

# Passwords Bloody Passwords

Steve Hanlon - Lot 592

[mrpc@hanmade.com](mailto:mrpc@hanmade.com)

494-2847

# Agenda

- General info about passwords
- Some password mgmt strategies
- "Bad Guy" Scenarios
- How to make a strong password - the best strategy

# Top 20 Passwords of 2013

1. 123456 (Up 1)
2. password (Down 1)
3. 12345678 (Unchanged)
4. qwerty (Up 1)
5. abc123 (Down 1)
6. 123456789 (New)
7. 111111 ( Up 2)
8. 1234567 (Up 5)
9. iloveyou (Up 2)
10. adobe123 (New)
11. 123123 (Up 5)
12. admin (New)
13. 1234567890 (New)
14. letmein (Down 7)
15. photoshop (New)
16. 1234 (New)
17. monkey (Down 11)
18. shadow (Unchanged)
19. sunshine (Down 5)
20. 12345 (New)

# My most favorite hack

```
foreach $user [on the network]
  while read pass;do
    rlogin -u $user -p $pass >> hack_file
  done < /usr/share/dict/words
end foreach
```

In 1989 with this simple program I was able to log into 250+ machines on a 400 machine network.

**Yes, I am a  
dangerous  
fellow**

# What's the Problem With Passwords?

- You need to have way too many
  - It would be nice if EVERYTHING trusted your Windows logon...
- You are allowed to choose weak passwords
  - sh34266 is not a good password
- You are confused which one to use
  - Wait, is this the one for FB? Or the Bank? Gmail?

# What's the Problem With Passwords?

- You can't remember the one you want
- You use the **SAME** one too often
  - very bad as it turns out
- You are freaked out by all the "hacking" in the news
  - your only real defense is a **STRONG** password

# Why is This So?

- There are no web password standards
- You are ***forced*** to use too many
- It's too easy to recover your password
  - and, of course, you forget the new one instantly
- You are lazy (secret: I'm lazy too)
- You don't understand this security stuff **\*\*AT ALL\*\*** (and why should you?)



# Your Daily Story of Passwords...

- You log into your Windows PC with one
- You bring up Facebook (with a "keep me logged in" feature)
- You access your email via a browser (with a "keep me logged in" feature)
- You log into your bank with a typed password every time - there is no "keep me logged in" feature

# But What Really Happened?

- Your Windows password can be really weak
- Your Facebook and email passwords are "remembered" - meaning that you are eventually going to forget what they are
- Or your browser stores an encrypted version of your password and stuffs it into the login field

# What is a Password Exactly?

- A string of text that only you know
- Is (or should) always be transmitted and stored strongly encrypted

You type into Amazon:

\*\*\*\*\*

(sh34266)



Gets stored at Amazon as:

*176qBlrxAuBbs\_otbTy7O\_WQd20JIF*

(using Military-grade encryption)

# Password Encryption...

...is serious business at serious companies like Amazon, Google, eBay, Citibank, etc

- Some of the smartest computer science people work in the field of encryption
- So you can trust that your strong\*\* password will be impossible to crack algorithmically

\*\*sh34266 is not a strong password

# Password Problems & Solutions

It's simple really. Write them all down!

- On a hidden piece of paper
  - but NOT in the rolodex
- Store them in a PC text file
  - So long as you have a strong Windows password
- Consider using a password mgmt program
  - **LastPass** gets high marks

# More Solutions...

I say this every month - use Google Chrome!!!

- Let Chrome "remember" as many passwords as your can
- Stay logged into to your Google Account to "sync" your passwords
- ***Having Chrome remember your password is never an excuse for not writing it down***

# "Bad Guy" Scenario #1 - Break In

You have a hidden paper copy with passwords and your PC is stolen.

- No bad guy is going to find your passwords
- Your Windows password is strong so it can't be broken into easily
- If you are using Chrome change your Google password - just in case
- Your passwords and logon info are safe

# "Bad Guy" Scenario #2 - Break In

You have a file on your PC with passwords.  
Your PC is stolen.

- Your Windows password is strong
- No normal bad guy is going to get into your PC
- You might consider encrypting the hard drive with Microsoft BitLocker



# "Bad Guy" Scenario #3 - Hack In

You write them in file stored in the cloud  
(Google Docs, Dropbox, etc)

- No bad guy is going guess or recover your strong password to Google/Dropbox
- Your passwords are safe

>>>> This is what Mr. PC does <<<<



# Example: "Target" Hack Analyzed

- Bad guys steal a database of 140 million encrypted passwords
- Bad guys have 1,000s of PCs on hand to crack these encrypted passwords
- Your password can be cracked in seconds or years... Lets see what makes a strong password!

# What Makes a Strong Password

- One word **Entropy**
- In computer speak it's called **randomness**
- This is something that can actually be calculated for YOUR password in advance
- Bad guys don't merely guess - they use word dictionaries first
- Longer is usually better - not always

What you might ***think*** is a strong password may not be so strong

<p>□□□□□□□□□□□□□□ □</p> <p>UNCOMMON (NON-GIBBERISH) BASE WORD      ORDER UNKNOWN</p> <p><b>Tr0ub4dor &amp; 3</b></p> <p>CAPS?      COMMON SUBSTITUTIONS      NUMERAL      PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)</p>	<p>~ 28 BITS OF ENTROPY</p> <p>□□□□□□□□ □ □□□□□□□□ □ □□ □ □□□ □□□□ □</p> <p><math>2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: <b>EASY</b></p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p>  <p>DIFFICULTY TO REMEMBER: <b>HARD</b></p>
<p><b>correct horse battery staple</b></p> <p>□□□□□ □□□□□ □□□□□ □□□□□ □□□□□</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~ 44 BITS OF ENTROPY</p> <p>□□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□</p> <p><math>2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>DIFFICULTY TO GUESS: <b>HARD</b></p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p>  <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

# Why "password" is a bad password

- Brute-Force attack:
  - $16 \cdot 1 \cdot 19 \cdot 19 \cdot 24 \cdot 15 \cdot 18 \cdot 4 = 9,980,928$  guesses
  - p:16, a:1, s:19, s:19, etc
  - about 3 hours to guess @ 1,000 guesses / sec
- But first I would just search a dictionary list of words. "password" would be around the 90,000th word.
  - About 9 seconds to guess.

# So... If you have a weak password...

- If Target had your encrypted weak password
  - it would take **Bad Guys** about 9 seconds to log into your target account.
- But we all know that using the password "password" is really dumb.
  - But are the passwords I use actually safe?
- Lets see!!!

# Is My Password Strong???

Test your passwords here:

<https://www.cygnius.net/snippets/passtest.html>

- This a very sophisticated strength analyzer.
- In fact, a perfect tool for building your next password.
- Let's try it!!!!

# A sample password

All the names of the dogs I had as a kid living with my parents

- ***Impossible*** to guess
- ***Impossible*** to forget

GingerSgtPuffSamCandy



# A Sample Password Con't

- So, is "GingerSgtPuffSamCandy" a strong password? You Betcha!
- That password generates "entropy" worth:

3,637,191,867,955	trillion seconds
60,619,864,466	billion minutes
1,010,331,074	billion hours
42,097,128	million days
115,335	thousand years to crack

# How Many Passwords Should I Have?

- Certainly more than one
- Depends on the company that is storing it and the value of the data protected by that password
  - Amazon, BankofAmerica, Gmail get the strong ones
  - Facebook less strong but different
  - Windows 7, 8: strong but different

# Other Password Issues

- "Keep me logged in" - this could be bad if your PC is stolen and you don't use a strong Windows password
- Weak "Security Questions" for password recovery
  - make it hard to guess
  - make your own question if possible

# Password TODOs

- Verify your banking security questions
  - And strengthen weak passwords for valuable data e. g., banks, brokerage accounts, email etc
- Upgrade all your most-used passwords and security questions
  - FB, Gmail, Yahoo mail, etc.
- Write down and hide all passwords
  - on paper or online