

Security: Keeping them out.

MACTECH

Scott M. Neal

Scott M. Neal has been utilizing and programming Apple products since first getting his hands on an Apple][+ and later NeXTcube.

Scott's believes strongly in automation--getting devices to do your work the way you want to, with minimal effort and stress. Often, the real benefits of device automation are underutilized.

Scott would prefer that you be empowered with how to automate (meaning script and program) devices YOURSELF to do what YOU want, not just what you may see yourself limited to by default application and service setups.

With that goal specifically in mind, Scott co-created acmeFoo, the Apple Technology focused training and development co-op, which offers training, courseware, and consulting on a peer level.



MACTECH

Data security and IT Security

- What is the difference?
- Not just encryption
 - e.g., if someone is logged into your machine and has access to unencrypted/decrypted information, what's the point?

Gap analysis

- How do you deal with the delta between technology capabilities and the needs of the business?
- Balance between IT iron fortress, and reasonable access to the business.
- Determine what is an appropriate balance for your organization or client.

The human element

- There's little that you can do about it.
- They will write their passwords down on a post-it
 - Especially if generated for them
 - 25 most popular passwords for 2013
 - <http://splashdata.com/press/worstpasswords2013.htm>
- They will use their street name, 1234, etc...
- All you can do is educate, and inform.
 - Scare tactics don't work.
 - Educate, don't lecture.
 - Have them generate their own passwords using tricks
 - O becomes 0/zero, S becomes 5, E becomes 3, etc.
 - camelCase

25 most common passwords

Rank	Password	Change
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

Rank	Password	Change
14	letmein	Down 7
15	photoshop	New
16	1234	New
17	monkey	Down 11
18	shadow	Unchanged
19	sunshine	Unchanged
20	12345	New
21	password1	Up 4
22	princess	New
23	azerty	New
24	trustno1	Down 12
25	0	New
??	8675309	Ask Jenny!

Source: <http://splashdata.com/press/worstpasswords2013.htm>

Why do administrators manage and maintain security?

- Creates a policy rather than people just occasionally remembering.
- Administrator exceptions to policy (yes, they are always there).
- Maintaining system/process integrity to ensure policy compliance.
- Identifying and handling violations of policy and, therefore, the safety of data.

What makes security difficult (and how to solve it)

- Password storage
 - Keychain
 - OS X
 - Pervasive
 - Create multiple keychains (even on a “keychain”)
 - GUI: Keychain Access.app
 - CLI: `security`
 - iOS
 - Pervasive
 - GUI: ? CLI ha!
 - Now iCloud Keychain to bring the two together
 - Third Party
 - Firefox, ...

What makes security difficult (and how to solve it)

- Man-in-the-Middle
- Ciphers
 - Symmetric
 - Shared Keys
 - Asymmetric
 - Public/Private Keys
 - <http://en.wikipedia.org/wiki/Cipher>
- PKI (Public Key Infrastructure) vs. Web of Trust
- iOS/Mac/others interaction

Terms and concepts you need to know:

- Encryption
 - Levels of Encryption (file, system, boot).
- Authentication
 - Certificates
 - PGP
- Environmental Obfuscation

Encryption on OS X

- Folder-level
 - Technology
 - 128/256 bit AES
 - Disk Image
 - Created by
 - Disk Utility
 - Finder
 - CLI
 - `diskutil`
 - `hdiutil`
 - Legacy FileVault
- Volume-level
 - Technology
 - CoreStorage
 - “Logical Volume Group”
 - Created by
 - Disk Utility
 - FileVault 2
 - CLI
 - `diskutil`

CoreStorage

- Introduced in Lion
 - ...along with Recovery HD
- Logical Volume Manager (LVM)
- Resources
 - http://en.wikipedia.org/wiki/Core_Storage
 - http://movies.apple.com/media/us/osx/2012/docs/OSX_MountainLion_Core_Technologies_Overview.pdf

FileVault: Old and New

- Legacy FileVault
 - Master Password
 - HORRIBLE for backups
- FileVault 2
 - CoreStorage
 - Recovery HD
 - Has its own login window
 - When correct password entered, volume decrypted
- <http://en.wikipedia.org/wiki/FileVault>

Authentication

- Certificates
 - PKI: Public Key Infrastructure
 - http://en.wikipedia.org/wiki/Public_key_infrastructure
 - Centralized
 - Pay \$\$\$\$ for privilege to use well-known root certificate
 - Root certificates for major players pre-installed
- PGP
 - Web of Trust
 - http://en.wikipedia.org/wiki/Web_of_trust
 - Non-centralized
 - “Key signing parties”

Authentication

- UUID
- Checksum
 - md5
 - CLI:md5
 - sha1
 - <http://support.apple.com/kb/ht1652>
 - CLI:openssl sha1
- Digital Signature
 - Not the same as eSignatures

Certificates on OS X / iOS

- Pervasive / built-in
 - Mail
 - Apple ID
 - Safari (and other web browsers)
- Require Certificate Authority (CA)
 - You can be your own for free (with limitations)
 - Levels of trust
- GUI
 - Keychain Access
- CLI
 - openssl

PGP on OS X

- Not default in OS X
 - Download GPG Tools for Mac
 - <https://gpgtools.org>
 - GUI:
 - GPG for Mail
 - plug-in for OS X Mail 10.6-10.9
 - GPG Keychain
 - GPG Services
 - allows you to encrypt/decrypt, sign/verify and import keys from text selections, files, folders, ...
 - CLI:
 - MacGPG Open source currently gnupg 2.0.22

PGP on iOS

- Not built into iOS
 - App Store
 - iPGMail
 - Symantec Mobile Encryption for iOS
 - oPenGP
 - ...
 - CLI:
 - ummm...

Digital Signatures on OS X

- Prevalent
 - Applications
 - Packages
 - GUI: nope...
 - CLI: `spctl`
 - <http://krypted.com/mac-os-x/signing-installation-packages/>
 - Gatekeeper
 - GUI: System Preferences
 - CLI: `spctl`
 - <http://krypted.com/mac-security/manage-gatekeeper-from-the-command-line-in-mountain-lion/>

Digital Signatures on iOS

- Prevalent
 - It's iOS, "it's all magic"

Environmental Obfuscation

- “Security by Obscurity”
- Server and Service Identification.
 - How are you naming your server?
 - How are you advertising it?
 - Some believe it makes it harder to find.
 - Don't depend on this.
- Process identification.
 - Mac does this automatically.

Port Management

- TCP vs. UDP
 - What are they?
 - How do they differ?
- Who has access to the ports?
- Do they need to be restricted?
- Typically done at the router so as to protect entire network
 - Can be done at the server level as well

Firewall

- Network Firewall
 - Router
 - "Vendors" ...
 - pfSense/m0n0wall
 - Computer: `ipfw`
- Application Level Firewall
 - OS X (even non-server)
 - GUI: System Preferences
 - CLI:
 - `socketfilterfw / defaults / launchd / config files`
 - <http://krypted.com/mac-security/the-os-x-application-layer-firewall-part-3-lion/>

Typically block everything but...

- Most common ports
 - SSH: 22
 - Web: 80, 443
 - Time server: 123
 - Mail: 993, 143/110
 - Some will do 80/443 with redirects on server.
 - Mail clients & deployment need this configured.
- How to know
 - Well known TCP & UDP ports used by Apple
 - <http://support.apple.com/kb/ts1629>
 - CLI
 - `/etc/services`

Case studies and examples

- NSA Prism.
 - Begun in 2007
 - “The Prism program collects stored Internet communications based on demands made to Internet companies such as Google Inc. and Apple Inc. under Section 702 of the FISA Amendments Act of 2008 to turn over any data that match court-approved search terms.”
 - [http://en.wikipedia.org/wiki/PRISM_\(surveillance_program\)](http://en.wikipedia.org/wiki/PRISM_(surveillance_program))
- Why susceptible?
- Using obfuscation rather than encryption.

Questions?



Scott M. Neal
smn.mg@acmefoo.org