Jerry Zigmont
MacWorks, LLC

Jerry is the owner of MacWorks, LLC, an Apple consultancy that provides statewide technical support for to businesses and individuals.

http://macworksllc.com
Twitter - @macworksllc

He is also a co-host of Command-Control-Power, a weekly podcast for the Apple support professional. With over 100 recorded episodes, the podcast focuses on all aspects of running a successful practice.

CMD–CTRL–PWR

http://commandcontrolpower.com

MACTECH PRO EVENTS

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

MACTECH PRO EVENTS

"I've got a feeling we're not in Kansas anymore!"

Viruses: Brief history of viruses coming to the Mac platform

- 1980's forward, Being an uninfected carrier
- 1990's forward, Word Macro Viruses
- AdWare: First appeared in 2012
- Trojan horses appeared on Mac in 2012 (Flashback Trojan)

According to Kaspersky Labs 2014 Security Bulletin

- In 2014, the average Mac user encountered nine cyberthreats. Detected 200 more pieces of Mac malware than in 2013 and blocked more than 3.5 million infection attempts on Mac OS devices.

What's the difference?

- Mac MalWare
  a) Viruses - capable of infecting with no user interaction
  b) Trojans - relies on tricking the user into downloading, installing and running it
- AdWare - display advertisements or browser redirects
- Windows Viruses - In 2012 Sophos cited that 20 percent were carrying one or more instances of Windows malware.
- *"Adware is the biggest threat affecting Mac users today."*
  Thomas Reed

Why Secure Systems?

- Invasion of privacy on a personal and corporate level
- Loss of trade - stolen corporate data or intellectual property
- Impact on productivity and performance
- Legal liability - Loss or breach of data i.e. HIPPA requirements or restrictions

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

What do I secure?
(Layers of Security)

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

Firewalls

- Firewall Description
- Should be your first line of Defense against Malware.
- Any business level firewall - Cisco, SonicWall (now owned by Dell), Watchguard
- Consumer Grade Router - Linksys, Airport, Zywall
- OS X Built-in Firewall - a last resort.

Using monitoring software to report problems

- Protection services (Firewalls, Network Security Appliances)
- Management software such as Watchman Monitoring detects malware and notifies you if one of your users is infected

WiFi Security

- WPA2 or WPA2 Enterprise (Radius)
- Use Strong Passwords / Change On Schedule
- Separate WiFi Network For Guests

VPNs: Why you need them

- 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

- McAfee SaaS formerly MXlogic
- SpamSoap (“powerd by McAfee ”) or Nuvotera
- OnlyMyEmail
- Barracuda’s Email Security Solutions

System / Physical Security

- First place to secure, Last layer to be dealing with Malware
- Firmware Passwords, Device & Data Encryption
- Gatekeeper
- Password Protection & Policies

OS X - System Protection

- Firmware Passwords
- Whole Disk Encryption
  - Built-In "File Vault" (10.7+)
  - Third Party (PGP Desktop or Symantec Endpoint)
- Anti-Virus
  - Products like ESET Cybersecurity
  - Avoid OS X as potential "Silent Carrier" for Windows-based viruses

iOS - System Protection

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

Gatekeeper

Gatekeeper

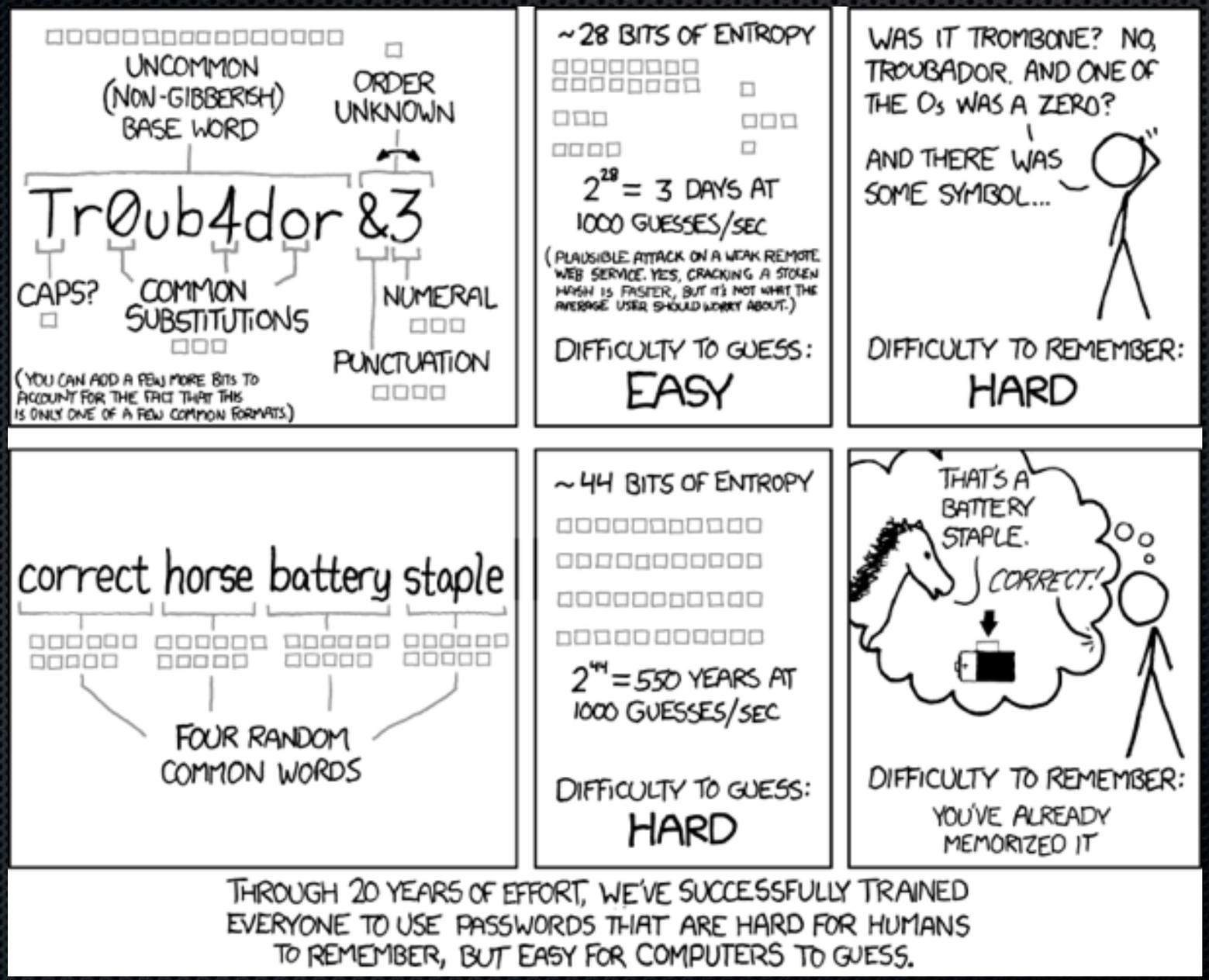
- Built in, limited, Malware protection (10.7.5+)
- Accessed via “Security & Privacy->->General->Allow apps downloaded from”

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 possibly use Password management software to handle the rest.

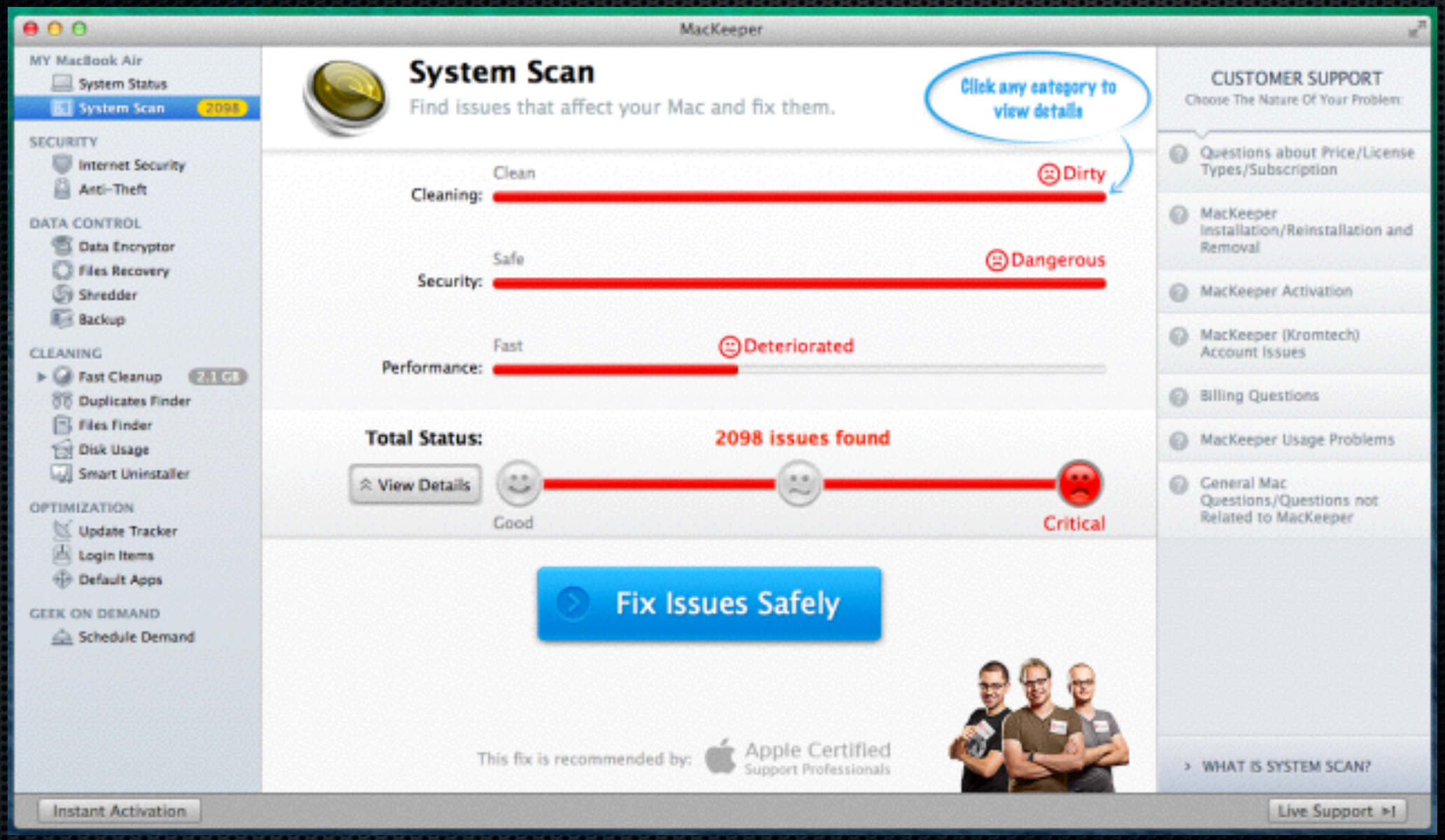
Was it trombone or troubadour?

http://xkcd.com/936/



The longer the password, the better

- Go as long as you can 12, 15 and even 20+ characters
- Use a password manager -- choose what matches your users needs best
  - 1Password, LastPass, DashLane
  - iCloud Keychain
- OK to keep notes in any SSL / Encryption protected app: or system: Notes, OneNote, etc…
  - Some people even use secure notes in Keychain


MacKeeper
MY MacBook Air
System Status
System Scan 2098
SECURITY
Internet Security
Anti-Theft
DATA CONTROL
Data Encryptor
Files Recovery
Shredder
Backup
CLEANING
Fast Cleanup 2.1 GB
Duplicates Finder
Files Finder
Disk Usage
Smart Uninstaller
OPTIMIZATION
Update Tracker
Login Items
Default Apps
GEEK ON DEMAND
Schedule Demand
System Scan
Find issues that affect your Mac and fix them.
Click any category to view details
Cleaning: Clean Dirty
Security: Safe Dangerous
Performance: Fast Deteriorated
Total Status: 2098 issues found
View Details
Good
Critical
Fix Issues Safely
This fix is recommended by: Apple Certified Support Professionals
CUSTOMER SUPPORT
Choose The Nature Of Your Problem:
Questions about Price/License Types/Subscription
MacKeeper Installation/Reinstallation and Removal
MacKeeper Activation
MacKeeper (Kromtech) Account Issues
Billing Questions
MacKeeper Usage Problems
General Mac Questions/Questions not Related to MacKeeper
WHAT IS SYSTEM SCAN?
Instant Activation
Live Support

Avoiding Adware Scanner Utilities

- "Genio Innovation!"
  - Genieo virus
  - Hard to remove. Proceed with caution
  - Utilities for removal
- MacProtector or MacGuard
- MacKeeper
- Avoid good software from bad sources.

Tools to use

- AntiVirus
  - VirusBarrier - Intego
  - avast! Free Antivirus
  - ESET Cybersecurity
  - Sophos Anti-Virus for Mac
    - *Resource For Antivirus from Thomas Reed - http://www.thesafemac.com/mac-anti-virus-testing-2014/*
- Watchman Monitoring - watchmanmonitoring.com
- Ghostery - https://www.ghostery.com/
- Malwarebytes - https://www.malwarebytes.org/antimalware/mac/

More Resources

- History Of Malware On Macs - https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/
- Malwarebytes Security Blog - https://blog.malwarebytes.org - formerly "The Safe MAc"
- CommandControlPower Podcast - Interviews With Thomas Reed -
  - Show #71 http://macs.ws/treed1
  - Show #110 http://macs.ws/treed2
- Kaspersky 2014 Security Bulletin - http://macs.ws/kaspersky 2014

Questions?

Jerry Zigmont
jerry@macworksllc.com

MACTECH PRO EVENTS