



AVOID BEING HACKED: A SUPER FAST PRIMER

BY JESSE HOMA AND PAUL BEASLEY

ATTACK VECTORS

Lots of ways for bad guys to get in- let's focus on three:

- Password Issues
- IoT Security
- Wireless Weaknesses



PASSWORD ISSUES

- Password uses
 - Authentication
- Verify current open threats
 - Email Address
 - Passwords
- Attackers will use the breaches of others against you
- Check here:

haveibeenpwned.com



Home Notify me Domain search Who's been pwned Passwords API About Donate

;-)have i been pwned?

Check if you have an account that has been compromised in a data breach

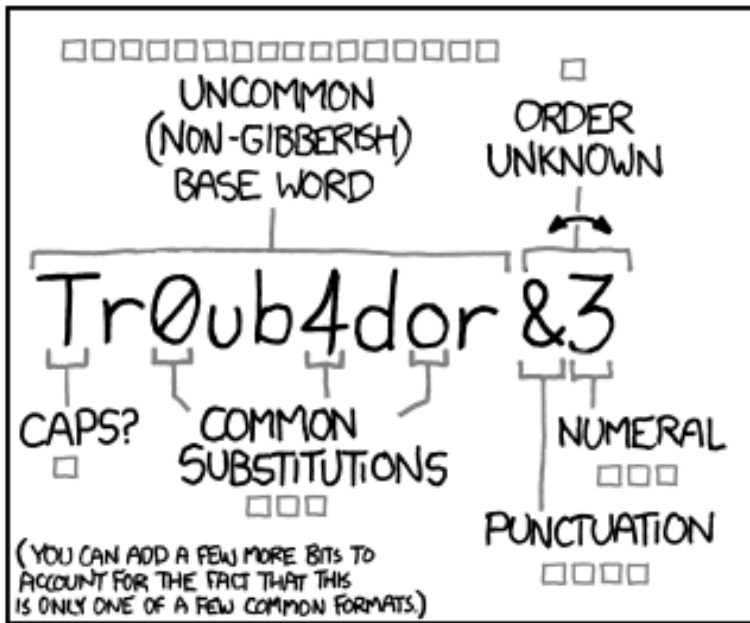
email address or username pwned?

229	4,000,536,425	53,481	50,687,074
pwned websites	pwned accounts	pastes	paste accounts

PASSWORD ISSUES

- The Man Who Wrote Those Password Rules Has a New Tip: N3v\$ŕ M1^d!
- New NIST Recommendations
 - NIST SP 800-63B
 - Appendix A
- Single-Factor Authentication
- Multi-Factor Authentication





~28 BITS OF ENTROPY

□□□□□□□□

□□□□□□□□

□□□□

□□□□

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

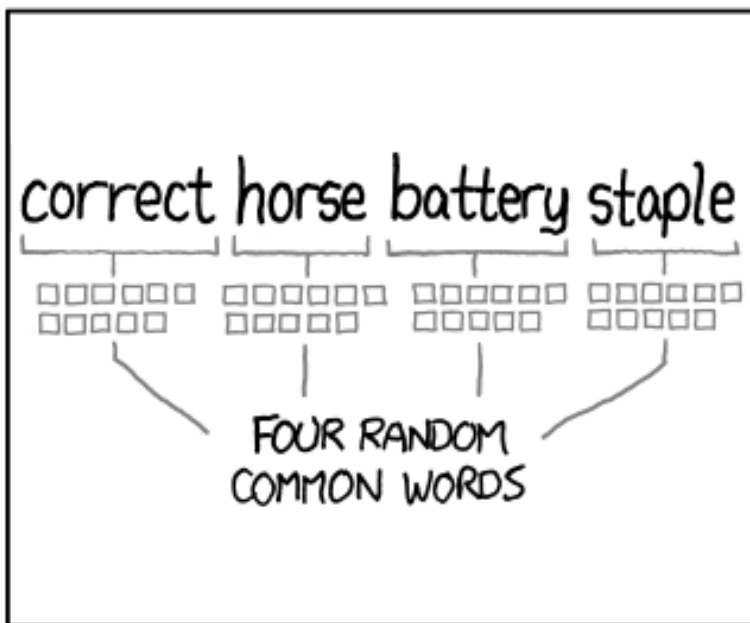
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

□□□□□□□□□□

□□□□□□□□□□

□□□□□□□□□□

□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

UPDATED GUIDELINES

- Complexity < Length
- No periodic password resets
- Enable “show password while typing”
- Allow paste in password fields
- Forbid commonly used passwords
- Don’t use password hints or knowledge-based authentication
- Limit number of password attempts
- Multi-factor authentication / SMS based concerns



PASSWORD TIPS

1

Don't rely on passwords alone to protect anything you value. **Turn on multi-factor authentication wherever possible.**

2

Use a phrase with multiple words that you can picture in your head, so it's difficult to guess but easy to remember.

3

Protect your most important accounts, like banking and primary email, by giving each a **unique passphrase**. A password manager can help.



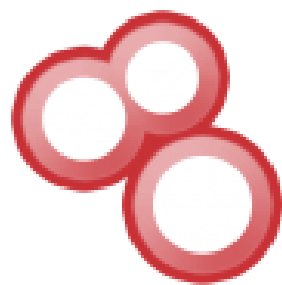
Password:



IOT SECURITY

Things to look for:

- Known good device security
- Firmware updates
- Network segmentation
- Firewall rules
- Research device vulnerabilities
 - Google Hacking Database
 - Shodan (for existing IoT)



SHODAN



DCS-900

ActiveX

Java

Setup

WTF DUDE CHANGE THE PASSWORD 2015-07-16 02:31:27



Home | Setting

26:38





DCS-900

ActiveX

Java

Setup

DCS-900 [5C64FA]

2017-10-16 11:13:15

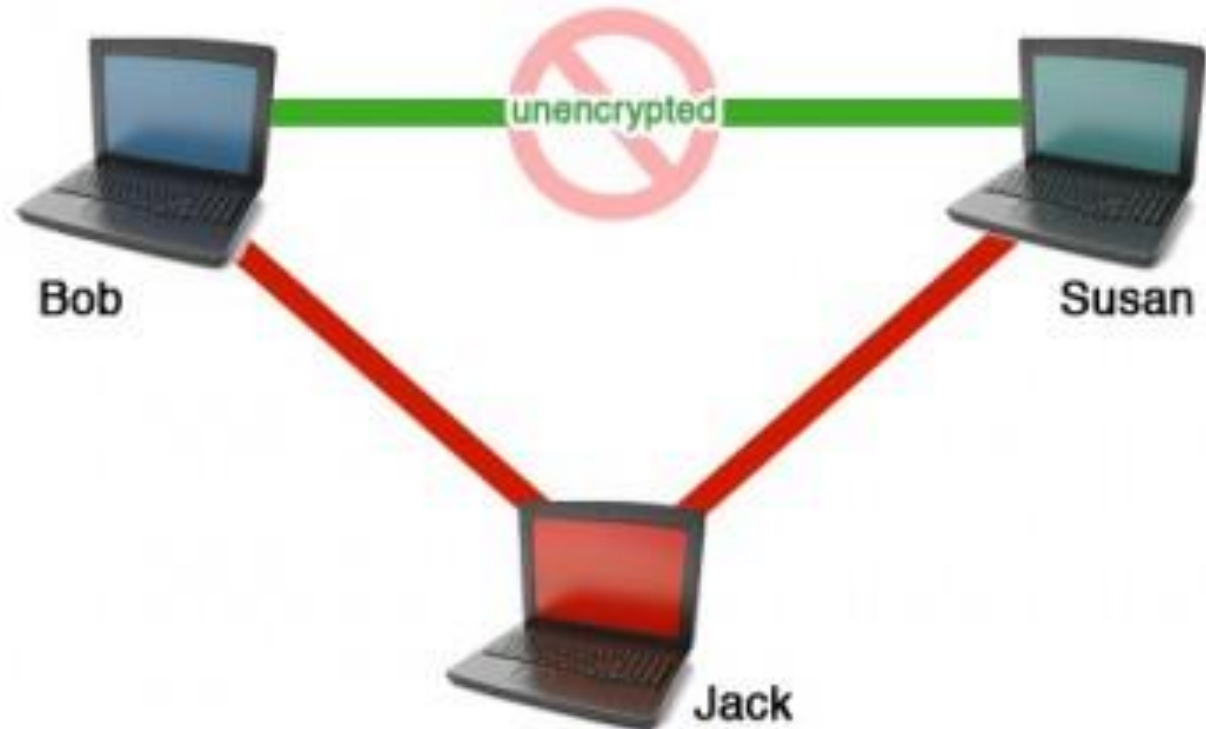


Live View



WIRELESS WEAKNESSES

- Man-in-the-middle attack
 - Compromised communication
 - Record and manipulate in transit data
 - Hard to detect



WIRELESS WEAKNESSES

- Wireless Eavesdropping
 - Create fake access point
 - Encourage users to connect
 - Record sessions
 - Manipulate data to compromise users



WIRELESS WEAKNESSES

• Wireless Connections

- Remembers previous connections
- Attempts to reconnect
- Attackers can use this data



SECURING AGAINST WIRELESS ATTACKS

- Avoid open wireless connections
- Avoid Auto-Connecting to hotspots
- Encryption when available
- VPN service





THANK YOU



JHOMA@CYBERADVISORS.COM



WWW.CYBERADVISORS.COM