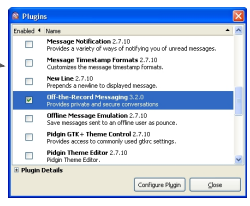
Obtaining: GPG available from http://www.gnupg.org/

Protections - Tools

Crypto-enabled tools - Tools for 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:

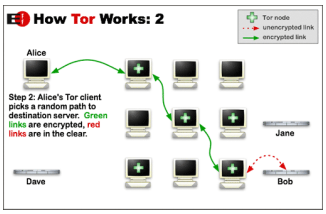
https://otr.cypherpunks.ca/

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



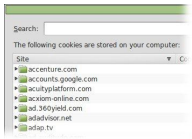
Privacy

“Privacy” is not the same as “Secrecy”

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

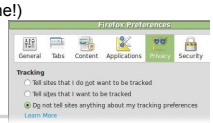
Cookies

- 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