Modern macOS Security

Mikey (@0x0304)

Former Abertay Hackers Vice Gaffer

@AbertayHackers

"I'm *not* a cryptographer, I just encrypt *a lot*"

- @isislovecruft

No l33t 0day 😢

High level understanding of modern macOS security technologies and mechanisms

Acknowledgements

- Howard Oakley (eclecticlight.co)
- Jonathan Levin (newosxbook.com)
- Patrick Wardle (objective-see.com)
- Sarah Edwards (mac4n6.com)
- Trammell Hudson, Xeno Kovah, Corey Kallenberg & Rafal Wojtczuk
- Pedro Vilaça (@osxreverser) (reverse.put.as)
- Rich Trouton (derflounder.wordpress.com)

Questions?
Shout them out!

(Remind me to repeat the question for the recording 😘)

Contents

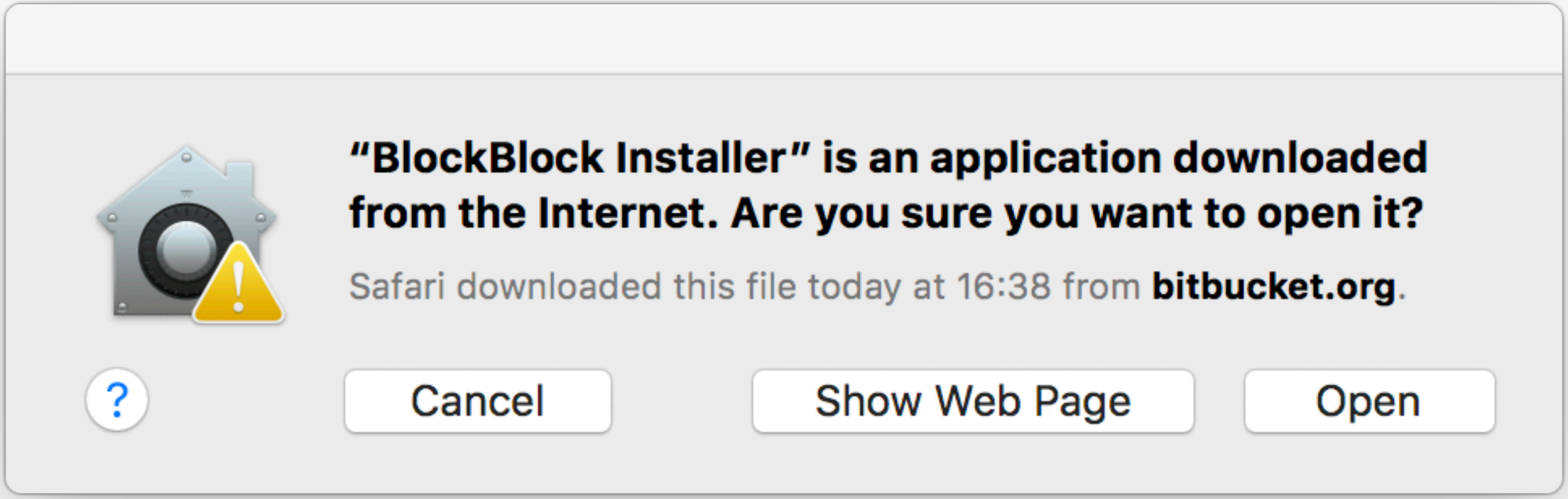
- Gatekeeper 🏰
- Disk Encryption (FileVault 2) (APFS) 🔐
- System Integrity Protection (SIP)
- Firmware (`eficheck`)
- Secure Boot (T2 Chip) 👢
- Security Tools 🛠️
- mOSL (macOS Lockdown)

macOS Mojave (10.14)

Windows vs. macOS

Gatekeeper 🏰

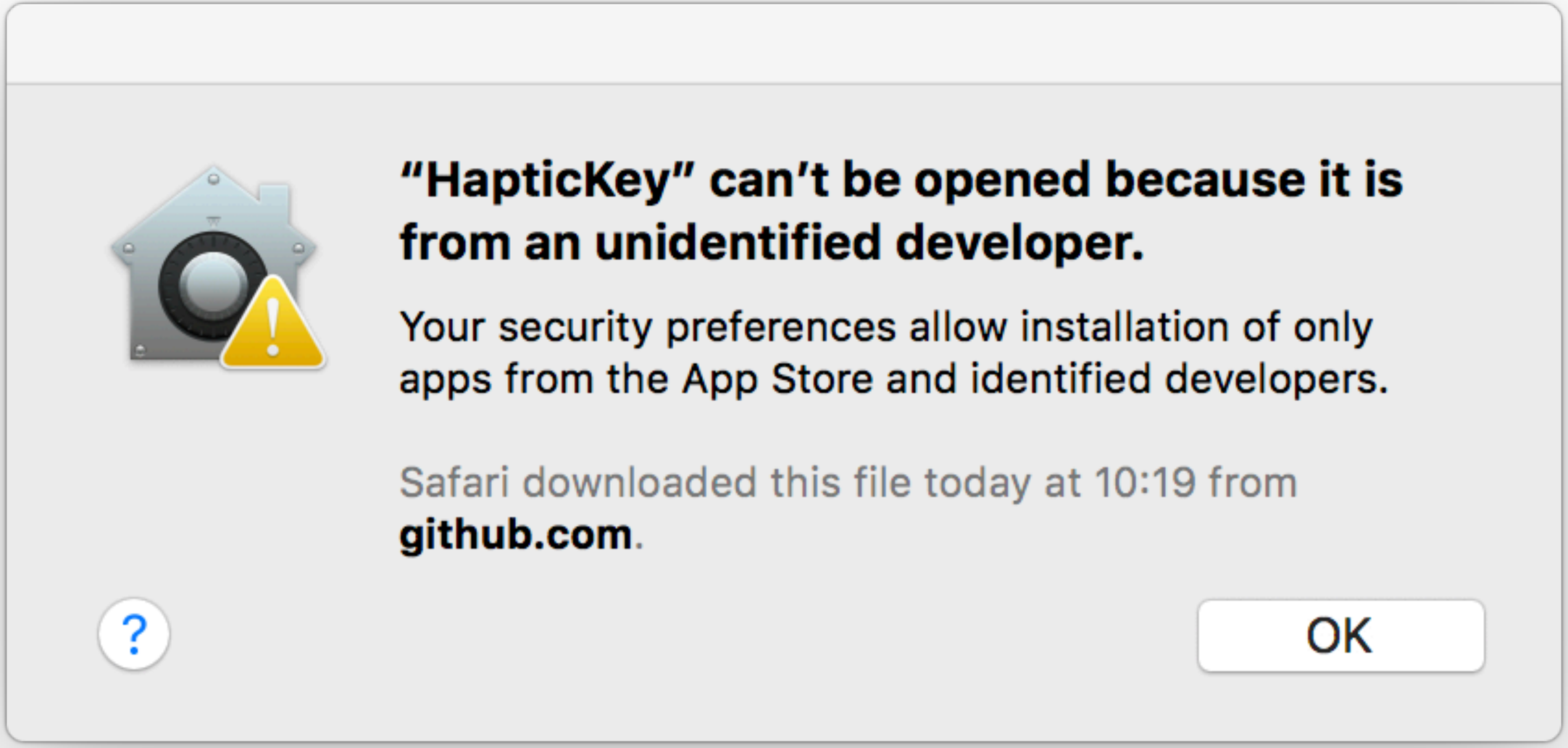
Quarantine 😷

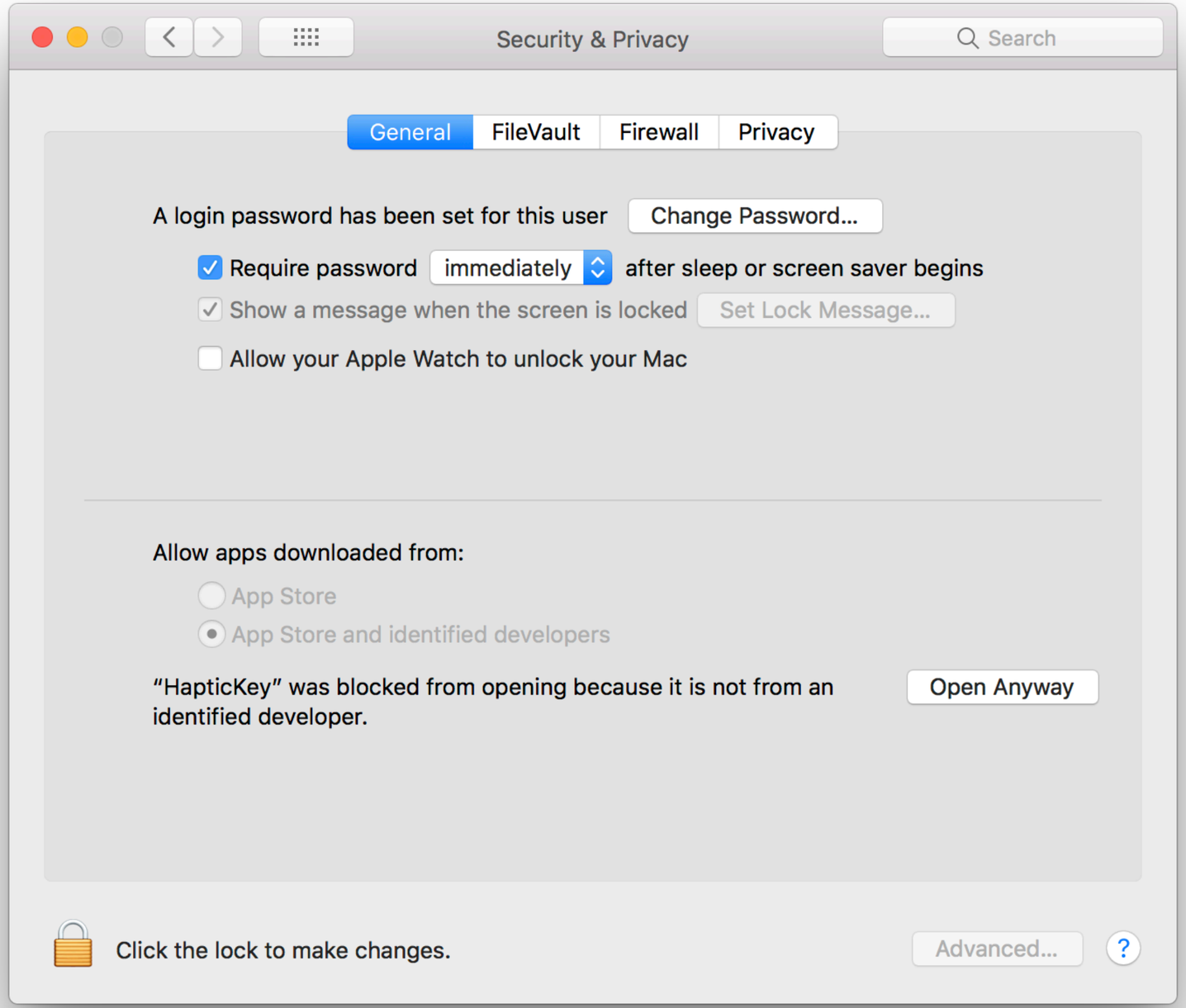

"BlockBlock Installer" is an application downloaded from the Internet. Are you sure you want to open it?
Safari downloaded this file today at 16:38 from bitbucket.org.
?
Cancel
Show Web Page
Open

BSidesMCR2018

```
mikey on 🍎IRATEMONK0x1 in /tmp/BSidesMCR2018
$ ll -@
total 4480
drwxr-xr-x  4 mikey  wheel   128B 16 Aug 10:20 ./
drwxrwxrwt  7 root   wheel   224B 16 Aug 10:20 ../
-rw-r--r--@ 1 mikey  staff   1.8M 16 Aug 10:20 BlockBlock_0.9.9.4.zip
        com.apple.lastuseddate#PS         16B
        com.apple.metadata:kMDItemDownloadedDate          53B
        com.apple.metadata:kMDItemWhereFroms     464B
        com.apple.quarantine      57B
-rw-r--r--@ 1 mikey  staff    73K 16 Aug 10:19 HapticKey.app.zip
        com.apple.lastuseddate#PS         16B
        com.apple.metadata:kMDItemDownloadedDate          53B
        com.apple.metadata:kMDItemWhereFroms     614B
        com.apple.quarantine      57B
mikey on 🍎IRATEMONK0x1 in /tmp/BSidesMCR2018
$
```

Gatekeeper 🏰

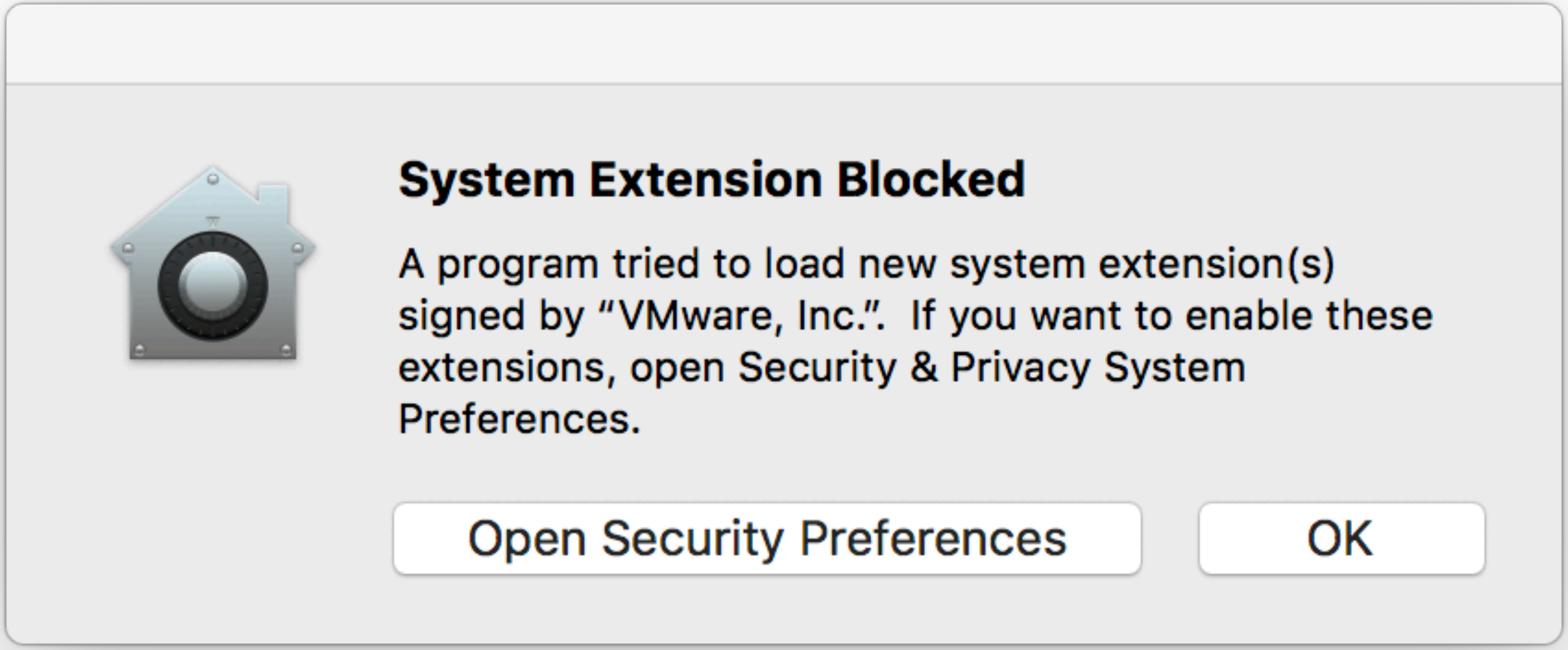

"HapticKey" can't be opened because it is from an unidentified developer.
Your security preferences allow installation of only apps from the App Store and identified developers.
Safari downloaded this file today at 10:19 from github.com.
?
OK

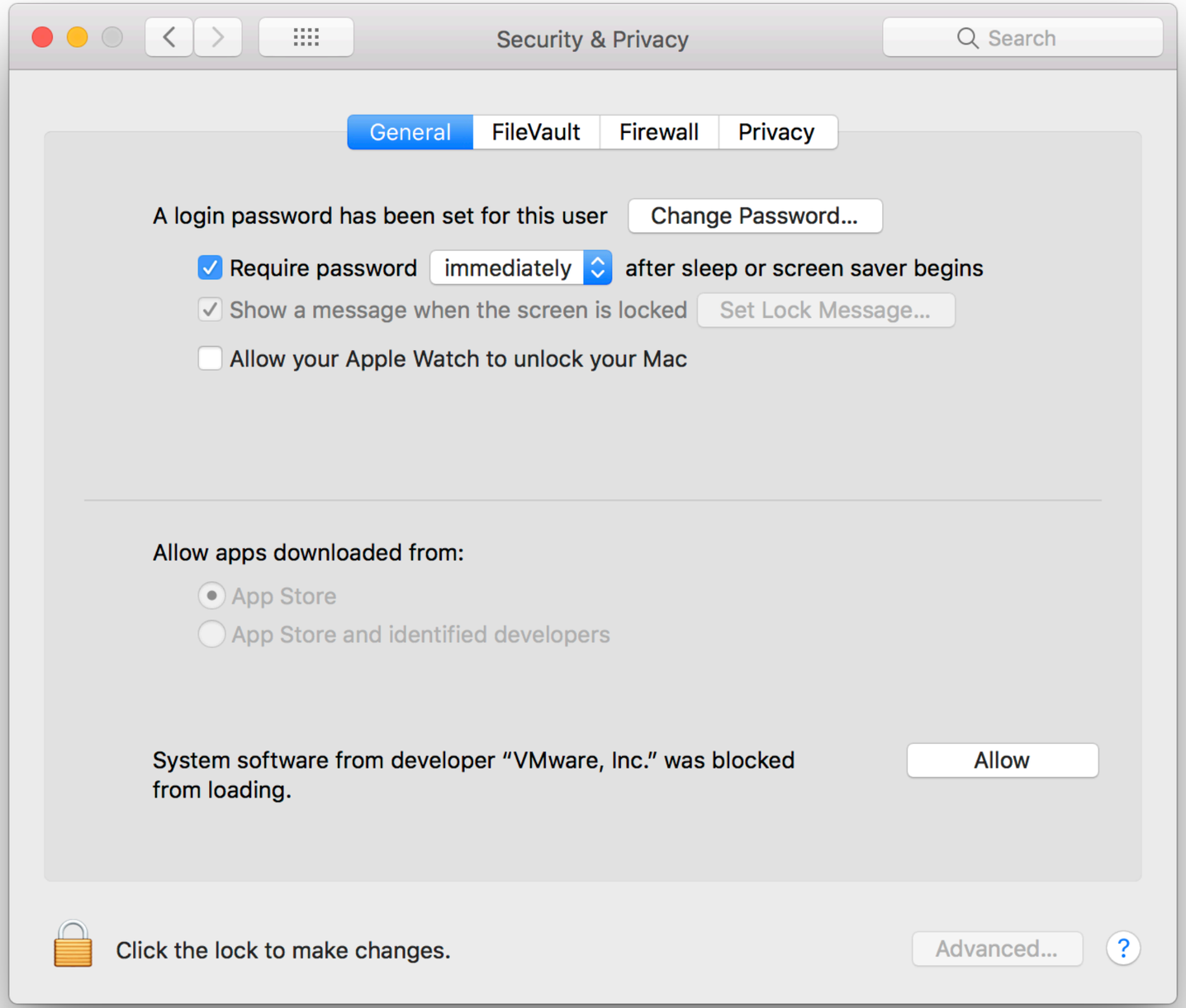

Security & Privacy
Search
General
FileVault
Firewall
Privacy
A login password has been set for this user
Change Password...
Require password
immediately
after sleep or screen saver begins
Show a message when the screen is locked
Set Lock Message...
Allow your Apple Watch to unlock your Mac
Allow apps downloaded from:
App Store
App Store and identified developers
"HapticKey" was blocked from opening because it is not from an identified developer.
Open Anyway
Click the lock to make changes.
Advanced...
?

BSidesMCR2018

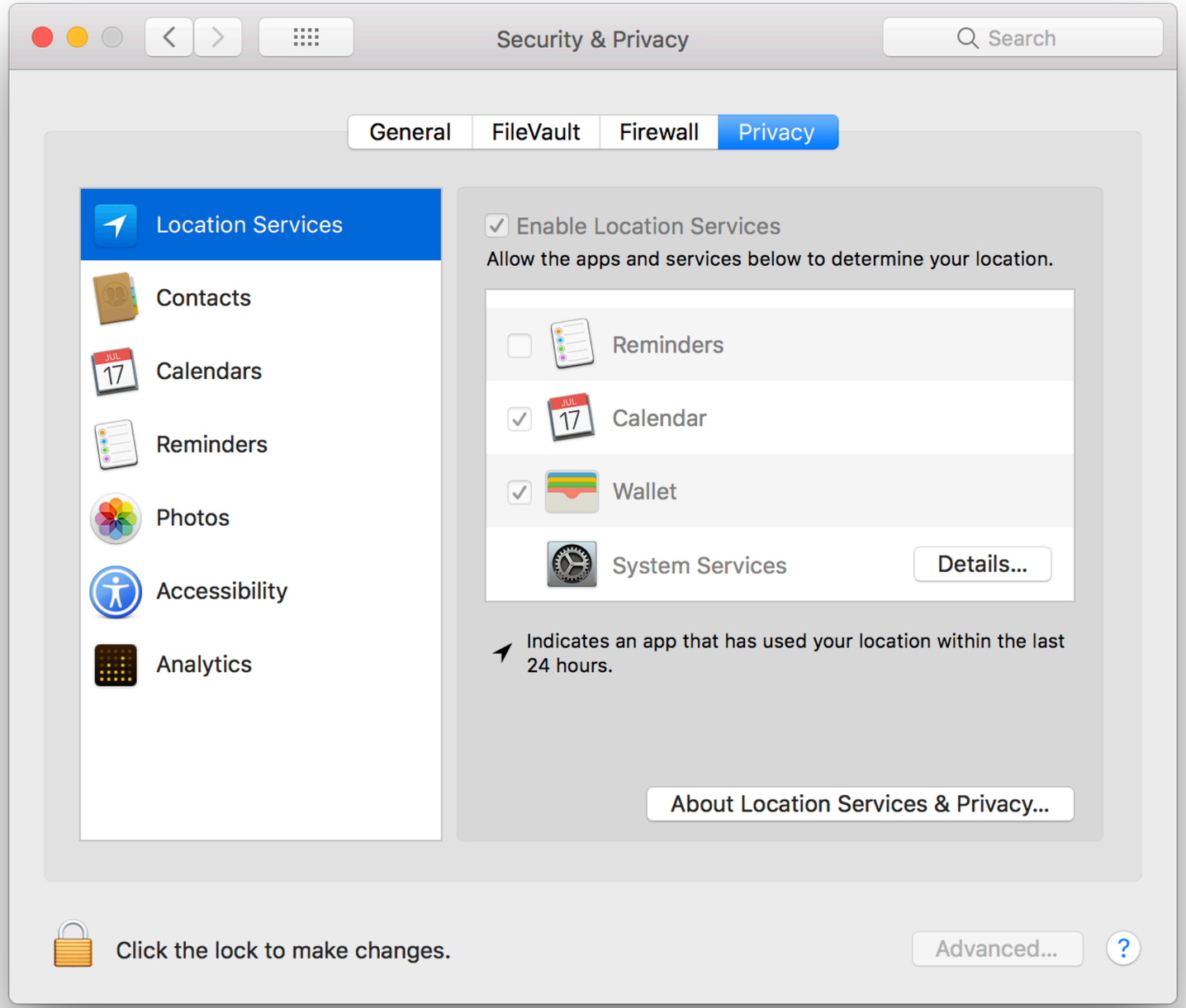
```
mikey on 🍎IRATEMONK0x1 in /tmp/BSidesMCR2018
$ spctl
System Policy Basic Usage:
       spctl --assess [--type type] [-v] path ... # assessment
       spctl --add [--type type] [--path|--requirement|--anchor|--hash] spec ... # add rule(s)
       spctl [--enable|--disable|--remove] [--type type] [--path|--requirement|--anchor|--hash|--rule] spec # change rule(s)
       spctl --status | --master-enable | --master-disable # system master switch

Kernel Extension User Consent Usage:
    spctl kext-consent <action>         ** Modifications only available in Recovery OS **
        status
            Print whether kernel extension user consent is enabled or disabled.
        enable
            Enable requiring user consent for kernel extensions.
        disable
            Disable requiring user consent for kernel extensions.
        add <team-id>
            Insert a new Team Identifier into the list allowed to load kernel extensions without user consent.
        list
            Print the list of Team Identifiers allowed to load without user consent.
        remove <team-id>
            Remove a Team Identifier from the list allowed to load kernel extensions without user consent.
mikey on 🍎IRATEMONK0x1 in /tmp/BSidesMCR2018
$
```


System Extension Blocked
A program tried to load new system extension(s) signed by “VMware, Inc.”. If you want to enable these extensions, open Security & Privacy System Preferences.
Open Security Preferences
OK


Security & Privacy
Search
General
FileVault
Firewall
Privacy
A login password has been set for this user
Change Password...
Require password
immediately
after sleep or screen saver begins
Show a message when the screen is locked
Set Lock Message...
Allow your Apple Watch to unlock your Mac
Allow apps downloaded from:
App Store
App Store and identified developers
System software from developer "VMware, Inc." was blocked from loading.
Allow
Click the lock to make changes.
Advanced...
?

Entitlements


Security & Privacy
Search
General
FileVault
Firewall
Privacy
Location Services
Contacts
Calendars
Reminders
Photos
Accessibility
Analytics
Enable Location Services
Allow the apps and services below to determine your location.
Reminders
Calendar
Wallet
System Services
Details...
Indicates an app that has used your location within the last 24 hours.
About Location Services & Privacy...
Click the lock to make changes.
Advanced...

```
mikey on 🍎IRATEMONK0x1 in ~
$ jtool --ent /Applications/Calendar.app/Contents/MacOS/Calendar | grep 'personal-information'
        <key>com.apple.security.personal-information.addressbook</key>
        <key>com.apple.security.personal-information.calendars</key>
        <key>com.apple.security.personal-information.location</key>
mikey on 🍎IRATEMONK0x1 in ~
$ |
```

Enhanced Runtime

Resource access

`com.apple.security.device.audio-input`	Audio input and microphone
`com.apple.security.device.camera`	Any camera exposed via AVFoundation
`com.apple.security.personal-information.location`	Location
`com.apple.security.personal-information.addressbook`	Contacts
`com.apple.security.personal-information.calendars`	Calendars and Reminders
`com.apple.security.personal-information.photos-library`	Apple Photos library
`com.apple.security.automation.apple-events`	Sending Apple Events to other apps

User Data Protections

All data categories

NEW

Location Services

Contacts

Calendars

Reminders

Photos

Mail

Messages

Safari Browsing History

HTTP Cookies

Call History

iTunes Backups

Time Machine Backups

Translocation

XProtect

hoakley / August 15, 2018 / Macs, Technology

XProtect: *Missing presumed dead?*

Malware Removal Tool (MRT)

FileVault 2 🔐

FileVault 2

- Volume level encryption[1]
- 128 bit AES-XTS
- On by default[2]

[1] AKA Full Disk Encryption

[2] Escrow to iCloud by default

Filesystem 🗃️

Hierarchical File System + (HFS+)

Circa 1998

Apple Filesystem (APFS)

Projects

```
mikey on 🍎IRATEMONK0x1 in ~/Documents/Projects
$ fdesetup status
FileVault is On.
mikey on 🍎IRATEMONK0x1 in ~/Documents/Projects
$ diskutil list
/dev/disk0 (internal):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                         1.0 TB     disk0
   1:                        EFI EFI                     314.6 MB   disk0s1
   2:                 Apple_APFS Container disk1         1.0 TB     disk0s2

/dev/disk1 (synthesized):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      APFS Container Scheme -                      +1.0 TB     disk1
                                  Physical Store disk0s2
   1:                APFS Volume IRATEMONK               191.0 GB   disk1s1
   2:                APFS Volume Preboot                 41.1 MB    disk1s2
   3:                APFS Volume Recovery                1.0 GB     disk1s3
   4:                APFS Volume VM                      1.1 GB     disk1s4

mikey on 🍎IRATEMONK0x1 in ~/Documents/Projects
$ |
```

Projects — -bash

```
0xmachos on 🍎MALLARD📦 in ~/Documents/Projects
$ fdesetup status
FileVault is Off.
0xmachos on 🍎MALLARD📦 in ~/Documents/Projects
$ diskutil list
/dev/disk0 (internal, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *42.9 GB    disk0
   1:                        EFI EFI                     209.7 MB   disk0s1
   2:                 Apple_APFS Container disk1         42.7 GB    disk0s2

/dev/disk1 (synthesized):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      APFS Container Scheme -                      +42.7 GB    disk1
                                 Physical Store disk0s2
   1:                APFS Volume MALLARD                 13.9 GB    disk1s1
   2:                APFS Volume Preboot                 20.8 MB    disk1s2
   3:                APFS Volume Recovery                518.1 MB   disk1s3
   4:                APFS Volume VM                      1.1 GB     disk1s4

0xmachos on 🍎MALLARD📦 in ~/Documents/Projects
$
```

System Integrity Protection (SIP)

SIP: What

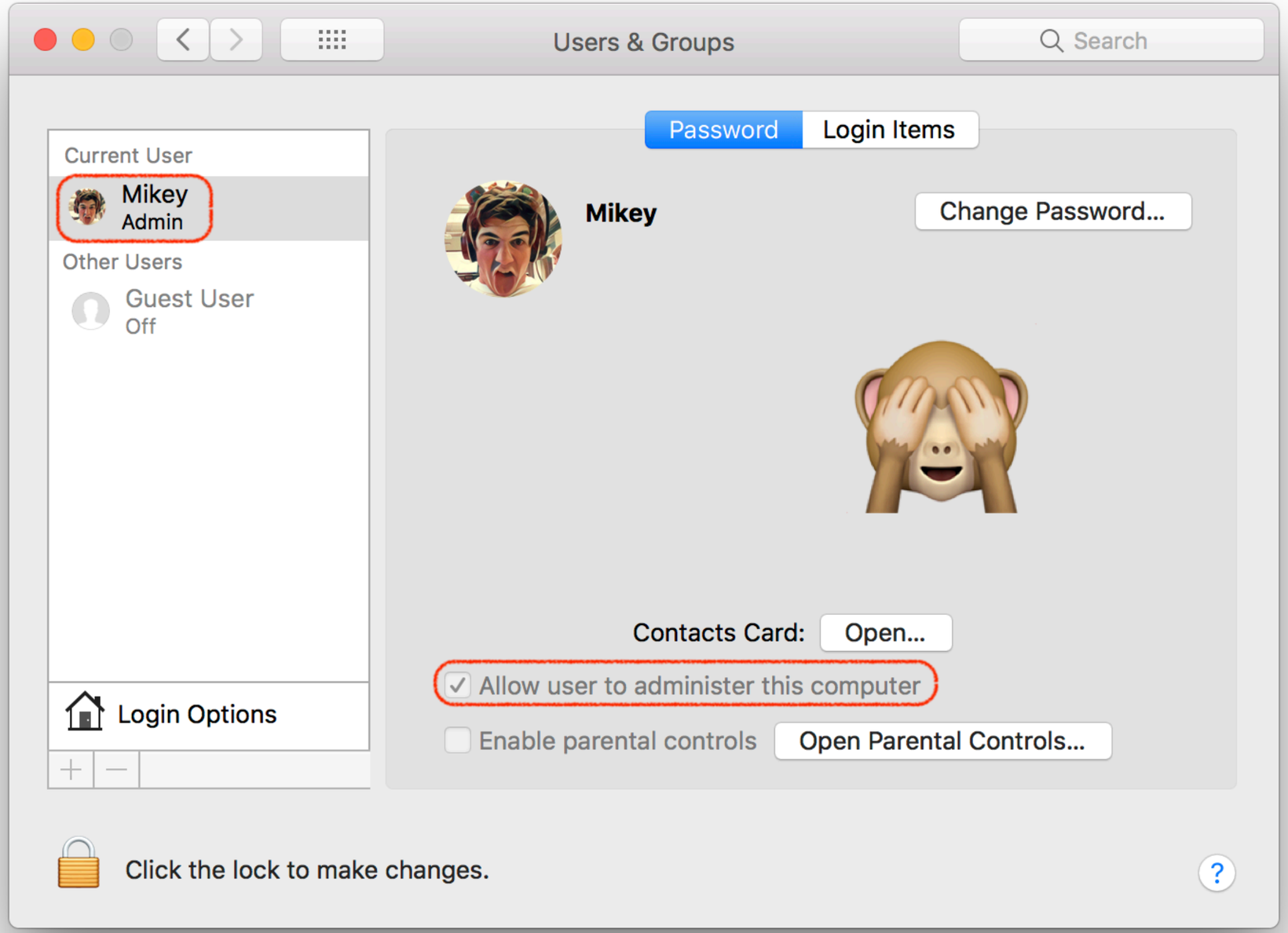
- Protect OS on **disk** & at **runtime**

SIP: How

- Limit power of `root`
- Reduces to a sandbox policy that applies to the whole system

SIP: Why

- Most Macs are **single user systems** with `root` privileges
- Malware **one** password or LPE away from full control


Users & Groups
Search
Current User
Mikey
Admin
Other Users
Guest User
Off
Login Options
Password
Login Items
Mikey
Change Password...
Contacts Card:
Open...
Allow user to administer this computer
Enable parental controls
Open Parental Controls...
Click the lock to make changes.

Kernel exploits ain't nuthing ta fuck wit

SIP: Overview

- System Locations can't be written to
- System Processes can't be interfered with
- Kernel Extensions (`kexts`) must be signed

SIP: Filesystem Protections

System Only	Available to Devs
/System	[~]/Library
/usr	/usr/local
/bin	/Applications
/sbin	

Sandbox

```
mikey on 🍎IRATEMONK0x1 in /System/Library/Sandbox
$ grep -A 2 'KernelExtensionManagement' rootless.conf | tail -n 3
KernelExtensionManagement       /System/Library/Caches/com.apple.kext.caches
*                               /System/Library/Extensions
                                /System/Library/Extensions/*
mikey on 🍎IRATEMONK0x1 in /System/Library/Sandbox
$ xattr -l /System/Library/Caches/com.apple.kext.caches/
com.apple.rootless: KernelExtensionManagement
mikey on 🍎IRATEMONK0x1 in /System/Library/Sandbox
$ ll -O /System/Library/ | grep 'Extensions'
drwxr-xr-x  340 root  wheel  sunlnk       11K 28 Jul 20:32 Extensions/
mikey on 🍎IRATEMONK0x1 in /System/Library/Sandbox
$ ll -O /System/Library/Extensions/ | grep 'Sandbox.kext'
drwxr-xr-x@   3 root  wheel  restricted   96B 22 Jun 07:13 Sandbox.kext/
mikey on 🍎IRATEMONK0x1 in /System/Library/Sandbox
$
```

local — -bash

```
mikey on 🍎IRATEMONK0x1 in /usr
$ sudo touch BSidesMCR18
touch: BSidesMCR18: Operation not permitted
mikey on 🍎IRATEMONK0x1 in /usr
$ cd /usr/local/
mikey on 🍎IRATEMONK0x1 in /usr/local
$ sudo touch BSidesMCR18
mikey on 🍎IRATEMONK0x1 in /usr/local
$ ls
BSidesMCR18  Homebrew/    etc/        opt/        texlive/
Cellar/      MacGPG2/     include/    sbin/       var/
Frameworks/  bin/         lib/        share/
mikey on 🍎IRATEMONK0x1 in /usr/local
$
```

SIP: Runtime Protections

SIP: Runtime Protections

- `restricted` flag
- Can't `fork` & `exec`
- Can't inject libraries
- No `Dtrace`
- No debugger attachment
- Can't kill

SIP: Configuration

```
csrutil
```

local — -bash

```
mikey on 🍎IRATEMONK0x1 in /usr/local
$ csrutil status
System Integrity Protection status: enabled.
mikey on 🍎IRATEMONK0x1 in /usr/local
$ csrutil disable
csrutil: failed to modify system integrity configuration. This tool needs to be
executed from the Recovery OS.
mikey on 🍎IRATEMONK0x1 in /usr/local
$ |
```

SIP: Configuration

- `csrutil enable --without`[3]
  - `kext`
  - `fs`
  - `debug`
  - `dtrace`
  - `nvram`

[3] Undocumented argument, caveat emptor 🔥

SIP: Configuration

```
nvram csr-active-config
```

Enhanced Runtime

AKA 3rd Party SIP

Enhanced Runtime

- **Opt in**
- Protections similar to system binaries
  1. Code Signing
  2. Debugging
  3. Resource Access
- Opt out via entitlements

Firmware

(U)EFI

(Unified) Extensible Firmware Interface

Thunderstrike 1 & 2

Trammell Hudson, Xeno Kovah & Corey Kallenberg

Thunderstrike 1

1. EFI validity only checked by a software CRC32 👀
2. Update is `bless`'d 🙏
3. "recovery mode boot"
   - Flashing code run at same time Option ROMs loaded
4. Option ROMs can overwrite EFI 🎉

Thunderstrike 2

1. Get `r00t` 🧙
2. Load kernel module to access RAM
3. Hook the S3 Sleep/ Resume script[4]
4. Unlock EFI Flash (`FLOCKDN`) 🔓
5. Overwrite EFI 🎉
6. Write payload to all connected thunderbolt devices 🐛

[4] Not always necessary

Dark Jedi

Rafal Wojtczuk, Corey Kallenberg

Dark Jedi

1. Close MacBook
2. Open MacBook
3. 🤔

Overwrite EFI from userland

Mitigations 🙅

Modern Mac EFI Security

OptionROM Loading

0xmachos — -bash

```
0xmachos on 🍎MALLARD📦 in ~
$ sudo firmwarepasswd -check
Password Enabled: No
0xmachos on 🍎MALLARD📦 in ~
$ sudo firmwarepasswd -mode
Mode: none
Option roms allowed

0xmachos on 🍎MALLARD📦 in ~
$
```

OptionROM Loading

```
mikey on 🍎IRATEMONK0x1 in ~
$ sudo firmwarepasswd -check
Password Enabled: Yes
mikey on 🍎IRATEMONK0x1 in ~
$ sudo firmwarepasswd -mode
Mode: command
Option roms not allowed

mikey on 🍎IRATEMONK0x1 in ~
$
```

`eficheck`

- Added in High Sierra (`10.13`)
- Runs weekly
- Corey Kallenberg & Xeno Kovah
- `/usr/libexec/firmwarecheckers/eficheck/eficheck`

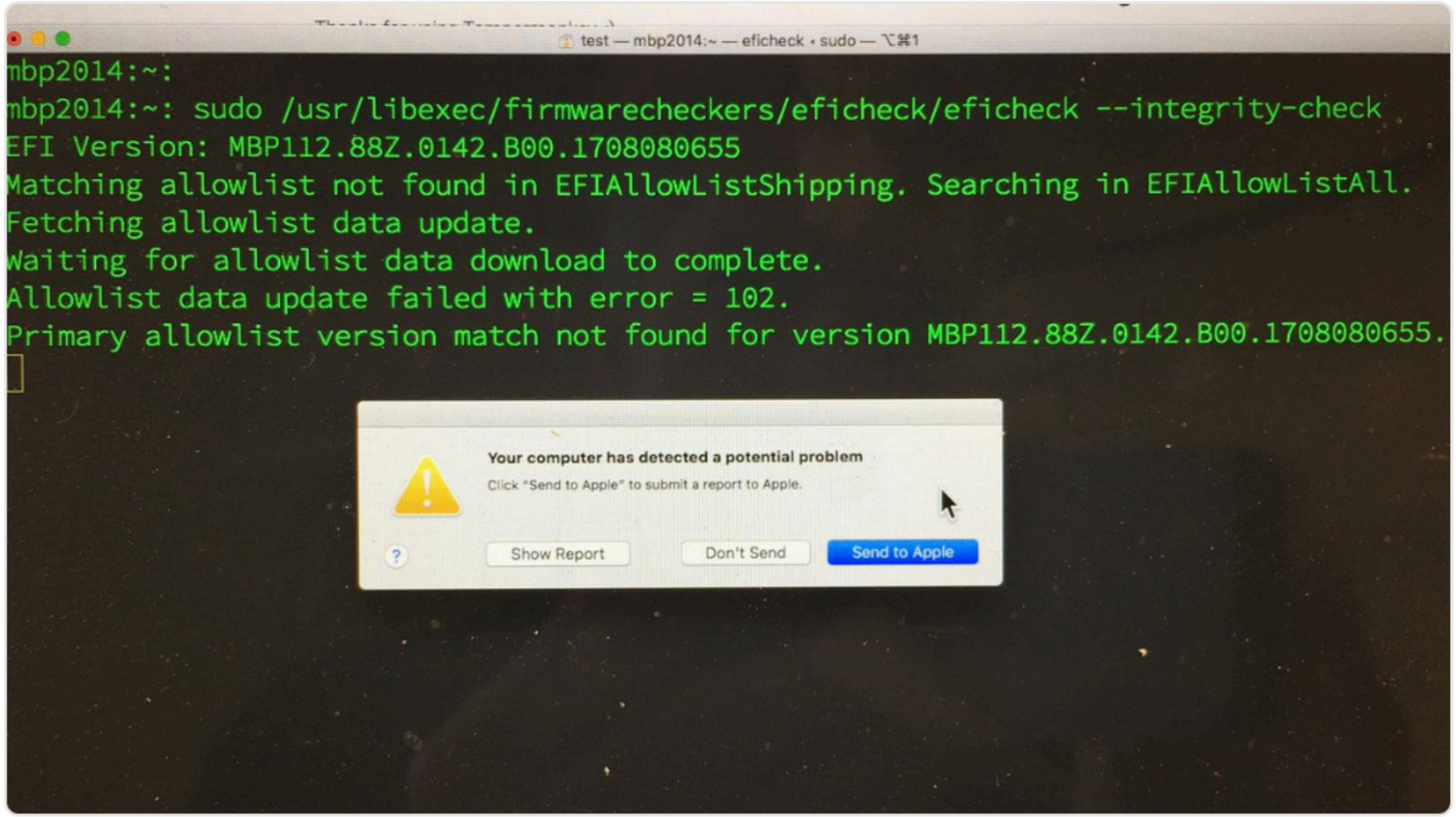
eficheck

```
$ /usr/libexec/firmwarecheckers/eficheck/eficheck --integrity-check
EFI Version: MBP133.88Z.0247.B00.1806261159
Primary allowlist version match found. No changes detected in primary hashes.
```

Trammell Hudson
@qrs

Following

Success! Thunderstrike 2 was found by the eficheck, although it doesn't take any active steps to conceal itself.



6:12 PM - 6 Nov 2017

eficheck: T2 Macs

```
$ /usr/libexec/firmwarecheckers/eficheck/eficheck --integrity-check
ReadBinaryFromKernel: No matching services found.
Either this system is not supported by eficheck, or you need to re-load the kext
IntegrityCheck: couldn't get EFI contents from kext
```

T2

T2: What?

- Repurposed Apple A10
- "Security Coprocessor"
  - Secure Boot
  - Full disk encryption

T2: Where

- iMac Pro (2017)
- MacBook Pro with Touch Bar (2018)

T2: Secure Boot

- Full Security[5] (*Default*)
  - Ensures your OS is **trusted** by Apple
- Medium Security
  - Ensures that the OS has been **signed** by apple
- No Security

[5] Requires internet connection

T2: Disk Encryption

- Hardware accelerated AES
- Automatic disk encryption[6]
  - Tied to a 256-bit AES key burned into your T2

[6] Still need to enable FileVault

Security Tools

BlockBlock

"continually monitors common persistence locations and displays an alert whenever a persistent component is added"

objective-see.com/products/blockblock

OverSight

"monitors mic and webcam, alerts the user when the internal mic is activated, or whenever a process accesses the webcam."

objective-see.com/products/oversight

obdev.at/products/littlesnitch

Anti-Virus?

mOSL

(macOS Lockdown)

Demo 🙈

Open Source 👀

github.com/0xmachos/mOSL

Questions?