Security.
Keeping them out.

Justin Rummel
justin@stonyrivertech.com
@justinrummel

Agenda

- Data Security
- Gap Analysis
- Human Element
- Why Manage
- What makes this hard

MACTECH

Data security and IT Security

- What is the difference?
- Not just encryption
  - Physical Access
  - Protection at all layers
- Data at rest, Data in motion

MACTECH

Gap analysis

Why do administrators manage and maintain security?

- Creates a policy rather than people just occasionally remembering.
- Administer exceptions to policies.
- Maintaining system/process integrity to ensure policy compliance.
- Handling violations of policy and, therefore, the safety of data.

MACTECH

Document and Communicate!

MACTECH

The human element

- There's nothing that you can do about it.
- They will write their passwords down on a post-it note.
- 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.

25 most common passwords

Rank	Password	Change from
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 from
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

MACTECH

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

Keeping them Out

MACTECH

Encryption

- Where? EVERYWHERE!
  - On Disk
  - Data in transit

Device Encryption on OS X

- Full Disk Encryption (FDE)
  - FileVault 2
    - System Preferences
    - fdesetup
  - Types
    - Individual
    - Institutional

- For non-boot volumes
  - Finder
  - diskutil (corestorage)

MACTECH

File Encryption on OS X

- Disk Utility
  - 128 or 256 bit AES
- hdiutil
  - Custom options!

MACTECH

Encryption on iOS

- Must have a passcode to enable Data Protection!
- “Instant remote wiping is achieved by securely discarding the block storage encryption key from Effaceable Storage, rendering all data unreadable”
- MDM
- Exchange
- iCloud

Authentication

MACTECH

What makes security difficult (and how to solve it)

- Ciphers
  - Symmetric
    - Shared Key(s)
  - Asymmetric
    - Public/Private Keys

- PKI (Public Key Infrastructure) vs. Web of Trust
- iOS/Mac/others interaction

What makes security difficult (and how to solve it)

- Password storage
  - Keychain
    - OS X
    - iOS
    - iCloud Keychain
  - 1Password
  - Firefox
  - Google

MACTECH

Certificates

- Certificates
  - PKI: Public Key Infrastructure
    - Centralized
      - Pay to use well-known root certificate (single or wildcard)
      - Or install your own!
    - Root certificates for major players pre-installed
- PGP
  - Web of Trust
    - Non-centralized
    - “Key signing parties”

Demo

Unique Validation

- Checksum
  - USE SHA256
- Digital Signature
  - Not the same as eSignatures

Certificates on OS X / iOS

- Built-in
  - Mail
  - 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`

Two Factor Authentication

- A second authentication step to ensure "you" are the owner of the account/data.
- Something you have (your phone)
- Software or Hardware based solutions

MACTECH

Two Factor (Software)

- SMS
  - Simple to implement.
  - Secure?
- iOS Applications
  - Authy
  - Google Authenticator

Two Factor (Hardware)

- YubiKey
- RSA SecurID
- Given one by your provider
- Apple… kind of

Two Factor Sites

- Twitter
- Google
- Microsoft
- Facebook
- Apple

MACTECH

http://twofactorauth.org

MACTECH

Data In Transit

MACTECH

Port Management

- TCP vs. UDP
  - What are they?
  - How do they differ?
- Who has access to the ports?
- Do they need to be restricted?
- Network and/or Computer level

MACTECH

Perimeter Firewalls

- SSH: Port 22
- Websites: Port 80, 443
- Mail: 25, 110, 143 and 993
  - TLS versions, else ensure SSL versions
- Outbound?

Firewalls

- Document
- Log collection, analysis
- Logging the right things?

Client Firewalls

- Built-in
  - Application Layer Firewall (ALF)
    - Checks the signing Cert
  - pf
  - iOS?

Other OS X Security

MACTECH

Gatekeeper

- Built-in
- Depends on settings in System Preferences

XProtect

- Built-In
- Apple's Anti-Malware
- Quaranteen Attribute
  - xattr -r -c filename.ext

The Right Tools

- Be able to apply and report on your clients
- Clients should check-in on a regular basis
  - Reports
  - Alerts
- Enforce written policy

Sources

Sources

- FileVault 2
  - http://support.apple.com/kb/HT5077
  - http://derflounder.wordpress.com/category/filevault-2/
- man hdiutil
- man diskutil
- http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf

MACTECH

Sources

- http://en.wikipedia.org/wiki/Web_of_trust
- http://en.wikipedia.org/wiki/Public_key_infrastructure
- http://support.apple.com/kb/HT5012
- https://lists.apple.com/mailman/listinfo/security-announce

MACTECH

Image Sources

- Unicorn: http://xenomisx.deviantart.com/art/MLP-FIM-UNICORN-Purple-Rain-322337147
- Rainbow: http://www.webdesignhot.com/free-vector-graphics/vector-abstract-rainbow-background/

MACTECH

Questions?

Justin Rummel
justin@stonyrivertech.com
@justinrummel

MACTECH