ACM NetSec

Cybersecurity Made Simple

Personal Security: Integrity

Agenda

- Recap
- Phishing
- HTTP/HTTPS
- MITM
- Wifi
- Software Signatures

CIA Principle

C — Confidentiality

I — Integrity

A — Accessibility

Last Session: Confidentiality

- Anyone still using TFA for MyUCLA?
- Anyone install a password manager since last session?
- Brief Summary

Hashing Revisited

- What makes a good hash function?
- How do hash functions tend to work?

Good (Cryptographic) Hash Functions

- Difficult to invert
  - Could find a user's password from a hashed database!
- Difficult to find two inputs with the same output (collision)
  - Could modify data and have it pass a checksum
  - Could modify data and have it pass a digital signature!!
- Several forms of collision attack exist
  - Finding two random strings that collide
  - Given a string, append data to it to produce the same hash
  - Given two different strings, append data to each to produce the same hash

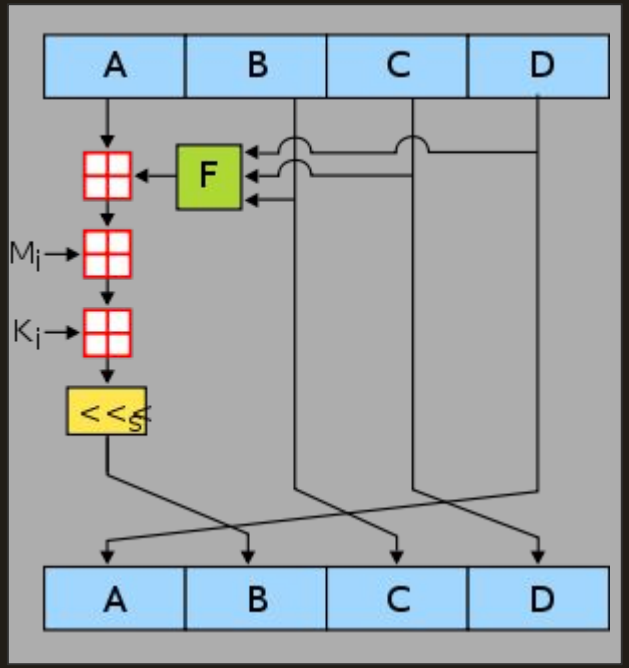
Bad (Cryptographic) Hash Function

- md5

=

How Hash Functions Work

- One round of md4 (48 total)
- A, B, C, and D are 32 bits
- Looks pretty random



Crypto Note

- Math problems can be used as a basis for hash functions
- E.g.
  - Message is an integer m
  - Everyone knows e (some exponent) and p (some really big prime)
  - Hash(m) = m^e (mod p)
- Finding the original number seems to be pretty hard
- If anyone figured out how to invert the hash, they could also solve this problem
  - This is how cryptographers “prove” security
- This isn’t used because it’s very slow and inconvenient

I

Integrity

Integrity:

Ability to ensure that data is an accurate and unchanged representation of the original secure information


Software update
"Mac Media Player" is out of date
The version of "Mac Media Player" on your system does not include the latest security updates and has been blocked. To continue using "Mac Media Player", download an updated version.
Download Media...
OK
The new version of Mac Media Player is ready to download.
DOWNLOAD

Agenda

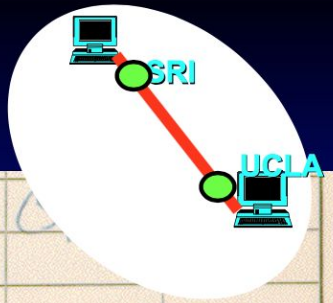
- Recap
- Phishing
- HTTP/HTTPS
- MITM
- Wifi
- Software Signatures

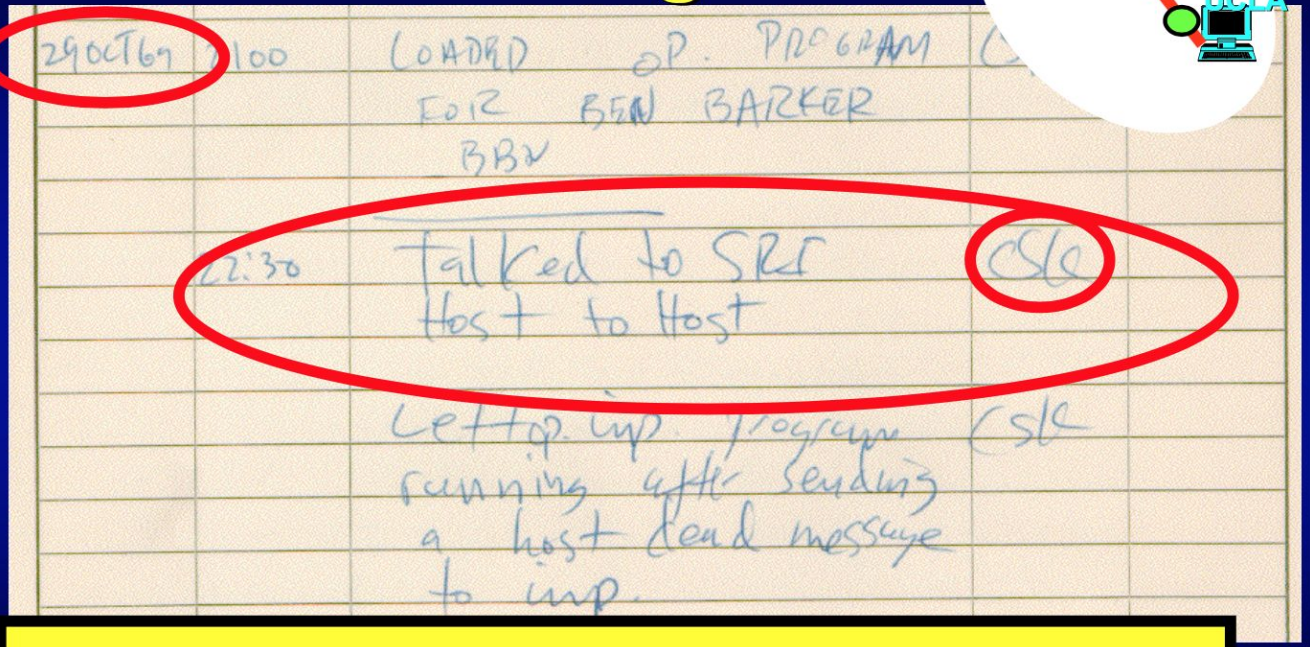
Brief History of the Internet: The First Spam

First Message on the Internet sent from UCLA to SRI

[SLIDES]

An Important Entry in Our IMP Log




29 OCT 69 2100 LOADED OP. PROGRAM
FOR BEN BARKER
BBN
22:30 Talked to SRI Csk
Host to Host
Left op. imp. program Csk
running after sending
a host dead message
to imp.

First Message on the Internet - ever!

But What WAS the First Message Ever [illegible] net?

- W[illegible]

LO !

©Leonar[illegible]

Spam !

- It surfaced as a critical and widely publicized event in April 1994 when two Arizona-based attorneys arguably became the two most hated individuals in the history of the Internet. It was Lawrence Canter and Martha Siegel, the famous "green card lawyers" who "spammed" the Internet.

The First Spam email

- From: Laurence Canter (nike@indirect.com)
  Subject: Green Card Lottery- Final One?
  Newsgroups: alt.brother-jed, alt.pub.coffeehouse.amethyst
  View: Complete Thread (4 articles) | Original Format
  Date: 1994-04-12 00:40:42 PST

Green Card Lottery 1994 May Be The Last One!
THE DEADLINE HAS BEEN ANNOUNCED.

The Green Card Lottery is a completely legal program giving away a certain annual allotment of Green Cards to persons born in certain countries. The lottery program was scheduled to continue on a permanent basis. However, recently, Senator Alan J Simpson introduced a bill into the U. S. Congress which could end any future lotteries. THE 1994 LOTTERY IS SCHEDULED TO TAKE PLACE SOON, BUT IT MAY BE THE VERY LAST ONE.

PERSONS BORN IN MOST COUNTRIES QUALIFY, MANY FOR FIRST TIME.

The only countries NOT qualifying are: Mexico; India; P.R. China; Taiwan, Philippines, North Korea, Canada, United Kingdom (except Northern Ireland), Jamaica, Domican Republic, El Salvador and Vietnam.

Lottery registration will take place soon. 55,000 Green Cards will be given to those who register correctly. NO JOB IS REQUIRED.

THERE IS A STRICT JUNE DEADLINE. THE TIME TO START IS NOW!!

For FREE information via Email, send request to cslaw@indirect.com

****

Canter & Siegel, Immigration Attorneys
3333 E Camelback Road, Ste 250, Phoenix AZ 85018 USA
cslaw@indirect.com telephone (602)661-3911 Fax (602) 451-7617

Enablers for the Dark Side

- The Internet allows anyone to reach hundreds of millions of users
  - easily,
  - quickly,
  - at essentially no cost (in money or effort),
  - anonymously.
- This is a perfect formula for enabling the dark side of the Internet.

Phishing

C

I

A

An attempt to illegally gather personal and financial information by sending a message that appears to be from a well known and trusted company

How to spot a phishing email

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Links in email

Note: If you dont fill the application your account will be permanently blocked.

Threats

Regards,

Facebook Copyrights Department.

Popular company

Spelling and Grammar

- Whenever a large company sends out a message on behalf of the company as a whole, the message is usually reviewed for spelling, grammar, and legality, among other things
- So if a message is filled with poor grammar or spelling mistakes, it probably didn't come from a major corporation's legal department

Suspicious links

- If the hyperlinked address is different from the address that is displayed, the message is probably fraudulent or malicious
- In Outlook and Apple Mail, the URL **can be identified by hovering over the embedded URL**
- Links that lead to .exe files

You can check out suspicious links by going to

- http://www.urlvoid.com
- https://www.phishtank.com

Spoofing popular websites or companies

- Often the URL will contain the domain name of a legitimate website, disguising the malicious intent of the link

Dear Customer

Doubling your money before you have even started playing!

http://translate.googleusercontent.com/translate_c?depth=1&hl=auto&sl=de&
url=www.google.com.bo&u=http://onlinecasino27.yolasite.com/casino2&
usg=ALkJrhigo2DxeKnp8k6CY7J-q-rVMUPqBw

Best Regards,

http://blog.urlvoid.com/1305/google-translate-used-by-spammers-to-bypass-anti-spam-filters/

Website Spoofing Demo

- Notice how after the credentials are entered, the normal facebook login page reappears
- If this file were attached to a web address, the attack could be distributed to anyone with the link

Personal Information

- Your bank doesn't need you to send it your account number. It already knows what that is.
- Similarly, a reputable company should never send an email asking for your password, credit card number, or the answer to a security question.

Send them your contacts information to enable them locate you immediately they arrived in your country with your package.

This is the information they needed from you..

1) Your Full Name ==========
2) Your Home Address==========
3) Your Fax==========
4) Your Cell Numbers==========
5) You personal identification===
6) Your Occupation=====

Agenda

- Recap
- Phishing
- HTTP/HTTPS
- MITM
- Wifi
- Software Signatures

Cryptography

Constructing and analyzing protocols that prevent third parties or the public from reading private messages

This is my message in plaintext


```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.5 (FreeBSD)
Comment: This is what your message looks like after encryption.

hQEOA1e+1x6YuUMCEAP/VJyavkOX0KRMdVJUS7TW7P/QWXe27a4T55oLsR6n4S/a
9nU/gLa7ZEeZDD8KCf975dCrf1y8fZzryrSwOxhZfWYYjJWYg/XE1JrrPPMfL/BU
OzmJrve3XNu+ECG4oWOqDcP+5kuI9LLTDMM3VX+Id61833UpBYUObGmIyCWXnBMD
/1f335KFdh0BvkXumG4Mp3NnXvVaOUNL7TMCUMKKNcTQhV4iXZmiW+aQqkGijWtX
ydzg39lr2/5pAlbJsVsMFHsZU01qe12n0tfl0mvcApOvQbr/Tpm2WES2jIc7ZFOv
1ShbEO5GkSiBude0W7K1t62sWQyQNj2nZ7wyzSyvOQDj0lgBxGAiolg1bkpzPx+W
z95B1lB25obPJsII9qSXl+V/NPgHuOI5WR5ASYabU22alEkGEU0ydmpJpYYlsCPA
esQ7EX+i1F8mB8FSMsGbfiQY3oRuOrOdW9O6
=FpRv
-----END PGP MESSAGE-----
```

Symmetric Key Cryptography

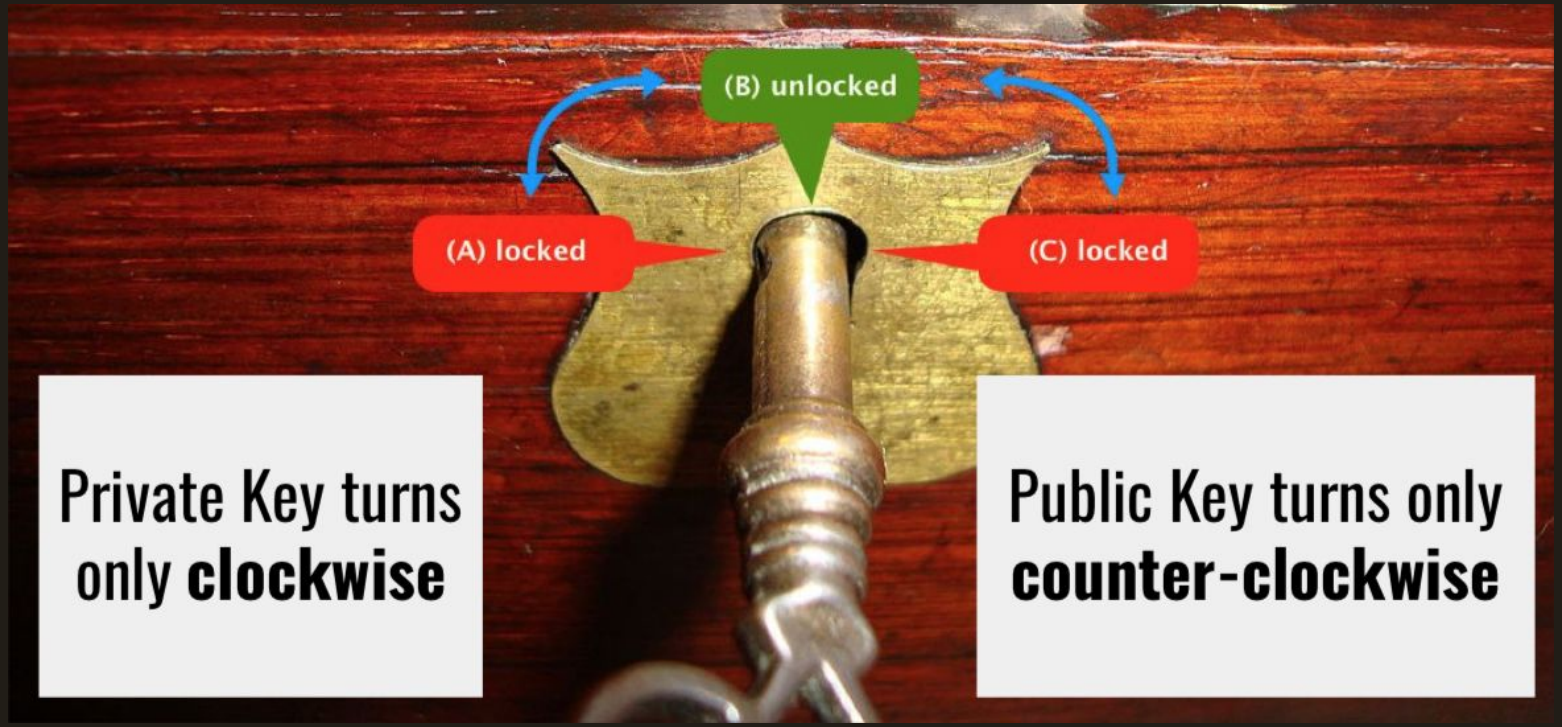
Algorithms for cryptography that use the same cryptographic keys for both **encryption** of plaintext and **decryption** of ciphertext

Symmetric Key

Public Key Cryptography (asymmetric key)

Cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner

Asymmetric Key



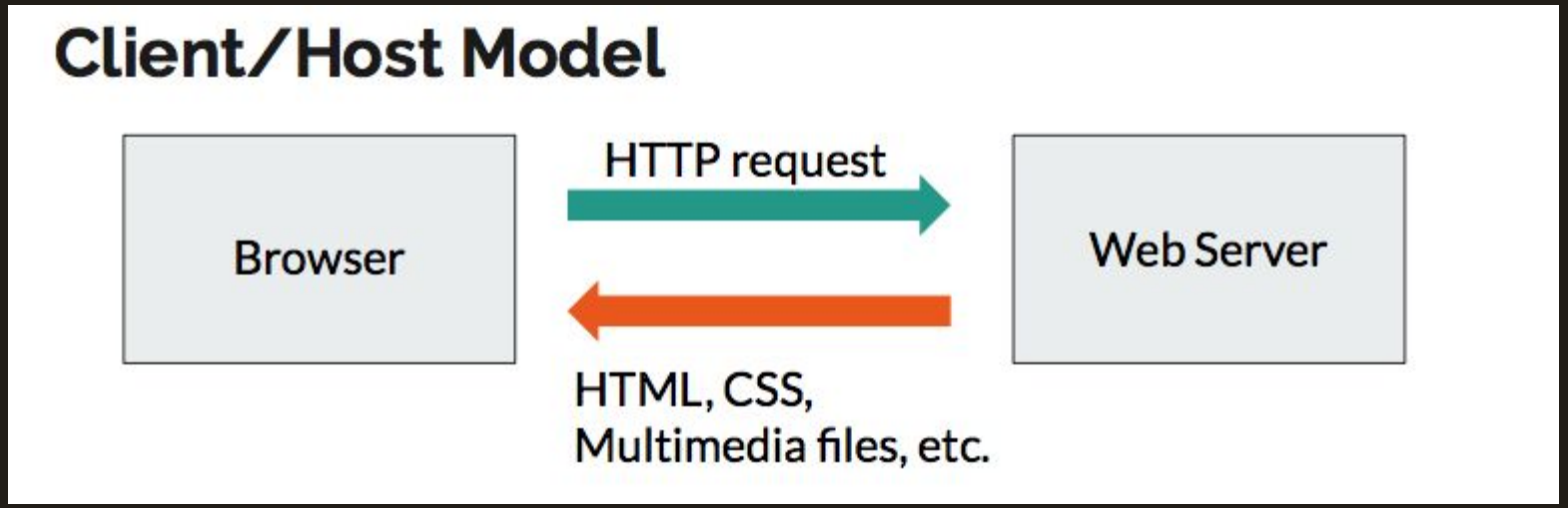
HTTP

HyperText Transfer Protocol

HTTP: An Analogy

- Imagine the internet is a town
- You are a client with an address that determines where you can be reached
- Businesses serve requests that are sent to them
- Crazy fast mailing service that takes requests in special language (HTTP)
- You submit a request, mail person builds a (TCP) track between your house and a business, and asks an employee for your request
- The business comes back with the relevant products

HTTP

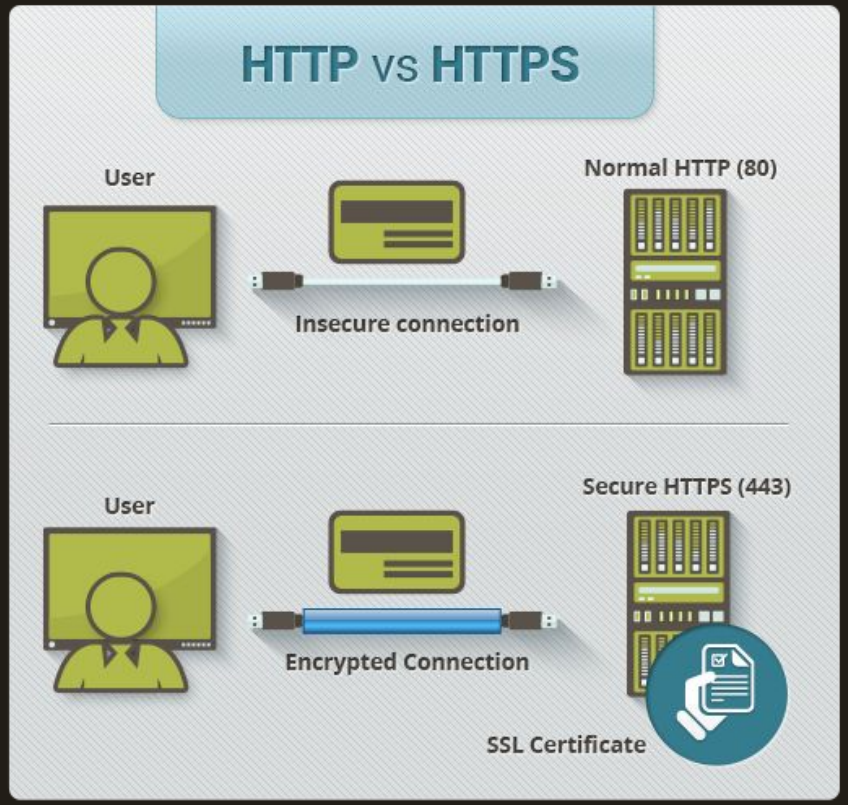

Client/Host Model
Browser
HTTP request
Web Server
HTML, CSS,
Multimedia files, etc.

HTTP vs. HTTPS

- (HTTP) - HyperText Transfer Protocol
- Unencrypted
- Unsafe for transfer of sensitive data

- **(HTTPS)** - HyperText Transfer Protocol **Secure**
- **HTTP over Transport Layer Security (TLS)**
- **Encrypted (both symmetric and asymmetric encryption)**
- **Safe for transfer of sensitive data**

HTTP vs. HTTPS



HTTPS

- Symmetric cryptography used to to encrypt transmitted data
  - Keys generated are **unique** to each session
- The identity of the communicating parties can be authenticated using public-key cryptography
- Each message uses a message authentication code to prevent undetected loss or alteration of the data during transmission

HTTPS


COMODO
SSL Certificate from Como
Comodo CA Ltd [GB]
https://www.instantssl.com
SSL Certificate from Como...
Comodo CA Ltd (GB)
Search
https://www.instantssl.com/
SSL Certificate from Comodo | Secure Socket Layer and More
Google
Opera
SSL Certificate from Co...
Trusted
www.instantssl.com
Search with Google

Agenda

- Recap
- Phishing
- HTTP/HTTPS
- MITM
- Wifi
- Software Signatures

Man-in-the-Middle

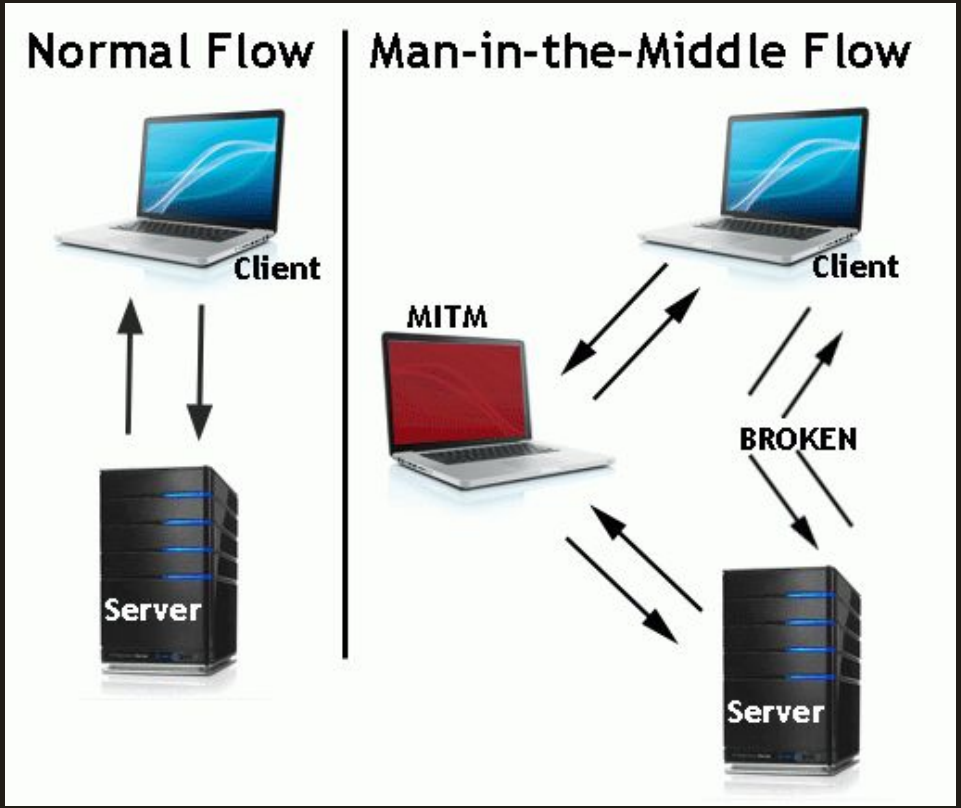
A cyber attack where a malicious actor inserts him/herself into a conversation between two parties

I

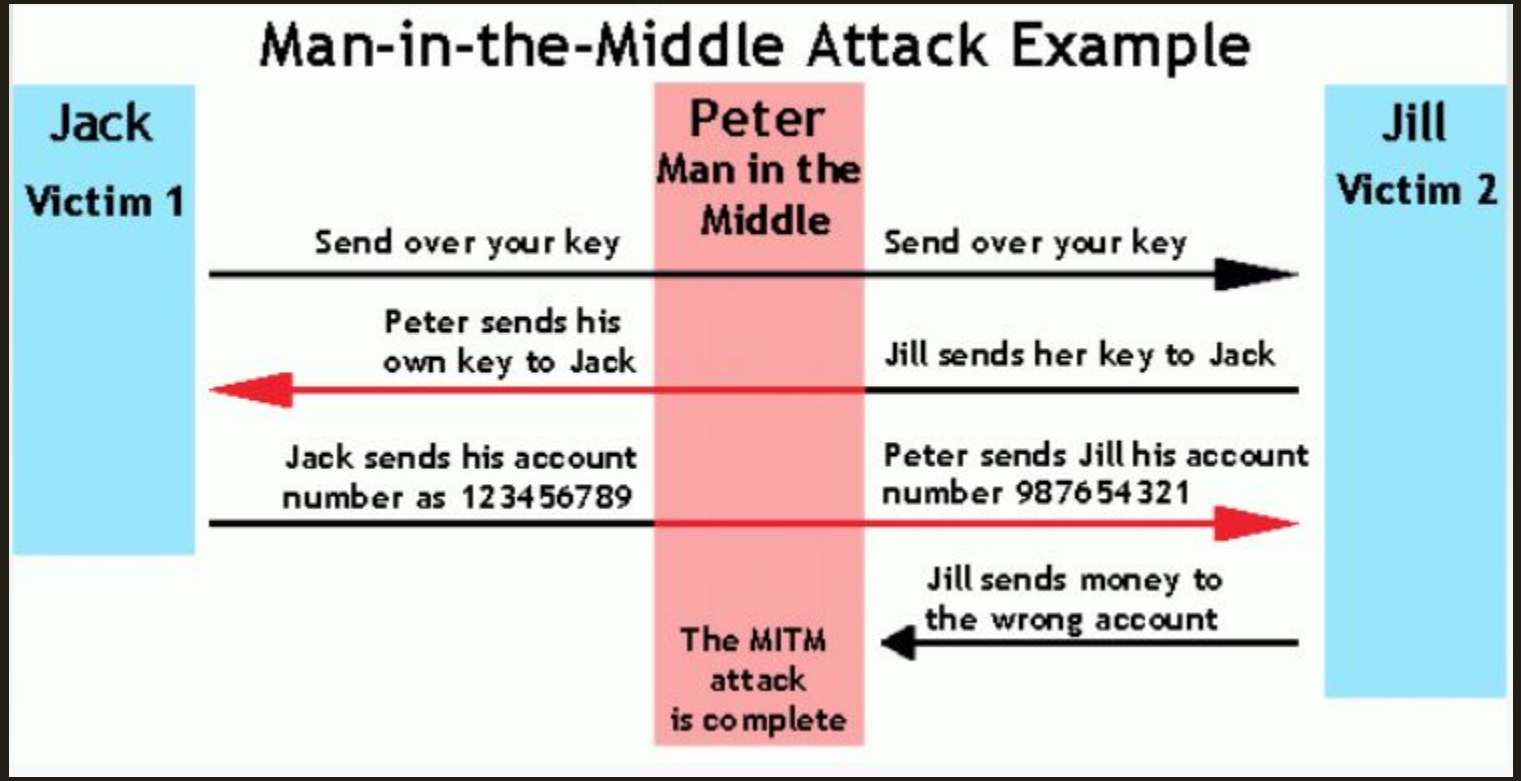
Integrity


CHASE
Log Off
CHASE COLLEGE (...3538)
Available balance
$1000.00
see activity
Transfer Money

Man-in-the-Middle



Man-in-the-Middle



[case] Online Voting

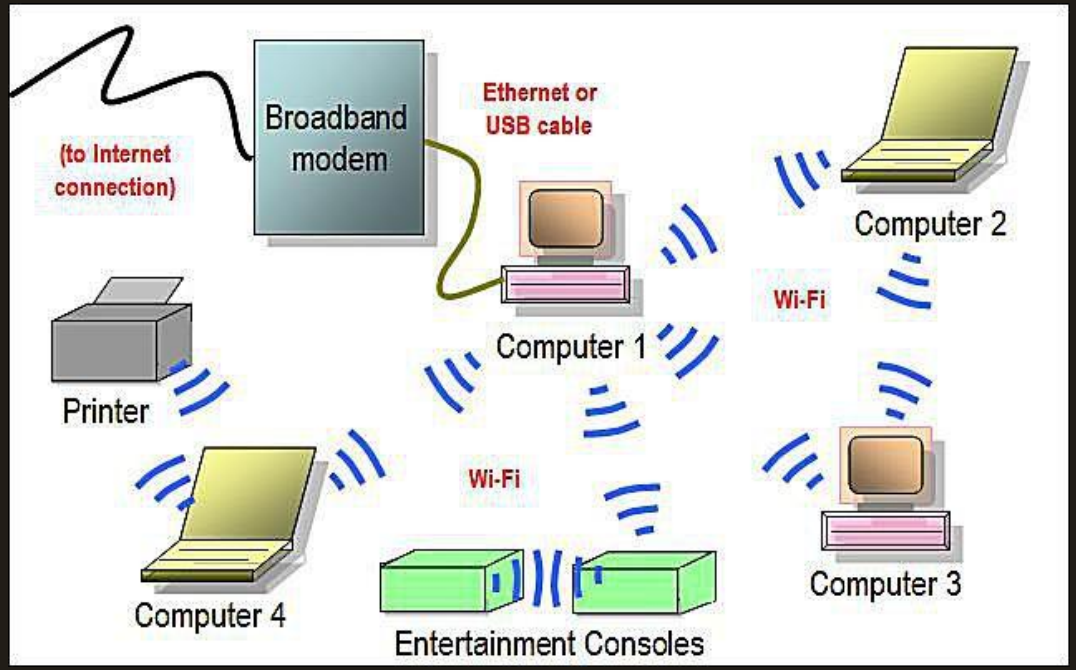
https://www.youtube.com/watch?v=w3_0x6oaDmI

Agenda

- Recap
- Phishing
- HTTP/HTTPS
- MITM
- Wifi
- Software Signatures

What even is wifi?

- Just radios
- Everyone has to agree to work together
  - Not interfere with connection
  - Not look at other's packets
- Historically this has failed



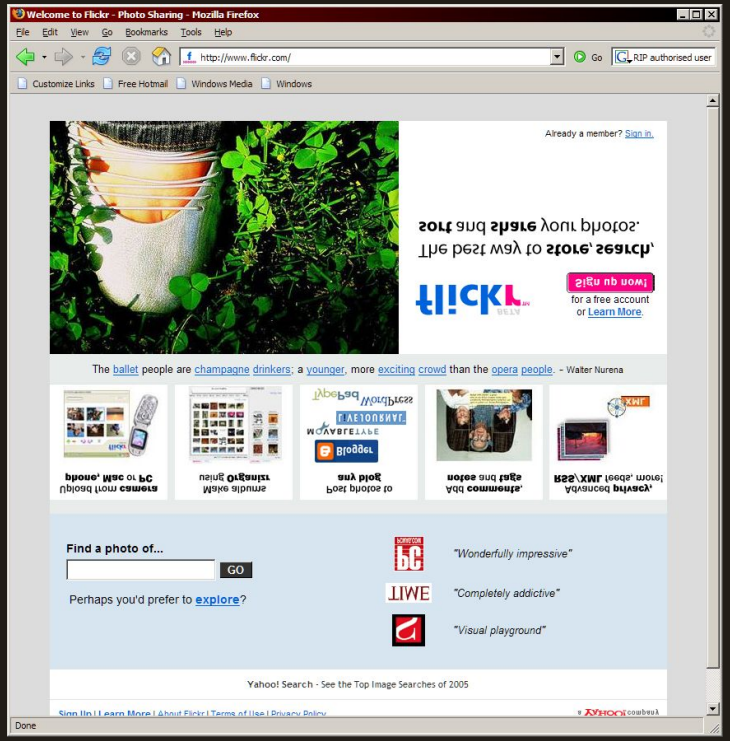
Attack 1: The Router Itself

- The internet is...
- The backbone tends to be corporations and government
- Not usually in their interest to violate integrity
  - They might just read some of it
- Much easier to manipulate data near the endpoints

Attack 1: The Router Itself

- Obvious confidentiality attacks
- But also...

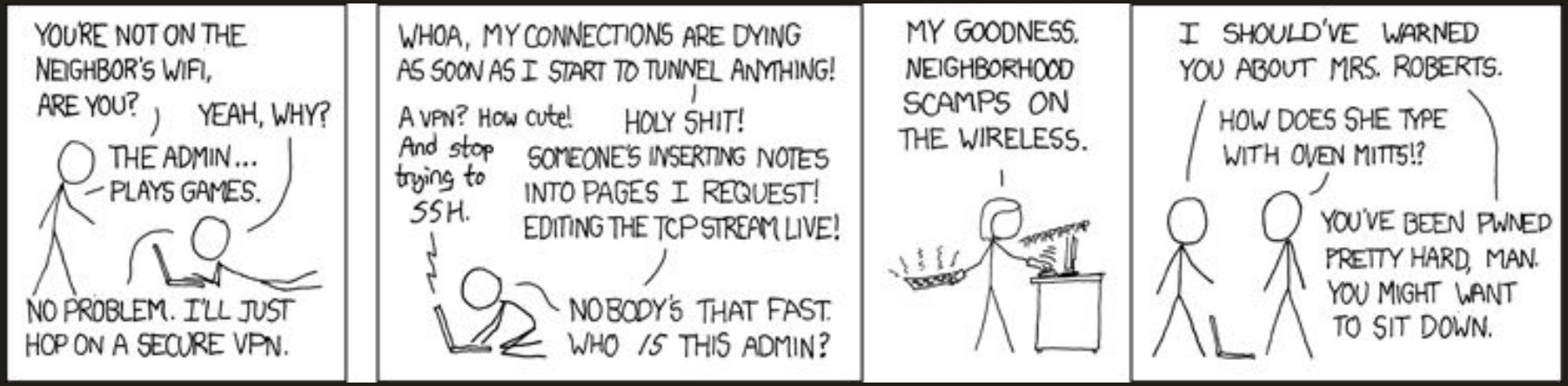
Attack 1: The Router Itself (upsidedownternet)



Attack 1: The Router Itself

- Or perhaps...

Attack 1: The Router Itself (xkcd)



Defense 1: VPN and HTTPS

- Encryption has integrity checks
- Routers can still modify packets
  - They will modify mysterious (to them) cyphertext
  - The interference can't be hidden

Attack 2: Malicious Users

- Radios see all waves as equal, so malicious users could
  - Pose as your access point
  - Pose as you
  - Send garbage (will talk about this during Availability)
- This is sufficient for an MITM!

Attack 2: Malicious Users

- Highly sophisticated attack

Defense 2

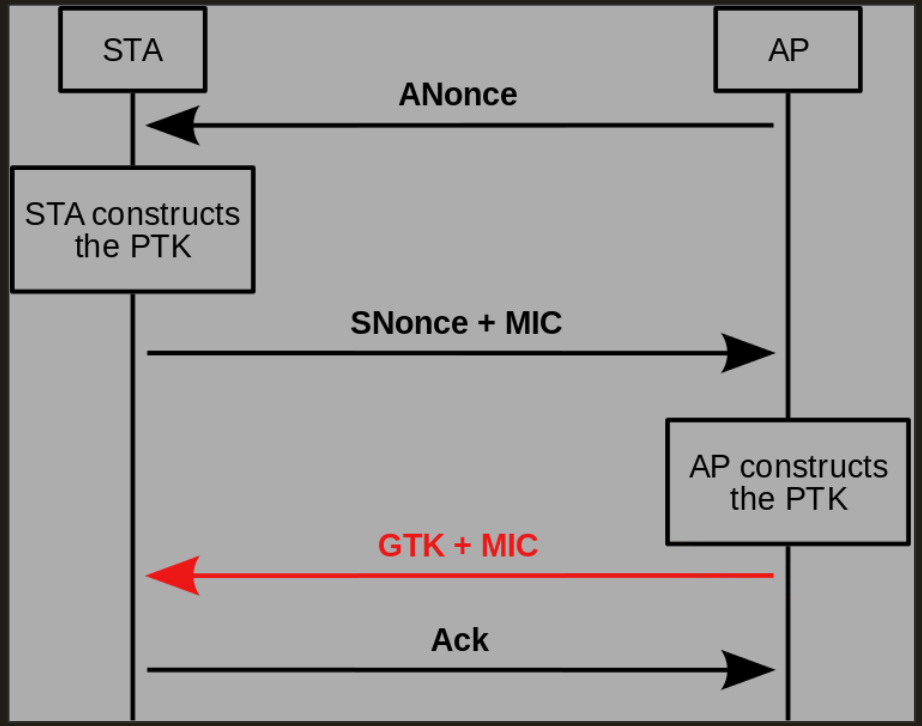
- Only use WPA2 wifi
- Wifi pineapple would attack as follows
  - Force disconnect (with wifi sorcery)
  - Spoof SSID and other wifi characteristics
  - You accidentally connect to pineapple
- Only works if pineapple owner knows password
- And the access point can't have a certificate
  - Rare, I've only seen one at security conference
- And the access point doesn't use WPA2-Enterprise
  - What eduroam uses - pineapple would need access to username/password
- VPN!!

Attack 3: Very Malicious User

- Brief case study of KRACK attack
- Actually several attacks
  - On routers, force reuse of same key
  - On Linux/Android, force install of all-zero key
  - Some more complicated versions for multi-access-point networks

Attack 3: Very Malicious User

- The way it should work
- Attacker steps in during red arrow
  - Attacks on AP happen just after the Ack



Defense 3

- Patch Patch Patch!
- And VPN

Agenda

- Recap
- Phishing
- HTTPS/TLS
- MITM/MITB
- Wifi
- Software Signatures

Why Sign Software

- Normal HTTPS web pages are “signed”
  - Encryption ensures the server sent them
  - Protocol ensures you trust the server
- Software you download is no exception
- However…
  - Download mirrors
  - Server compromises
  - Legacy websites with C applets that never configured HTTPS, and someone near you has a suspicious looking router

Why Sign Software

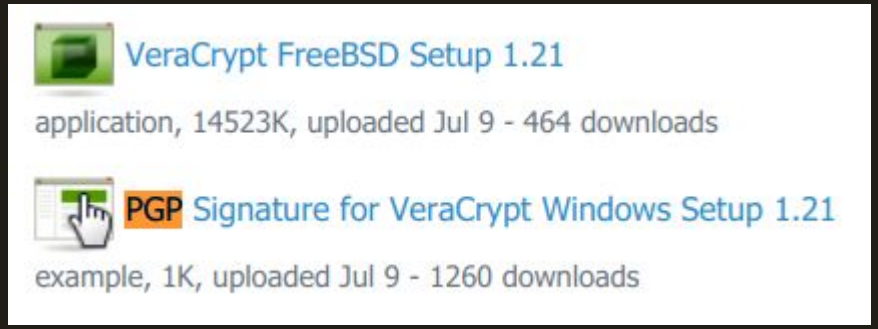
- Normal HTTPS web pages are “signed”
  - Encryption ensures the server sent them
  - Protocol ensures you trust the server
- Software you download is no exception
- However…

Why Sign Software

- Want developer's signature!
- Developer is a whole bunch of people
- ALl right, want some trusted distributor's signature

How To Verify Signature

- App Store / Repository
  - Already done!
- Otherwise, GPG or checksum
  - Not frequently used because of inconvenience
  - Sometimes find it on



Thanks for coming!

- https://tinyurl.com/PerSec3