W. Ian Blanton

W. "Ian" Blanton is the founder/Owner of Tizite Consulting, dedicated to leveraging Apple technology to bring top-notch IT Consulting to individuals and organizations in Eastern Mass (and elsewhere).

Ian has a 26 year background in IT, and has supported Mac/iOS in military installations, one-person design shops, pharmaceutical corporations and non-profits since 1991.

Security, Viruses and Malware.
It's real. It's now.
You need to take it seriously

Where we discuss the History, Threats, and What You Can Do About Them.

The One Ring of Security

Perfect Security

- Security is a trade off between convenience and safety
- You have to work with your clients/users to determine what level of security you and they are comfortable with.
- You have to be willing to say "no", sometimes.

“I thought the Mac was immune to viruses”

- Macs are not magically immune to malicious software.
- Malware hasn’t been kids making viruses “because they can” for some time - it’s big business, with real potential damage.
- The malware problem on Mac OS X is nothing like as bad as it is on Windows.

Viruses, the history of viruses coming to our platform

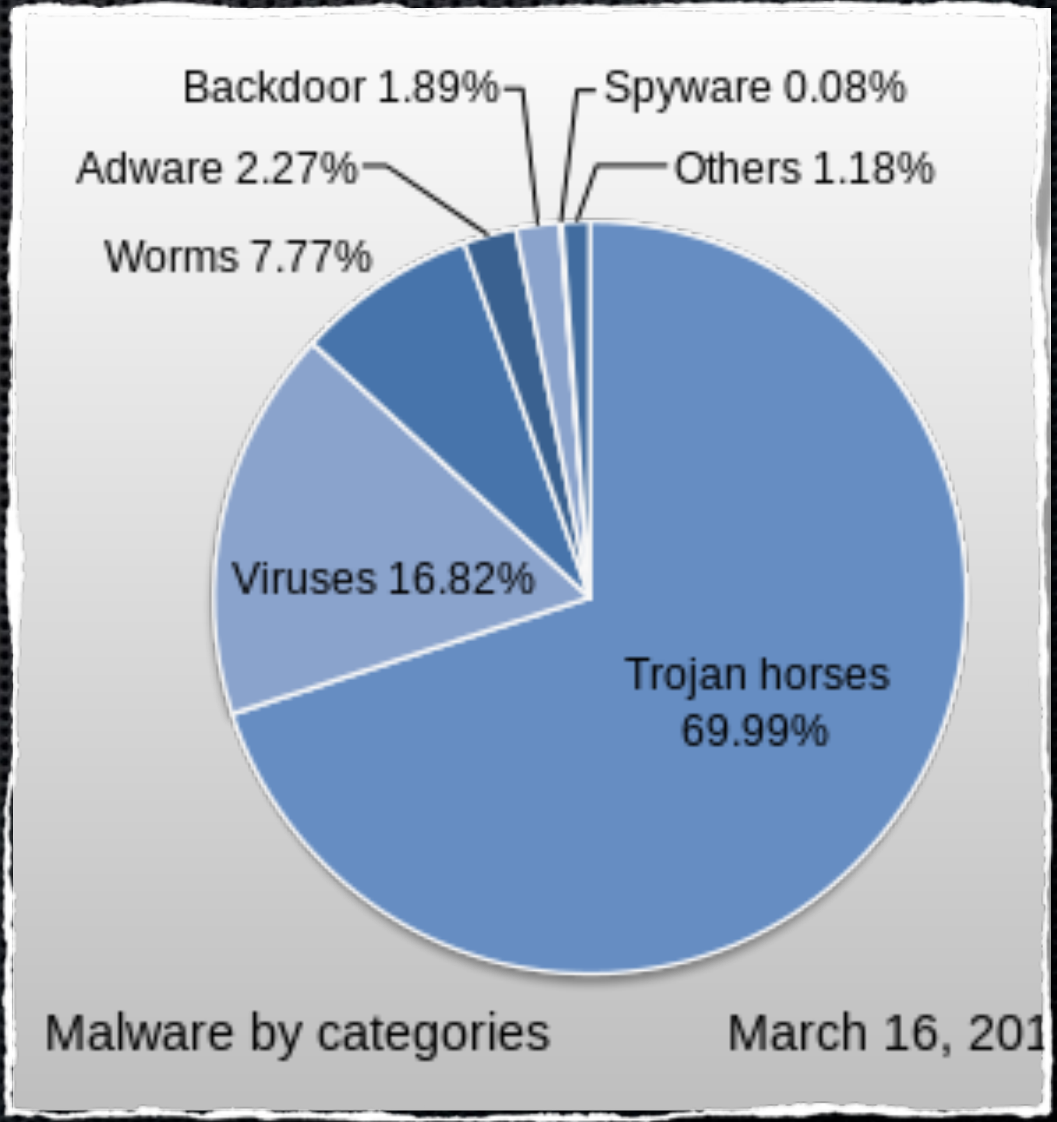
- Malware: From the early 1980s.
- 1980's forward, Being an uninfected carrier
- Mid 1990's forward, Word Macro Viruses
- AdWare: First appeared in 2012
- First widespread Trojan horse appeared on Mac in 2011 (MacDefender)
- Widespread use of malicious RAT (Remote Admin Tool) software - 2012

Moving from complacent to vigilant one decade at a time

- 1980's - Most truly negative effects were "side effects" of software.
- 1990's - Malicious software had single use/aim.
- 2000's - Malware becomes big business, with mutiple goals/aims.
- April 2015 - Simda botnet, containing 770,000 (Windows) PC's shut down by authorities.

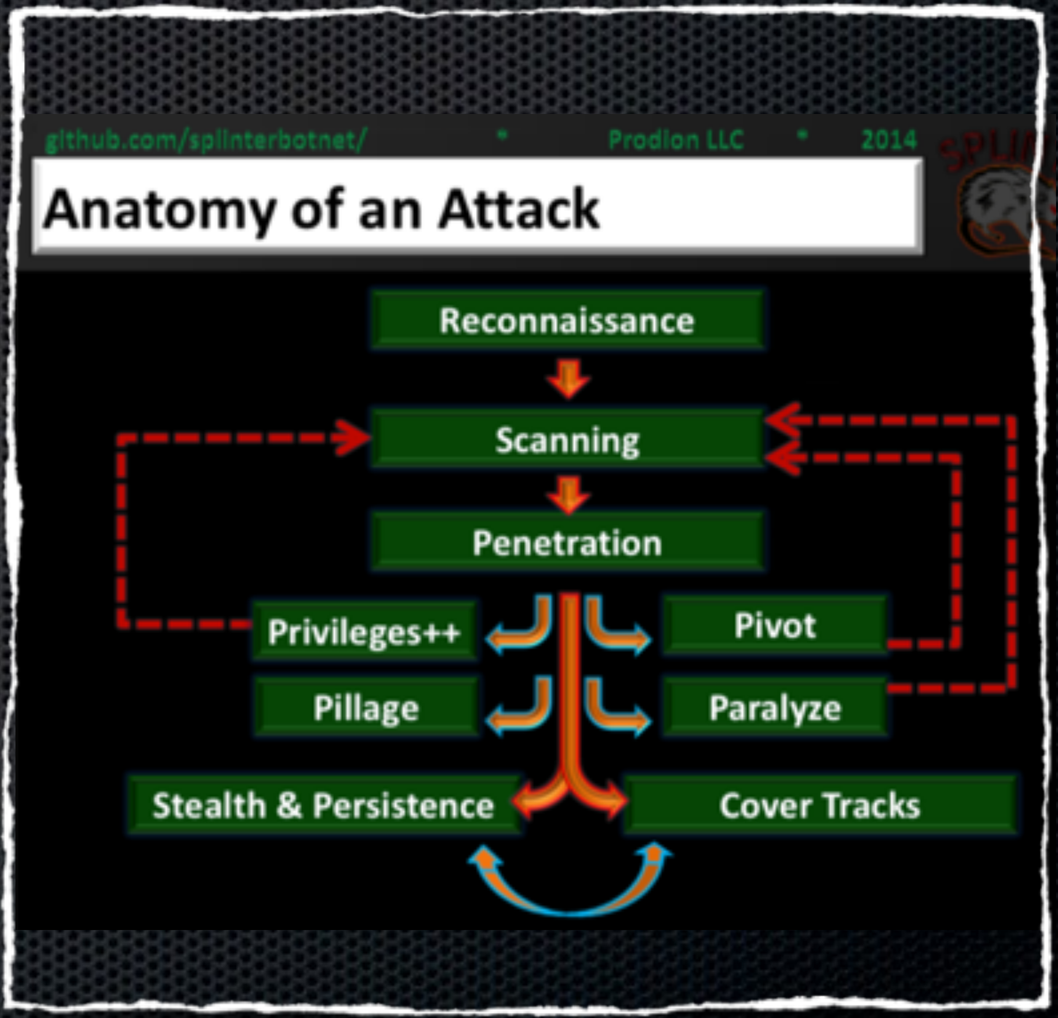
What's the Difference?

- Malware
  - Trojan Horses
  - Viruses/Windows Viruses
  - AdWare



So, what do they do?

- Data Loss
- Botnet (Zombie Nets)
  - DDOS
  - Spammers
- Keyboard logging
  - Credit Card Theft
  - Passwords
  - Loss of Trade Secrets/Private information
- RATting
  - Webcam & full system control
  - Blackmail
  - Extortion



github.com/splinterbotnet/ * Prodion LLC * 2014

Anatomy of an Attack

Why Secure Systems?

- Invasion of privacy.
- Loss of trade/company secrets.
- Impact on work/productivity/performance.
- Legal liability for data breaches.
- Blackmail/Extortion.

Layers of Security (Simplified)

- 1st layer - Firewall & Network Security
- 2nd Layer - System/Physical Security and User Policies.

What do I secure?

- Network Security.
  - Firewalls
    - Malware, Trojan Horses and Virus protection.
  - VPN
- System/Physical Security.

What do I secure?

- Network Security.
- System/Physical Security.
  - Malware, Trojan Horses and Virus protection.
  - Password Policies.
  - Firmware Passwords
  - Device Encryption
  - Password Policies

Developing a strategy

- Define the needs
  - Individual users
  - Small groups
  - Larger Deployment
- Identify the best software for your specific environment
- Determine your strategy (ex: Server Malware scanning v. Desktop)
- Provide training/user education for the system you deploy

Using monitoring software to report problems

- Protection services (Firewalls, Network Security Appliances)
- Management software such as Watchman Monitoring detects malware and notifies you

Firewalls/Network Security

- First Defense against Malware and system intrusions.
- VPN’s to secure external users connections.
- EMail Continuity and Spam scanning.

Firewalls

- How they work.
- Should be your first line of Defense against Malware.
  - Any business level firewall - Cisco, Dell SonicWALL, Watchguard.
  - OS X Built-in Firewall - a last resort.

VPNs: Why you need them

- Basic architecture
- Simplest implementation for a small business
- Using a Router/Firewall to host a VPN
- Using OS X Server to host a VPN

Email Continuity, Spam and Virus filtering

- MXlogic
- SpamSoap (now Nuvotera)
- eVitera
- Barracuda's ESS
- Network appliances

System/Physical Security

- First place to secure, should be last layer to be dealing with Malware.
- Password Protection & Policies
- Data Encryption

“Do you have a backup?” means “I can’t fix this.”

- Maxim 41, “The Seventy Maxims of Maximally Effective Mercenaries”

Follow the 3-2-1 rule of backups

- 3 copies of anything you care about - Two isn't enough if it's important.
- 2 different formats - Example: Dropbox+DVDs or Hard Drive+Memory Stick or CD+Crash Plan, or more
- 1 off-site backup - If the server and drives was stolen, how useful will your backups be?

OS X - System Protection

- Firmware Passwords
- Whole Disk Encryption
  - Built-In “File Vault” (10.7+)
  - Third Party (PGP Desktop or Symantec Endpoint)
- Anti-Virus
  - Current Mac Security threats
  - OS X as potential "Typhoid Mary" for Windows-based viruses

iOS - System Protection

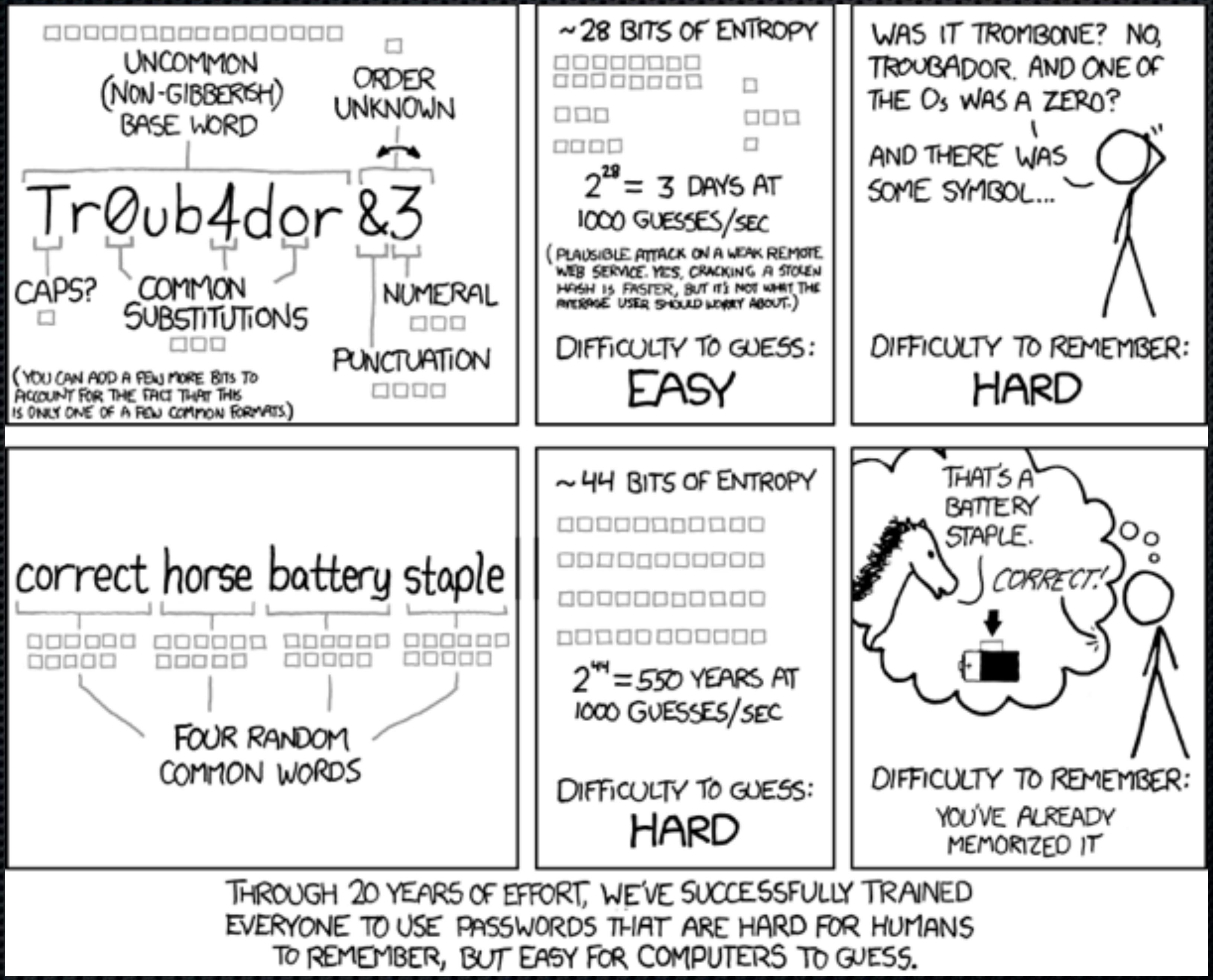
- Device Passcodes and Auto-wipe
- Hardware Data Encryption
- Encrypting iOS Backups.
- Touch-ID
- Remote Wiping

Password Policies & Management

- Password policies are where the "rubber meets the road" in defining good policies.
- If your users are writing their passwords down, your policy needs work.
- Leverage Password Management software along with user education.
- Longer passwords/pass-phrases as primary passwords (System/admin passwords) and use Password management software to handle the rest.

Correct, Horse Battery!

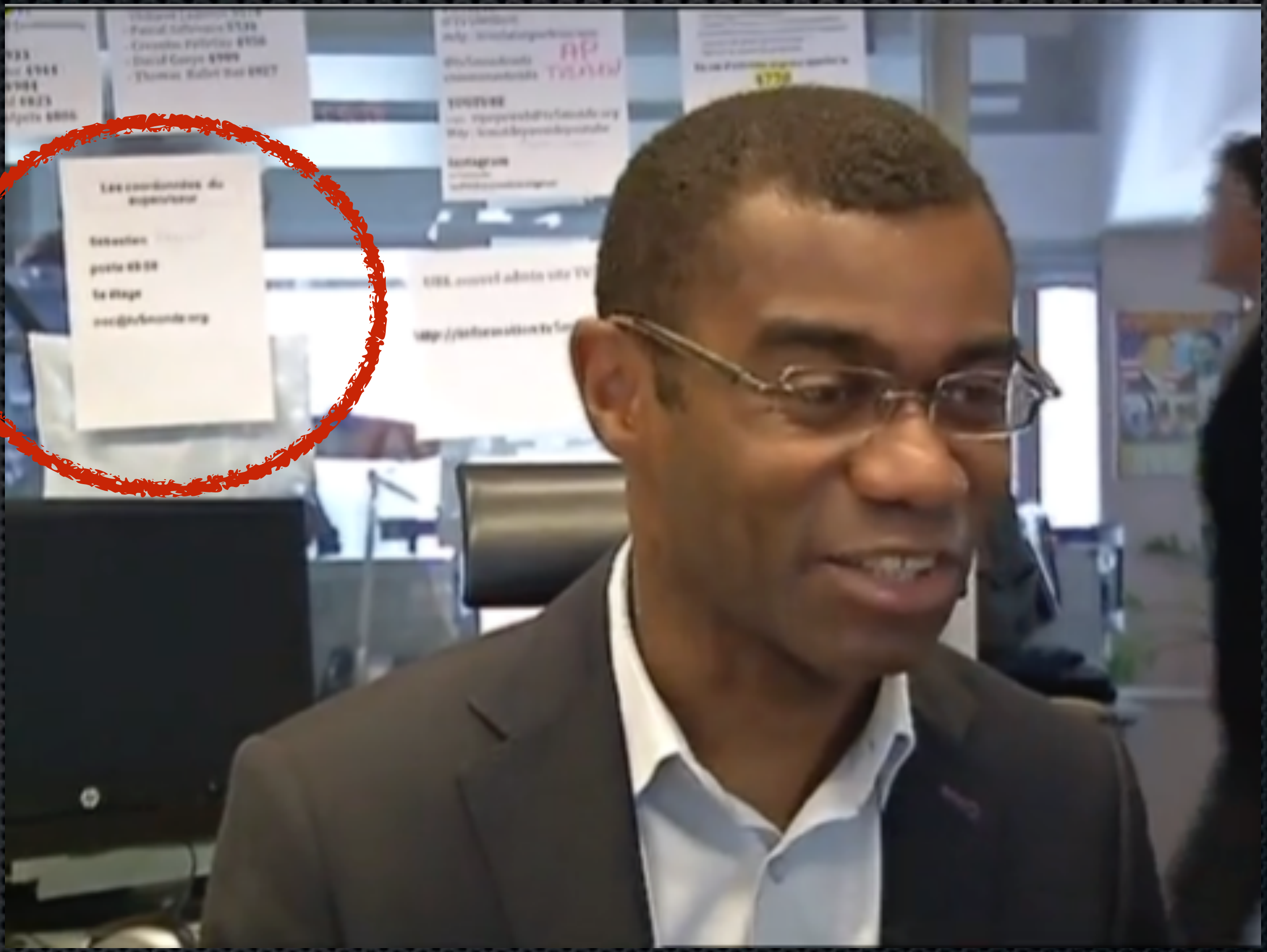
http://xkcd.com/936/


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 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 Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

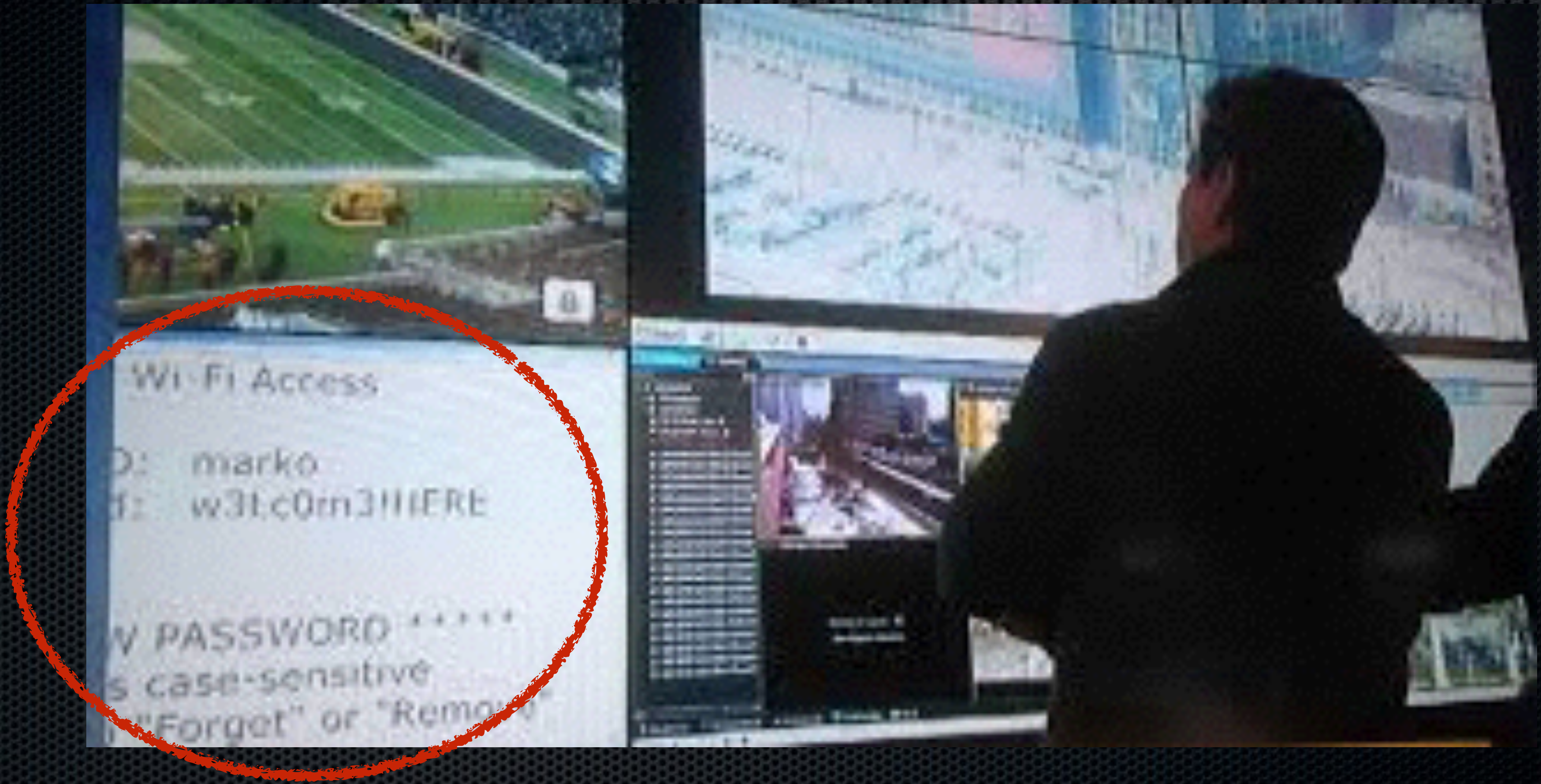
Length is everything.

- Encourage the use of pass-phrases, rather than passwords.
  - Randomly Generated pass-phrases.
- Use a password manager -- choose what matches your users best.
  - 1Password
  - LastPass
  - iCloud Keychain
- Ok to keep notes in any SSL/encryption protected app: Notes, OneNote, etc…
  - Some people even use secure notes in Keychain
  - Beware of “replacing” the keychain, however

What's wrong with writing passwords down?



It can happen to anyone



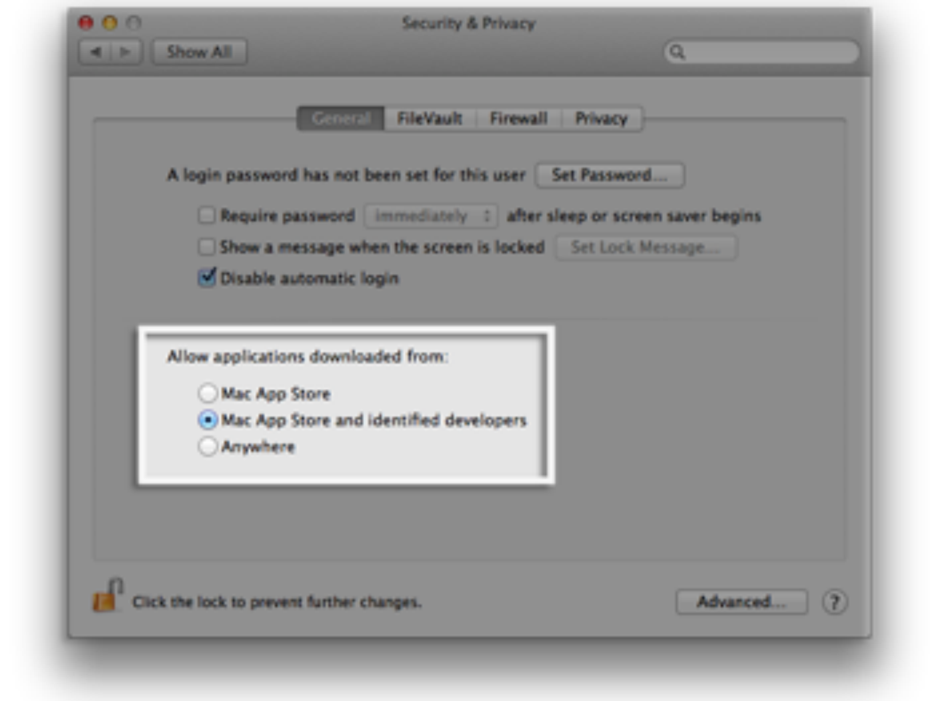
Avoiding
Adware Scanner Utilities

- How bad is Genieo?
  - Genieo virus
  - Hard to remove. Proceed with caution
  - Utilities for removal
  - https://support.apple.com/en-us/HT203987
- MacProtector
- MacKeeper
- Avoid good software from bad sources.

Gatekeeper

Gatekeeper

- Built in, limited, Malware protection (10.7.5+)
- Accessed via "Security & Privacy->->General->Allow apps downloaded from"



A login password has not been set for this user

☐ Require password immediately after sleep or screen saver begins

☐ Show a message when the screen is locked

☑ Disable automatic login

Allow applications downloaded from:

○ Mac App Store

● Mac App Store and identified developers

○ Anywhere

Click the lock to prevent further changes.

Tools to use

- BitDefender Virus Scanner: Free
- ClamXAV: free - https://www.clamxav.com/
- Sophos
- McAfee
- Watchman Monitoring
- Ghostery - https://www.ghostery.com/
- AdwareMedic - http://www.adwaremedic.com/index.php
- Parallels/VMWare

More Resources

- https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/
- http://www.thesafemac.com
- Gatekeeper - https://support.apple.com/en-us/HT202491
- Adware Removal: https://support.apple.com/en-us/HT203987

Questions?

W. “Ian” Blanton
ian@tizite.consulting