Lecture 10.2
Computer and Network Security

Announcements

- LA-8 due Tuesday
  - Quiz only, 23 questions, (3 misses allowed)
- LA-8 Challenges posted
- Oral Presentation rubric posted
- University News
  - Spring Break
  - Counseling Services (1529 Belmont Street, Norco Building) at (208) 426-1459 or email healthservices@boisestate.edu
  - mood, sleep, feelings of hopelessness or a lack of self worth

Last Time

- Cybercrime Attacks
  - Phishing, Spear-Phishing, Whaling, Vishing, Smishing, Pharming
  - SQL Injection
  - DoS and DdoS
- Cybercrime Examples
- Political Cyber Attacks
- Online Voting

Today

- Passwords
  - Cracking
  - Entropy
- Info Security Best Practices
  - Personal Information
  - Financial Transactions
  - Security Questions
  - Browser Settings
  - Emails
  - Online Accounts
  - Networking
  - Computers
  - Devices

Password Creation

- True random password strength can be measured reliably
- Humans create predictable passwords
  - Any pattern assists crackers
    - Lists of common passwords
    - Natural language online dictionaries
    - Breached databases of plaintext passwords
    - Systematic obfuscation (p@$$w0rd cr@ck3r)
    - Any modified versions of these

Password Fails

- 2020 Top Passwords
  - 123456
  - 123456789
  - qwerty
  - password
  - 1234567
  - 12345678
  - 12345
  - iloveyou
  - 111111
  - 123123
- Other common passwords are:
  - Nothing
  - Secret
  - Password1
  - Admin
- Classics
  - 987654321
  - qwertyuiop
  - mynoob
  - 123321
  - 666666
  - 18atcskd2w
  - 7777777
  - 1q2w3e4r
  - 654321
  - 555555
  - 3rjs1la7qe
  - google
  - superman
  - hello
- 1q2w3e4r5t
- 123qwe
- zxcvbnm
- 1q2w3e
- abc123
- monkey
- letmein
- football
- dragon
- baseball
- login
- sunshine
- master

Password Cracking

- Most modern systems do not store plaintext passwords
- Instead - cryptographic hashes
  - MD5, SHA, etc.
  - SHA256(admin) => b86a4d73ea36be60f4f416644e0b1386c40043819d75cd037ddfb9c109a18c53
- Online – submit guesses to server
  - Very slow, not feasible for brute force attacks
- Offline – steal database of hashes
  - Hash guesses and compare values
  - Relatively fast
  - 2007: 112k guesses/sec
  - 2020: 17M guesses/sec
  - Pre-compute many values for faster comparisons
    - Dictionaries
    - All short passwords
    - Rainbow tables – method of compressing space tradeoff

Password Strength

- Strength measures average attempts to guess
- Information entropy of password given by:

  N = number of possible symbols

  L = length of password

  $H = \log_2 N^L = L \log_2 N$

- Example: string of four [a,b] characters

  N = 2

  L = 4

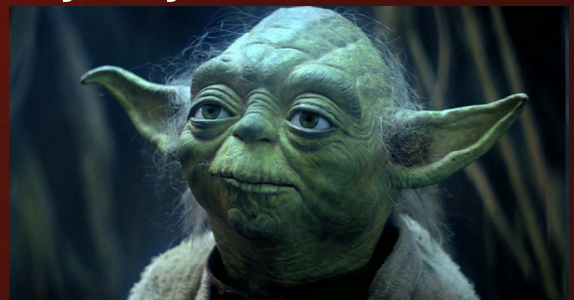
  Number of guesses $N^L = 2^4 = 16$

  [aaaa], [aaab], [aaba] ... [bbba], [bbbb]

  $H = L \log_2 N = 4 \log_2 2 = 4$

Password Entropy

- How much entropy do we need?
  - Assume worst case offline guesses
    - 20M/sec = ~1.7T/day = ~630T/year
    - 63P guesses in 100 years
  - N^L = 63P
  - H = 55.8
  - N=2 => L = 56
  - N=26 => L = 12
  - N=52 => L = 10 (H=9.8)
  - N=62 => L = 10 (H=9.4)
  - N=96 => L = 9
  - N=96 and L=20 => H =131.7 => 7.01Y years (y = yotta)



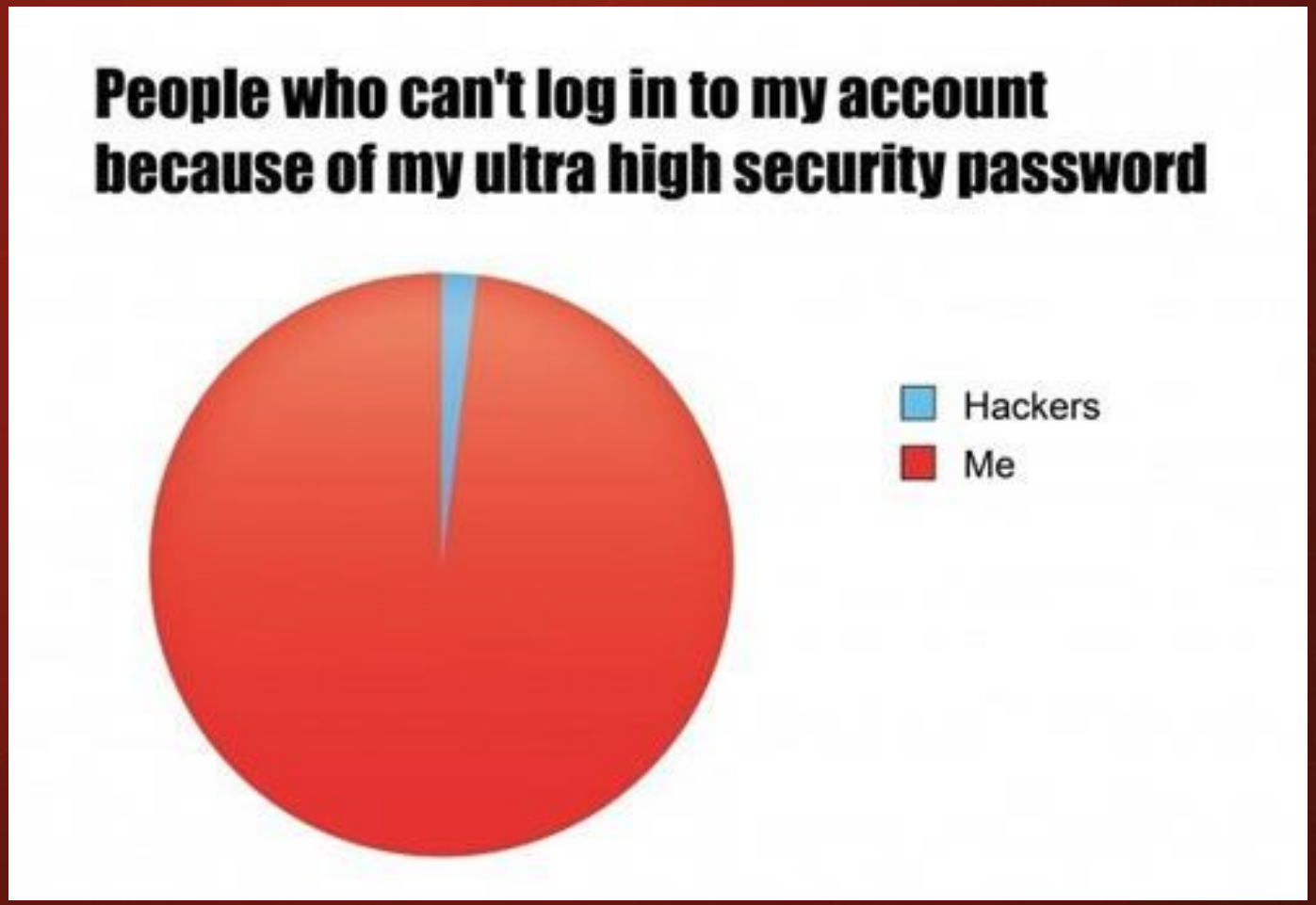
Password Entropy

- N=52 L=10 H=~55.8 Time=100 years
- Assumptions
  - Truly random N
  - 100 years *worst case*
  - Non-distributed cracking
  - Non-quantum
- Using 10-letter word in your password removes randomness
  - N=35529 L=1 => H= 15.1 Time=0
- Substituting numbers for letters removes randomness:
  - p@ssw0rd
- Using common sequences removes randomness:
  - rotflmao
- Using numbers removes randomness:
  - Admin763
- Mask attack exploits known patterns:
  - N=96, L=9 => H=55.8, 100 years
  - XxxxxxxNS mask: $26x96^{6}x10x34$ => H=52.6, 11 years

Password Entropy

- N=52 L=12 H=~55.8 Time=100 years
- ~ 1,000,000 English words
  - Average adult knows 20-30k words
- N=10,000 L=4 H=~53 Time=15 years
  - Random selection => use dice?
  - Five dice => 6^5 = 7776 wordlist
  - N=7,776 => L= 4 H=~51.7 Time=6 years
  - Roll 5 dice lookup word, repeat 4 times:
    - crane mustard jump repose
    - Easy to remember, easy to type
  - Alternative:
    - Random sentence from song, movie, book
    - Ifoughtthelawandthelawwon
  - Many accounts have max limit, password policies
    - ifotdelawndelaw1
    - iftlatl1

Password Best Practices



Password Best Practice

- Best: Password Manager
  - Generates truly random with all policies
  - Protect with long memorable phrase
  - Easy to cut and paste into websites
- Otherwise:
  - Use minimum 10 characters
  - For shorter passwords (8-15) characters use mixed case, numbers, and symbols *randomly*
  - *Never* reuse a password
  - Do not use personal info to derive password
  - Do not use dates (pattern-based)
- Use MFA wherever possible

Personal Information

- SSN, Drivers License, School ID, Middle Names, Financial and Medical Accounts
- Use need-to-know policy
  - Give as little info as necessary
    - Only use middle names when needed
    - Do not give SSN, DL to retailers, online accounts
- Be careful with offline info
  - Only carry minimum cards you need
  - Shred or cutout sensitive info before discarding
  - Move to online documents whenever possible

Financial Transactions

- Scammers have successfully performed man-in-the-middle email financial thefts
  - Victims purchasing house receive instructions for wiring payment
- Best Practices for Online Financial Transactions
  - Double check who sent you an email
  - Telephone the bank or recipient and confirm account numbers
  - For large amounts, transfer a smaller amount and confirm receipt with the company
  - Never send personal or banking details over email
  - Be suspicious of requests for financial or personal information
- Setup alerts on all financial accounts for suspicious activity

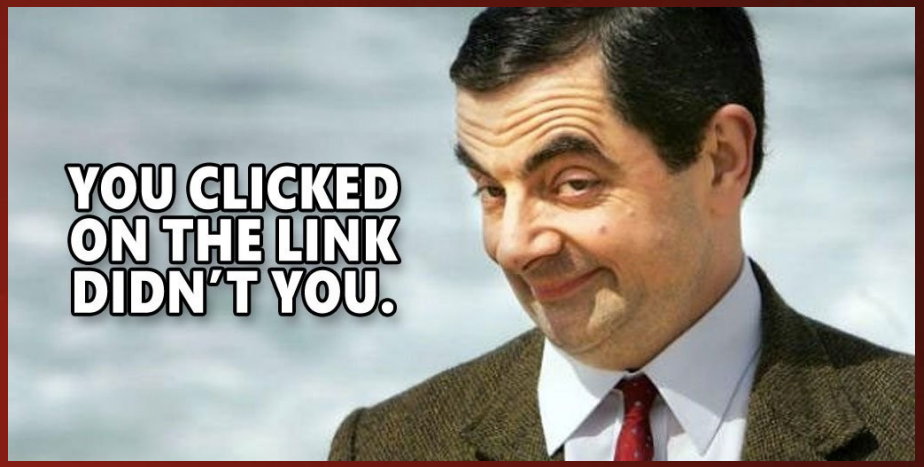
Security Questions

- Sites often require security questions when resetting a password
- Do not use real answers based on personal information that can be discovered
- Answers are not passwords – do not need entropy
- Decide on a method for deriving answers only you know but easy to remember
- Example:
  - Citibank: What was the make of your first car?
  - Site+fantasy car => CitibankFerrari
    - Unique to each site so cannot be stolen and reused
    - Stronger method would be harder to decipher and generalize

Browser Settings

- Keep browser up-to-date
- Regularly review plug-ins and extensions
  - Delete unused/unwanted
- Use HTTPS whenever available
- Only cache passwords on your private computer
- Disable pop-ups
- Use encrypted cookies
- Consider AdBlock or NoScript
- Disable automatic downloads to defeat drive-by phishing
- Consider not using Google Chrome
  - Good security
  - Bad Privacy
  - Closed source
  - Alternatives: Firefox, Brave, IceDragon, Tor, Safari

Email



- Do not open attachments
- Do not click on links
  - Hover over link to see URL
  - Copy/paste to browser – inspect before accepting
- Do not assume From is correct
- Do not send opt-out to spam
- Make sure your mail settings are secure:
  - Connection use SSL/TLS or STARTTLS
  - Authentication use Encrypted Password

Online Accounts

- Facebook
  - Turn off Manage Future Activity
  - Turn off Face Recognition
  - Disable third party app tracking:
    Settings→Apps and Websites→ Active
  - Unlink your profile from search engines:
    Settings→ Privacy → Do You Want Search Engines Outside of Facebook to Link to Your Profile?
  - Tune your post privacy: Settings→ Privacy
  - Turn off targeted ads: Settings→ Ads → Ad Settings → Ads that include your social actions = No One
  - Avoid Like and Share buttons on the web

Online Accounts

- Google (myaccount.google.com)
  - Privacy and Security Checkup
  - Consider turning off Web and App Activity
    - Turns off all tracking
    - Degrades user experience significantly
    - Alternative: Set automatic data deletion after 3 or 18 months (data has already been leveraged)
  - Consider turning off location history
  - Consider turning off Ad Personalizations
  - Use 2FA

Networking

- Beware of WiFi honey pots
  - Scammers setup phony HotSpots: „Starbucks Free WiFi”
- When using open WiFi data is in the clear
  - Airports, Hotels, etc.
  - Use one of these options:
    - Use VPN (encrypts all traffic)
    - Ensure HTTPS, secure cookies, eMail settings, etc.
    - Incognito browser and no personal sites
- ISPs track users
  - Consider VPN

Computers

- Use disk encryption
- Wipe disk before discarding computers
- Enable auto-updates
- Use anti-malware software if necessary
- Configure firewall settings
- Turn off all unused services/daemons
  - SSHD, HTTPD, telnet, etc.
- Password protect removable media

Protecting Your Internet-Connected Devices

- Make sure you've installed latest security patches.
- Before buying an Internet-connected device, see if manufacturer is taking reasonable security precautions.
- Immediately change the default password of devices you connect to the Internet.
- Choose a different password for each of your devices.
- Consider replacing insecure Internet-of-Things devices.

Summary

- Be proactive for security and privacy
- Be protective of your personal information
- Use good security hygiene for all your accounts
- Use strong passwords and MFA

Next Time

- Computer Reliability
  - Read chapter 8