ACM NetSec

Cybersecurity Made Simple

Personal Security

ACM NetSec, Fall 2017

Confidentiality

Update: Next Week

Facebook Tech Panel:

Monday, October 23rd

Boelter 3400

6:30 PM

https://www.facebook.com/events/1405795962851010/

We will resume Personal Security the next Monday

Agenda

- **Myths vs. Realities**
- Messaging
- Passwords
- Case Studies
- TFA
- ISP's, Browsers, and Personal Info
- Government and Confidentiality

Common Myths

- Nobody cares about my computer
- Who would go through the effort of targeting me?
- It would be obvious if my computer was compromised

Nobody cares about my computer

- "I have nothing worth stealing"
- Personal data, credit card info, accounts
  - What would be the repercussions of just getting a username and password for your Amazon account?
- Some attacks don't steal any of your information, they exploit your need for your own information
  - Ransomware

Who would go through the effort of targeting me?

- Everyone is a valuable target
  - Personal data, contact lists, account info, credit cards
- Sometimes the target is not the individual, but the organization
  - Social engineering attacks rely on human entry points for corporate exploitation
- Attacks are easily automated
  - Spam, embedded links

It would be obvious if my computer was compromised

- When someone takes advantage of your data, they do not want you discovering them

Agenda

- Myths vs. Realities
- **Messaging**
- Passwords
- Case Studies
- TFA
- ISP's, Browsers, and Personal Info

GPG Recap

- Who are you trusting?
    - GPG Software
    - Key Server
    - **Communication Channel**
    - **Receiver of the encrypted message**

- Pretty minimal trust.
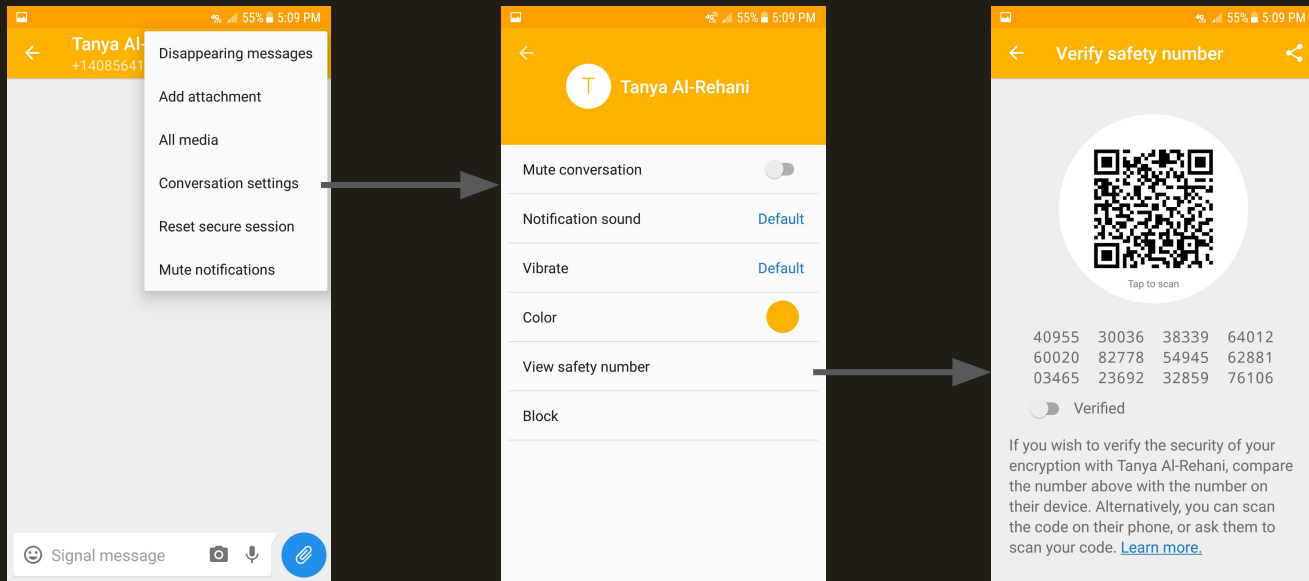- What else can we do this way?

Encrypted Messaging

- Signal/Whatsapp
- How do they work?
  - Similar, except keys are "ephemeral" - temporary
  - In GPG, email + keyID served as an identifier
  - Here, it is your Whatsapp account or (for Signal) your phone number
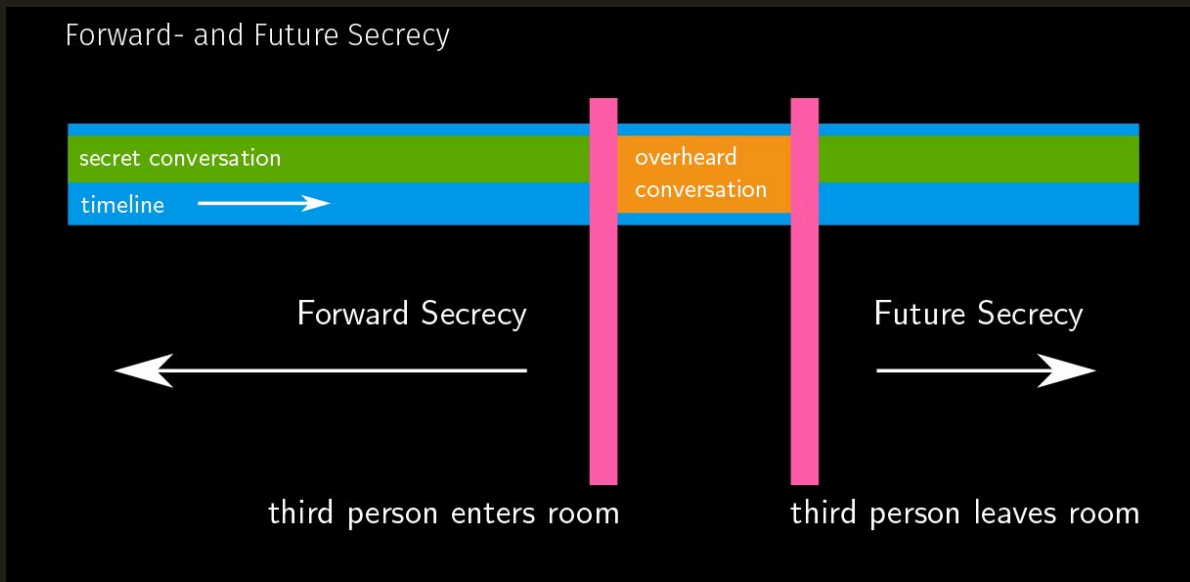- Much harder to do incorrectly than GPG!
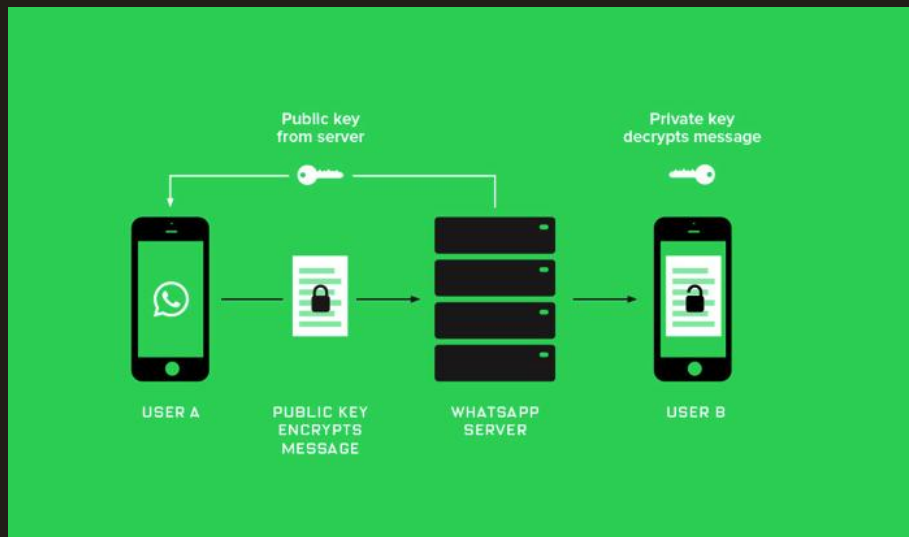
Signal Identity

- ● Security Code
  - ○ Kind of like a GPG key ID - derived using the long term keys

Signal Confidentiality

- Signal also has forward and future secrecy
  - Compromise of a key does not decrypt past messages

Forward- and Future Secrecy

secret conversation

timeline

overheard conversation

Forward Secrecy

Future Secrecy

third person enters room

third person leaves room

- Still vulnerable to metadata collection

Agenda

- Myths vs. Realities
- Messaging
- **Passwords**
- Case Studies
- TFA
- ISP's, Browsers, and Personal Info

Wireshark Demo

Password Hash Algorithms

- One way

- Each input produces a single, unique output

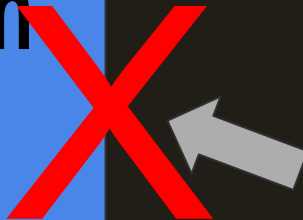- The same input string will ALWAYS produce the same output string

# Workflow for account registration and authentication

1. Create account

2. Password is hashed

3. Upon login, hash is compared to the one stored on database

4. If the hashes match, the user is granted access

5. Repeat 3 and 4

https://crackstation.net/hashing-security.htm#normalhashing

How Hashes are Cracked

Approach 1: Guess the password

1. Guess the password
2. Hash each guess
3. Guess hash = hash?
   a. Yes, you got it!
   b. No, try again

Two Methods:
1. Brute Force
2. Dictionary
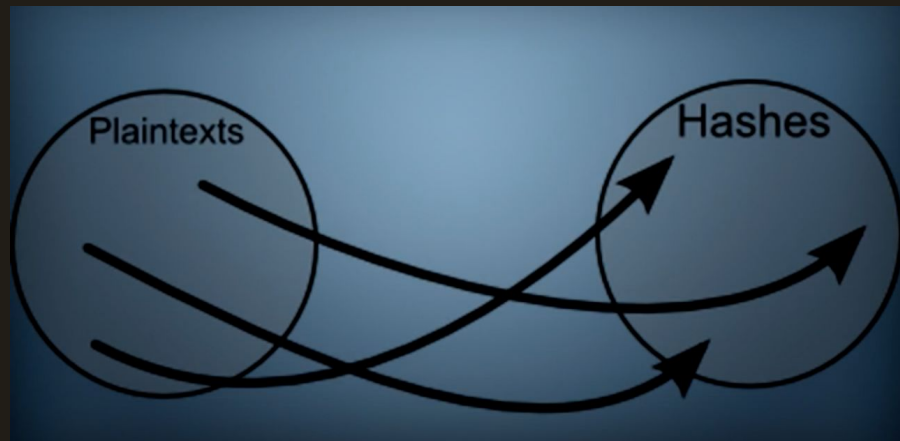
Brute Force Attacks

- Try every possible combination
- Always eventually find the password
- Very computationally expensive
- Inefficient

Brute Force Attacks

"123456789" (9 characters, all numbers)   14.17 minutes

"vacation" (8 characters, all lowercase letters)   2 days

"blUeFisH" (8 characters, mixed uppercase & lowercase)   1.44 years

"r3Dcr0W5" (numbers included)   5.88 years

"%ZBGbv]8" (ASCII included, 8 characters)   45.2 years

"%ZBGbv]8g?" (ASCII, 10 characters)   289,217 years

Dictionary Attacks

- Pulls from "Dictionary" file
- Hash each guess and compare
- Further processing is often applied to the files, such as l33t speak


```
Dictionary Attack

Trying apple        : failed
Trying blueberry    : failed
Trying justinbeiber : failed
        ...
Trying letmein      : failed
Trying s3cr3t       : success!
```

Approach 2: Look it up

- Searchable table
- Search the table to see if the hash is there
  - Yes, you got it!
  - No, you're out of luck
- This process can also be reversed with **Reverse Lookup Tables**
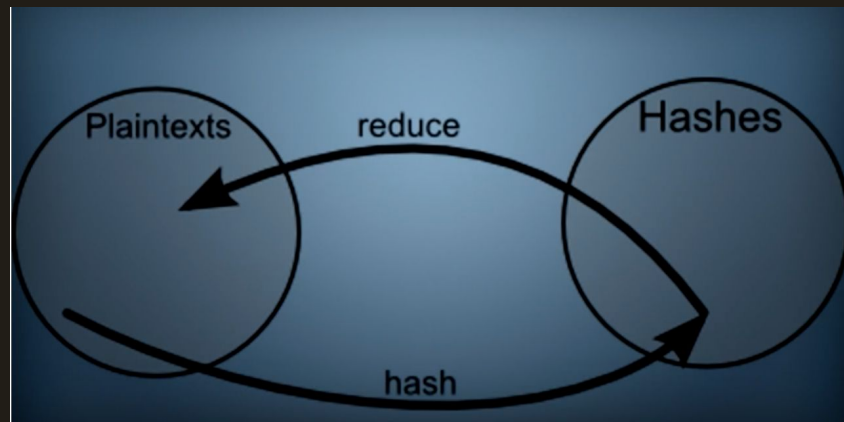
Lookup Tables


```
Searching: 5f4dcc3b5aa765d61d8327deb882cf99: FOUND: password5
Searching: 6cbe615c106f422d23669b610b564800:  not in database
Searching: 630bf032efe4507f2c57b280995925a9: FOUND: letMEin12
Searching: 386f43fab5d096a7a66d67c8f213e5ec: FOUND: mcd0nalds
Searching: d5ec75d5fe70d428685510fae36492d9: FOUND: p@ssw0rd!
```

- Pre-compute the hashes of a certain dictionary
- Look up the hash you're trying to crack

Reverse Lookup Tables

```
Searching for hash(apple) in users' hash list...      : Matches [alice3, 0bob0, charles8]
Searching for hash(blueberry) in users' hash list... : Matches [usr10101, timmy, john91]
Searching for hash(letmein) in users' hash list...    : Matches [wilson10, dragonslayerX,
joe1984]
Searching for hash(s3cr3t) in users' hash list...     : Matches [bruce19, knuth1337, john87]
Searching for hash(z@29hjja) in users' hash list...  : No users used this password
```

- Associate users to hashes
- Use dictionary or brute force to get
- Especially effective because people often use similar passwords

What These Mean For Us

- **Brute Force**
  - Password length
- **Dictionary**
  - Common words/expressions are susceptible
  - Substitutions are accounted for
- **Lookup Tables**
  - Common passwords are at risk

Typical Password Guide

Possible Alternative Solution
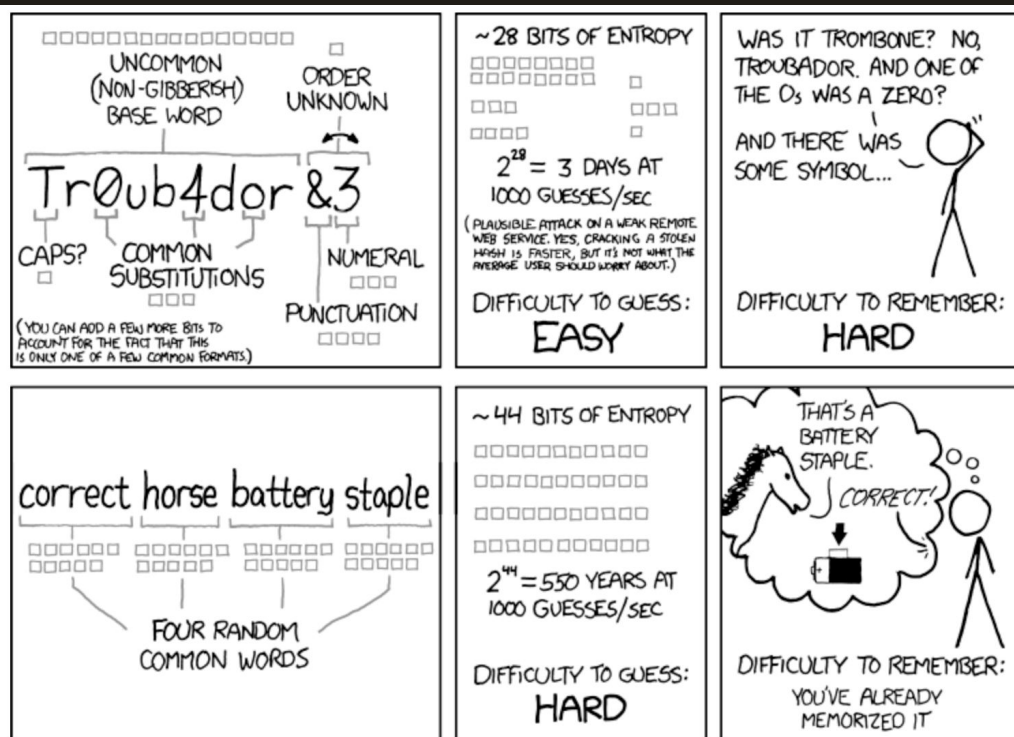
Password Managers

To name a few...

- 1Password
- LastPass
- Dashlane
- Others

Agenda

- Myths vs. Realities
- Passwords
- **Case Studies**
- TFA
- ISP's, Browsers, and Personal Info

[case] LastPass

- Detected breach quickly
- Notified customers
- Only authentication hashes were compromised, no vault data
- Hash algorithms are strong

[case] LinkedIn

- 4 year time gap. Breach discovered in 2012, data released in 2016
- Not all users were notified
- Poor hash algorithm (SHA-1)
- Stored without salt

https://www.troyhunt.com/observations-and-thoughts-on-the-linkedin-data-breach/

[case] Equifax

- Slow to detect and notify consumers
- Difficult-to-find link for checking if affected
- URL Spoof
- Name and SSN are not things you can change, passwords can be changed

Have I Been Pwned?

https://haveibeenpwned.com

Agenda

- Myths vs. Realities
- Messaging
- Passwords
- Case Studies
- **TFA**
- ISP's, Browsers, and Personal Info

Two Factor Authentication for MyUCLA

http://tinyurl.com/uclatwofactor

Agenda

- Myths vs. Realities
- Messaging
- Passwords
- Case Studies
- TFA
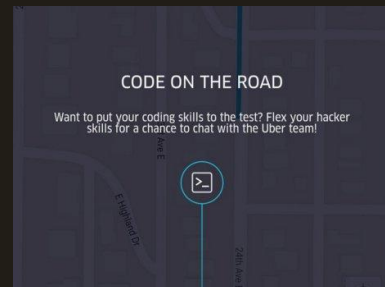- ISP's, Browsers, and Personal Info

Why care?

- Everyone is trying to track your behavior
  - Who you talk to
  - What you look at
  - Where you are
- Used for targeted advertising.
- Maybe you want to keep this private.
- ...Or just avoid creepy targeted advertising

- Most importantly, you should have a choice

How is this done?

- Physical Behavior
  - Wifi MAC address
  - Phone GPS data
- Online Behavior
  - Browser fingerprinting
    - Cookies
    - History
  - IP Address
  - Web page behavior
    - Especially inside of a site
- Optional at-home lab: Wireshark de-anonymization

"Spying billboards" under fire for using phone data to track shoppers

CODE ON THE ROAD

Want to put your coding skills to the test? Flex your hacker skills for a chance to chat with the Uber team!

How to Prevent it?

- Ad Blocker
  - Ads can have access to a lot of browser information, and be tied to other accounts.
  - Traditional - AdBlock, uBlock Origin
  - Smart - EFF's Privacy Badger
  - Nuclear - noscript (just disable everything)
- VPN
  - Disguises IP address from website, but not from VPN
- TOR Browser
  - Nobody knows both the source and destination IP
  - Very slow!
- Be very picky about services you use.
  - DuckDuckGo
  - ProtonMail

Feedback Form and Attendance Code

http://tinyurl.com/PersonalSecurity2