

# The Apple of Your EFI

## An Updated Study of EFI Security

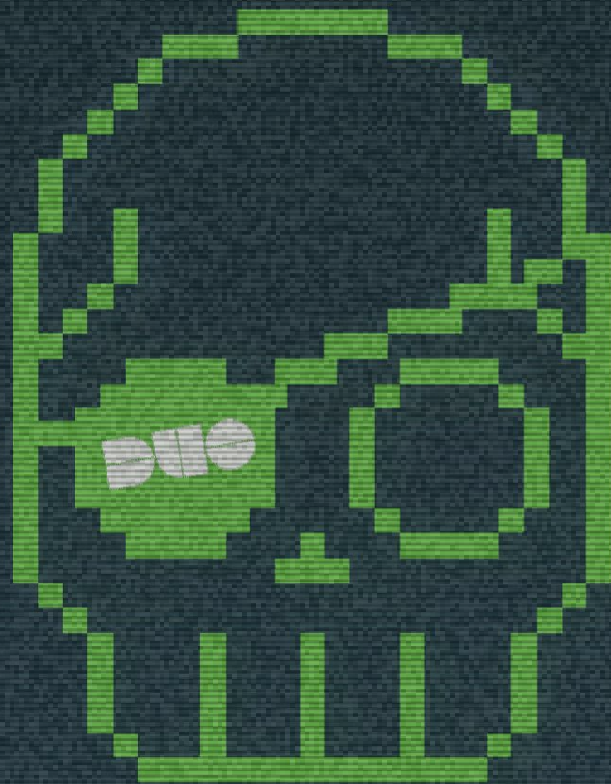
**Pepijn Bruienne (@bruienne)**

**Rich Smith (@iodboi)**

**Duo Security**

Black Hat Europe 2017

6/12/2017



# About Us

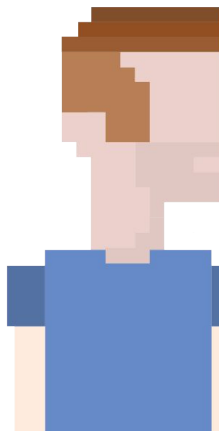
- **Pepijn Bruienne (@bruienne)**

- R&D Engineer in Duo Labs
- Focus on R&D, RE and further breaker of all things Apple
- Recovering Mac Admin
- OSS maintainer of some popular Mac Admin tools



- **Rich Smith (@iodboi)**

- Director of R&D, Duo Labs
- Enjoy researching at scale, post-exploitation, firmware & Python
- Worked in security far too long now I think!



# About Duo

- **We're with Duo Labs, Duo Security's research group**
- **We break things (or attempt to) and then:**
  - Write code to un-break it
  - Talk about it
  - Write papers & blogs about it
- **We build things:**
  - Prototype new security products & approaches for Duo
  - Think about what customers future security needs will be
  - Release open source code to share things we experiment with
    - Check out the recent releases of [IsThisLegit?](#) and [Phinn](#)
- **We're hiring!**



# Research tl;dr

Shine some light onto firmware security as compared to software security

We analysed all OS, Security and EFI firmware release by Apple for 10.10/.11/.12/13

- This is all about what Apple is releasing EFI update wise
- About 3 years worth of update data, discovered many anomalies

We got data from >73K Mac systems to see the real-world state of EFI installs

- All about how well the EFI updates Apple released are being installed

We compared both datasets to see how well the real world matched the expected state of EFI versions running



# Things We Will Cover Today

## Context

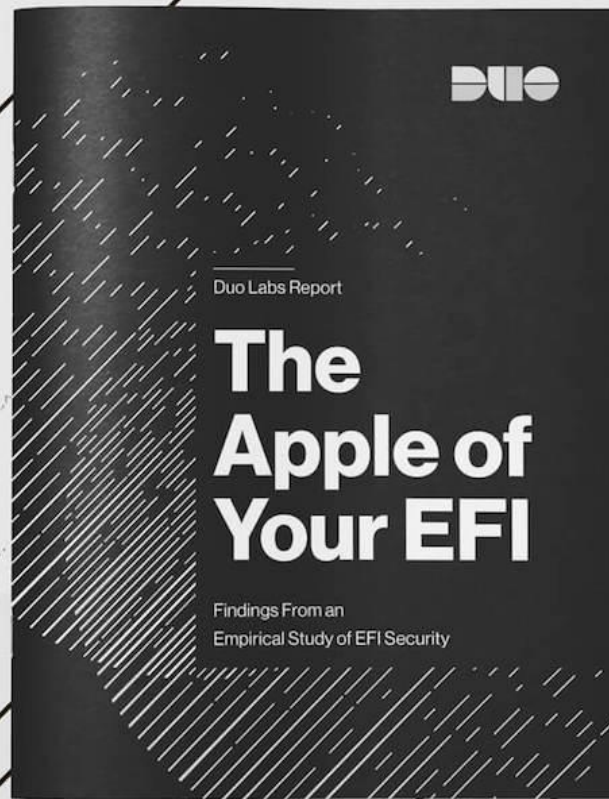
- History of existing Apple EFI security research
- How Apple Macs update their firmware

## The New Work

- What we did
- What we found
- What you can do
- What we're releasing

**Lots more information  
in our technical paper**

**<http://duo.sc/2x1AA9R>**



# EFI is Everywhere

Intel EFI - mid-1990s

UEFI standard - 2005

Apple EFI - 2006



# EFI Killed the Open Firmware Star

- **Apple EFI**

- Shipped in first-generation Intel Macs in early 2006
- Intel switch = **no more Open Firmware** (PPC legacy)
- First models shipped with EFI were iMac and MacBook Pro
- Must support new Mac hardware and features
- Supports platform-specific things like:
  - NetBoot
  - Internet Restore
- Entirely invisible to end users

# What Makes Attacking EFI Attractive?

- **Stealth**

- It's very hard to detect if EFI / firmware is compromised

- **Persistence**

- It's hard to remove implants from EFI
- Reinstalling the OS or replacing HDD is not sufficient

- **Access to everything\***

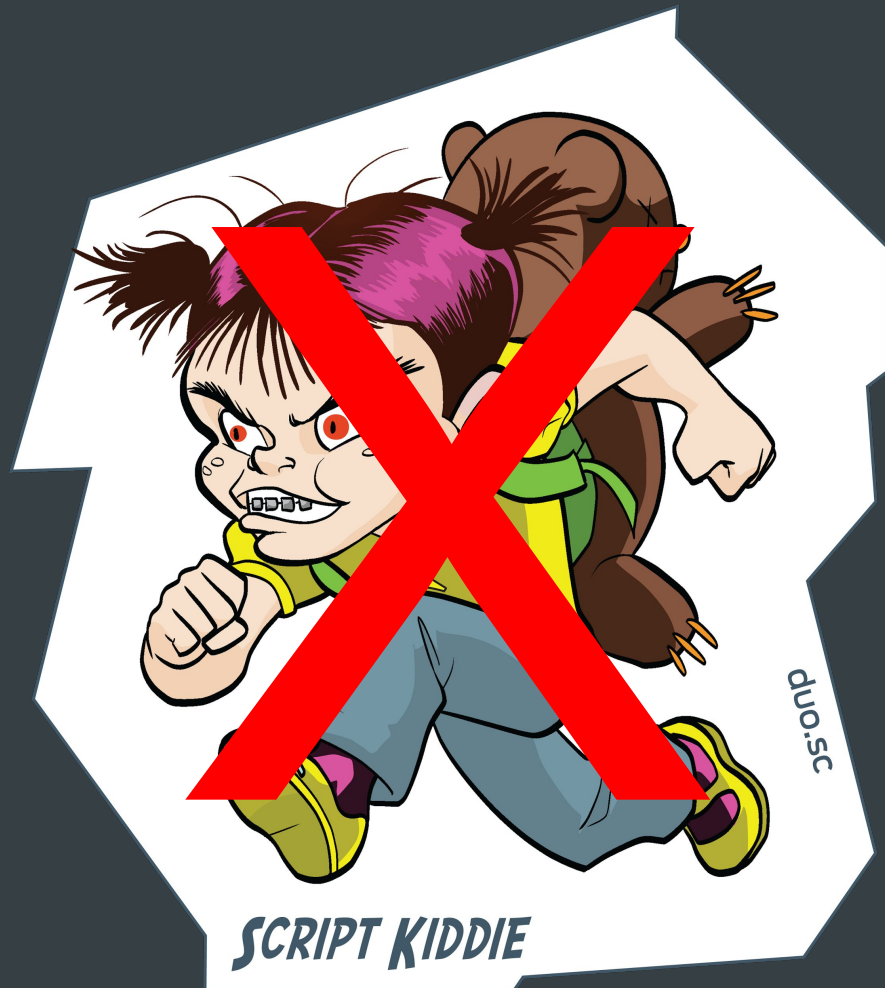
- Running at Ring -2 means that security controls at higher layers can be circumvented
- Pretty much arbitrary read/write to disk and memory

## Protection Rings

- Ring 3 : Applications
- Ring 0 : OS / Kernel
- Ring -1 : Hypervisor
- Ring -2 : EFI

# Who Wants to Attack EFI?

- Well-funded adversaries:
  - 'Nation-states'
  - Industrial espionage
- This is not your script kiddie tool



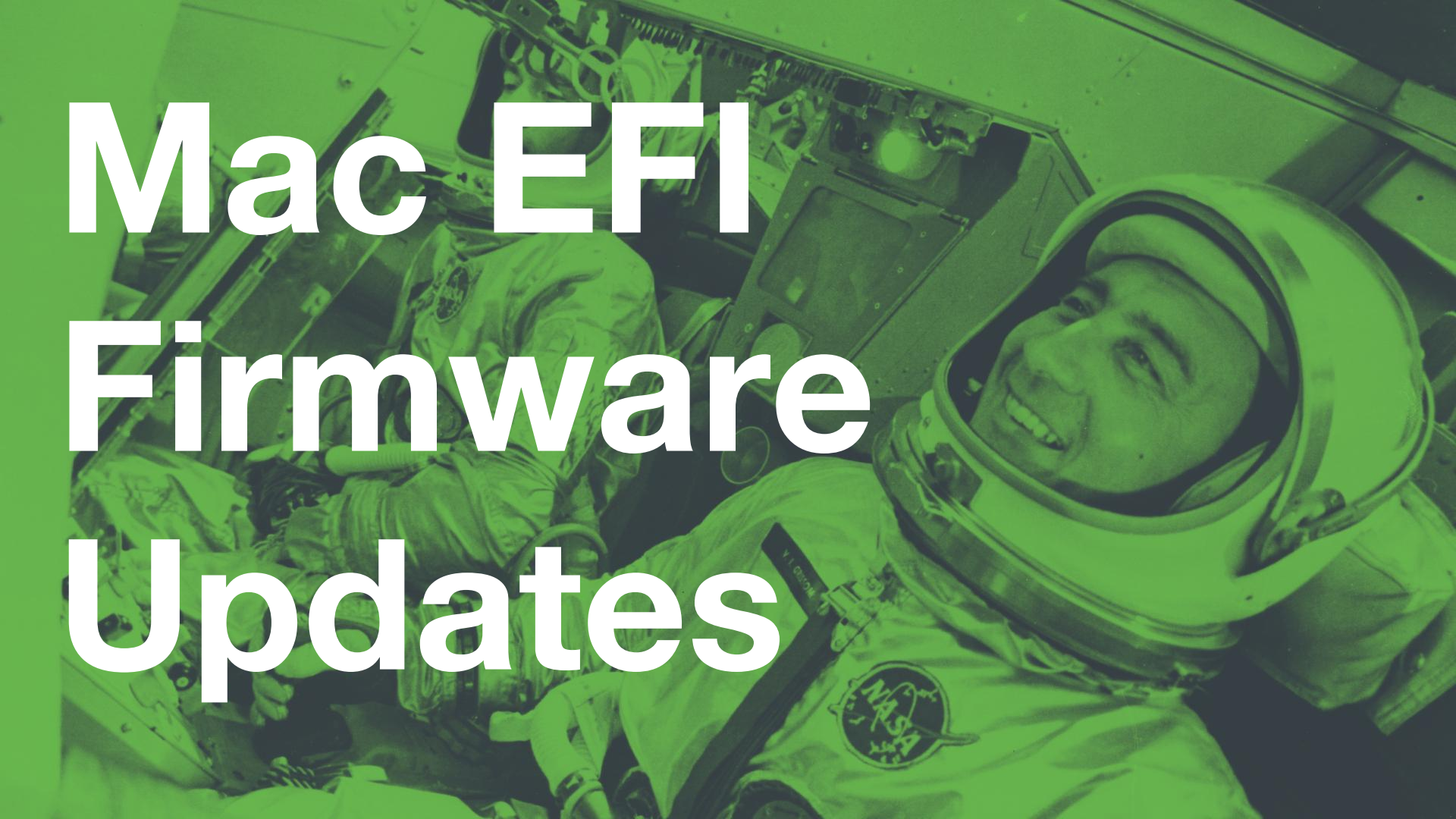
# A Brief History Of Apple EFI Security



# EFI Security Research in Brief

- ***‘DE MYSTERIIS DOM JOBSIVS’*** - 2012 - snare - Black Hat 12
- **Sonic Screwdriver - 2012+** - Wikileaks ‘Vault7’ leaks - Sea Eye Aye?
- **ThunderStrike 1 - 2014** - Trammell Hudson @ 31c3
- **ThunderStrike 2 - 2015** - Trammell Hudson, Xeno Kovah,  
Corey Kallenberg @ Defcon 23
- **PCI DMA attack - 2016** - Ulf Frisk @Defcon24
- **Lots of other cool EFI research**
  - **Pedro Vilaça** - Is There an EFI Monster Inside Your EFI? @ 44Con/SyScan Beijing ...
  - <https://reverse.put.as>

# Mac EFI Firmware Updates

A green-tinted photograph of an astronaut in a space suit, smiling, with technical equipment visible in the background. The astronaut is wearing a white space suit with a NASA patch on the chest and a white helmet. The background shows various mechanical components and wiring, suggesting a space station or shuttle interior.

# How Does EFI Get Updated?

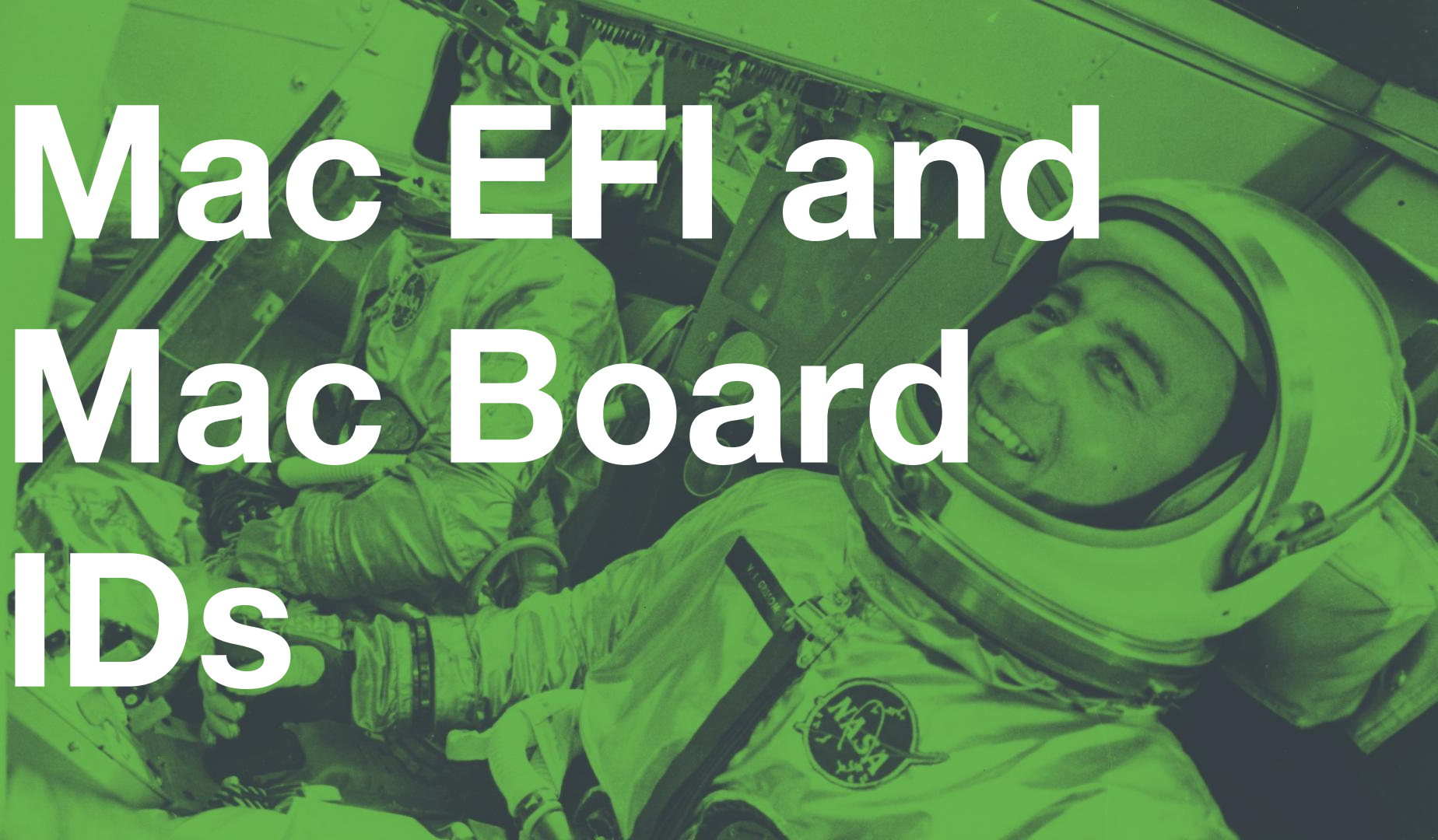
Prior to 2015 - manual

After ThunderStrike

# The Apple EFI Update Process

- **As of late 2015 - ThunderStrike response**
  - Update is shipped as a standard Apple PKG installer
  - Payload-free PKG runs **efiupdate** to bootstrap EFI updater
  - Ships with complete set of current EFI **.scap** or **.fd** bundles
  - **\$MODEL\_\$MAJOR\_\$MINOR\_LOCKED.\$EXT**
  - The postinstall script invokes **efiupdate**
  - The tool copies the correct firmware to the ESP (EFI System Partition)
  - The file is then blessed using the **bless** command:
    - `bless -mount / -firmware MBP111_0138_B21_LOCKED.scap --verbose --recovery`
  - EFI update gets one shot to get it right, will not run again until next OS update

# Mac EFI and Mac Board IDs



# Figuring Out Compatibility

Apple has to ship a lot of EFI payloads

Does every model have its own EFI payload?

Does the EFI payload contain the info?

How can the updater know?

# Matching Specific Models With EFI

- **Apple uses various identifiers for Mac models**

- **Model ID:** `<Model><major,minor>`
- Example: **iMac17,1**
  - Minor version denotes different configs (21", 27")
  - Apple reuses these when spec bumps happen
  - In the past Apple shoved multiple configs into one single major,minor model ID
- **Board ID:** `Mac-<8 or 16 character hex string>`
- Unique for specific model and rev
- Stored on logic board, get via `ioreg -l | grep -i board-id`
- Example **iMac17,1** ==
  - `Mac-B809C3757DA9BB8D`
  - `Mac-DB15BD556843C820`
  - `Mac-65CE76090165799A`

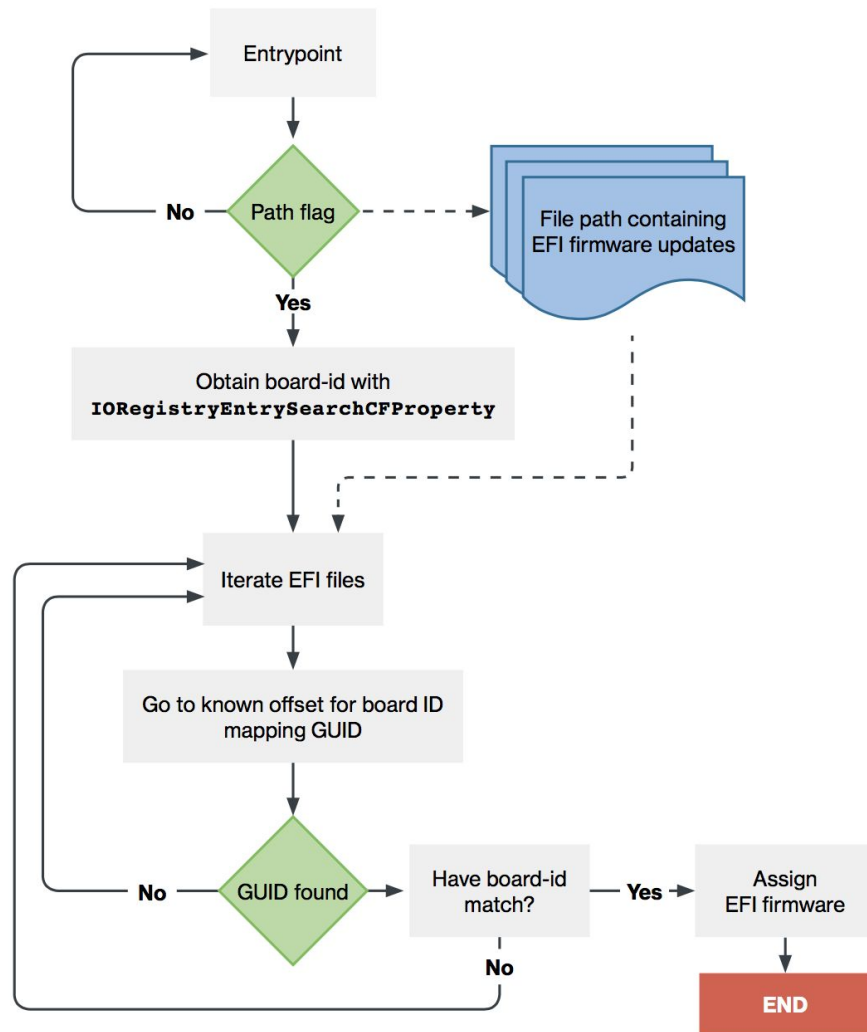
# Matching Specific Models With EFI

- **How does the firmware updater match EFI and Mac model?**
  - The EFI payload contains board IDs with which it is compatible
  - Stored in GUID **781F254A-C457-5D13-9275-1BF5D56E0724**
  - Firmware updater looks for 4-byte header **0x7C000019**
  - 8 byte chunks are used for storing compatible board IDs, up to 120 bytes
  - Represents the hex string of the board ID **Mac-B809C3757DA9BB8D**
  - Grabs board ID of Mac via **IORegistry** API
  - If match is found == use this EFI firmware bundle

# Does Every Model Get Its Own EFI Bundle?

- **Some models are rolled into a single EFI bundle**
  - Example: **MacBookAir7,1** and **MacBookAir7,2**
  - MBA 7,1 = **11"** model / MBA 7,2 = **13"** model
  - **MacBookAir7,2** EFI version string: **MBA71.0166.B26** □
  - What does this mean?
  - Some EFI payloads contain multiple board ID entries
  - GUID **781F254A-C457-5D13-9275-1BF5D56E0724** holds up to 15
  - Apple uses this GUID to group compatible models, fewer files to maintain
    - ...thus fewer files to potentially mess up (more later)

# EFI Update Flowchart



# Our Research Questions



# What Did We Want To Find Out?

How well does EFI firmware security support compare to software security support?

Are all Mac systems treated equally in terms of EFI patches?

Are all OS versions treated equally in terms of EFI patches?

How well does the real world compare to what Apple released?

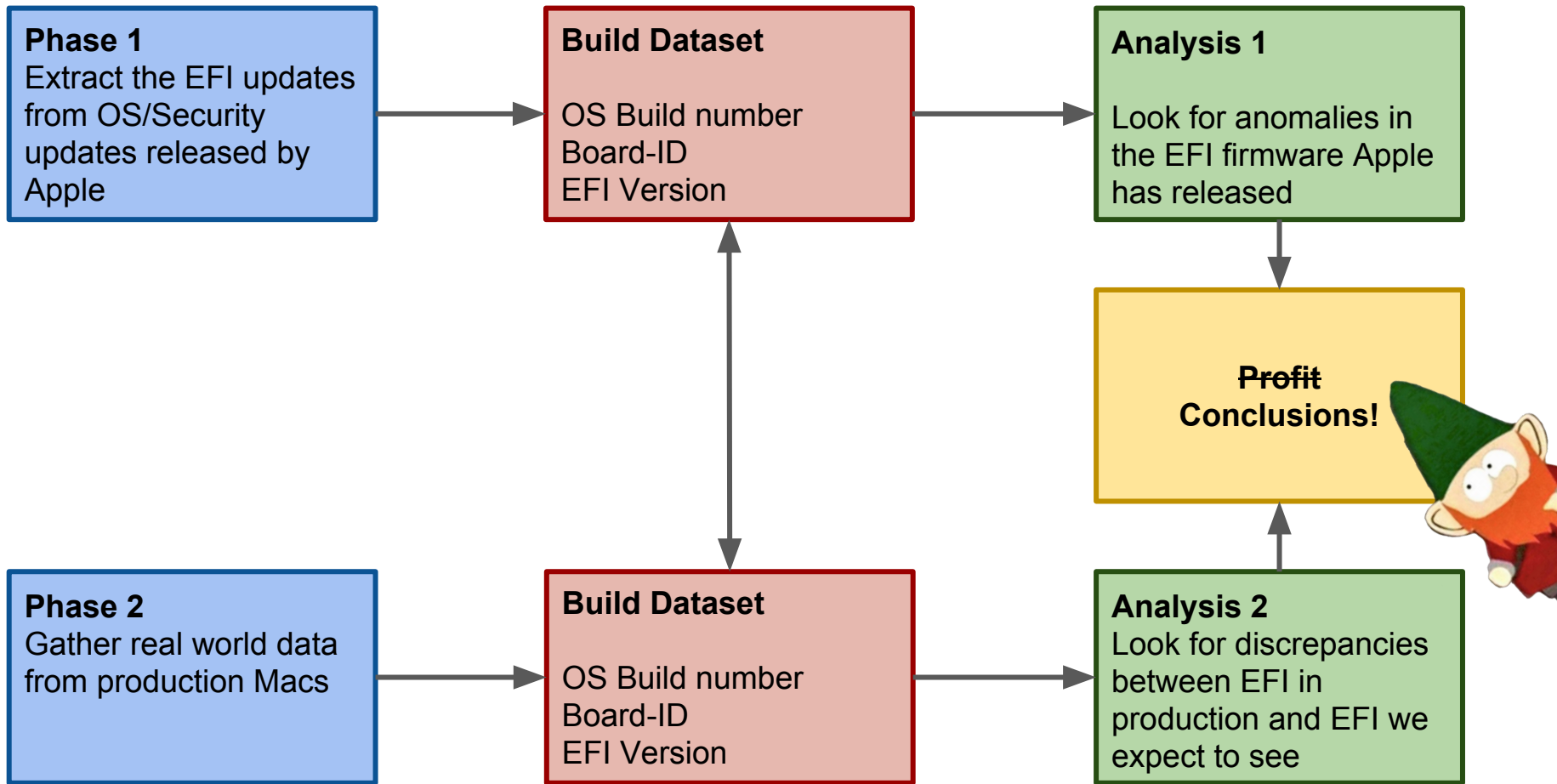
What is the visibility to EFI security support for admins & end users?

# Common EFI Update Issues

- **Do EFI updates “just work”?**
  - EFI updates are hidden, slip-streamed with OS updates
  - This must mean they *always* work and have a robust fail mode, right?
- **Do same EFI updates ship for all “supported” OS versions?**
  - If the EFI support model matches the OS one they should be identical
- **Does the real world match the ideal world?**
  - A check in the field should come back with 100% match
- **If it does not, can Apple users find out easily?**
  - Spoiler alert: not quite that simple

# The Analysis





# Phase 1 - Build a Picture of What Apple Released

- First we gathered all OS & Security updates released by Apple for 10.10, 10.11, 10.12 & 10.13
- Extracted all the EFI updates from them
- Built a dataset of triplicates, this formed an idealised baseline dataset

| OS Build number | Mac Model/Board ID             | EFI Version            |
|-----------------|--------------------------------|------------------------|
| 16G29           | IM151/<br>Mac-42FD25EABCABB274 | IMI151-0207-B29        |
| ↓               | ↓                              | ↓                      |
| 10.12.6         | iMac 27" 5K Late 2014          | EFI Ver. 0207 Build 29 |

|                                                         |            |          |          |          |          |          |          |          |          |
|---------------------------------------------------------|------------|----------|----------|----------|----------|----------|----------|----------|----------|
| com.apple.pkg.update.security.2016-006Yosemite.14F2009  | 2016/10/24 | 0118 B12 | 0118 B12 | 0179 B12 | 0207 B05 |          |          |          |          |
| com.apple.pkg.update.os.10.12.1.16B2657                 | 2016/10/24 | 0118 B13 | 0118 B13 | 0179 B13 | 0207 B07 | 0207 B03 | 0206 B01 | 0105 B09 |          |
| com.apple.pkg.update.security.2016-007Yosemite.14F2109  | 2016/12/13 | 0118 B14 | 0118 B14 | 0179 B14 | 0207 B08 |          |          |          |          |
| com.apple.pkg.update.os.SecUpd2016-003ElCapitan.15G1217 | 2016/12/13 | 0118 B14 | 0118 B14 | 0179 B14 | 0207 B08 | 0207 B04 | 0207 B04 | 0105 B08 |          |
| com.apple.pkg.update.os.10.12.2.16C67                   | 2016/12/13 | 0118 B14 | 0118 B14 | 0179 B14 | 0207 B08 | 0207 B04 | 0207 B04 | 0105 B11 |          |
| com.apple.pkg.update.os.10.12.3.16D32                   | 2017/01/23 | 0118 B17 | 0118 B17 | 0179 B17 | 0207 B11 | 0207 B07 | 0207 B07 | 0105 B15 |          |
| com.apple.pkg.update.security.2017-001Yosemite.14F2315  | 2017/03/27 | 0118 B12 | 0118 B12 | 0179 B12 | 0207 B05 |          |          |          |          |
| com.apple.pkg.update.os.SecUpd2017-001ElCapitan.15G1421 | 2017/03/27 | 0118 B13 | 0118 B13 | 0179 B13 | 0207 B06 | 0207 B03 |          | 0105 B08 |          |
| com.apple.pkg.update.os.10.12.4.16E195                  | 2017/03/27 | 0118 B20 | 0118 B20 | 0179 B21 | 0207 B16 | 0207 B11 | 0207 B11 | 0105 B20 |          |
| com.apple.pkg.update.os.10.12.5.16F73                   | 2017/05/15 | 0118 B44 | 0118 B43 | 0179 B21 | 0207 B16 | 0207 B11 | 0207 B11 | 0105 B20 | 0145 B06 |
| com.apple.pkg.update.security.2017-002Yosemite.14F2411  | 2017/05/15 |          |          |          |          |          |          |          |          |
| com.apple.pkg.update.os.SecUpd2017-002ElCapitan.15G1510 | 2017/05/15 | 0118 B20 | 0118 B20 | 0179 B21 | 0207 B16 | 0207 B11 | 0207 B11 | 0105 B20 |          |
| com.apple.pkg.update.os.MacBookProUpdate.16F2104        | 2017/06/05 | 0118 B44 | 0118 B43 | 0179 B21 | 0207 B16 | 0207 B11 | 0207 B11 | 0105 B20 | 0145 B06 |
| com.apple.pkg.update.security.2017-003Yosemite.14F2511  | 2017/07/19 |          |          |          |          |          |          |          |          |
| com.apple.pkg.update.os.SecUpd2017-003ElCapitan.15G1611 | 2017/07/19 | 0118 B20 | 0118 B20 | 0179 B21 | 0207 B16 | 0207 B11 | 0207 B11 | 0105 B20 |          |
| com.apple.pkg.update.os.10.12.6.16G29                   | 2017/07/19 | 0118 B47 | 0118 B47 | 0179 B31 | 0207 B29 | 0207 B20 | 0207 B20 | 0105 B26 | 0145 B09 |

- Looked for anomalies & discrepancies in the EFI updates Apple released
  - Which Mac models saw EFI updates and when they saw them
  - Missing EFI updates
  - Differences between the updates released for 10.10, 10.11, 10.12, 10.13
  - EFI version anomalies

## Phase 2 - Build a Picture of How EFI Looked in the Real Word

- Collected data from **73,383** Macs deployed in production
  - Same data triplicates of OS Build, Mac Model/Board-ID, and EFI version
- Of those we extracted **54,744** that were running 10.10, 10.11, 10.12
  - Older OS versions were no longer under security support by Apple
  - Old EFI is the least of their problems!!
- For any Mac model, on a specific OS version we could predict the EFI it *should* be running
- We then compared the datasets to see how well the real world matched the perfect world model built from the updates themselves



# Research Findings



# What Issues Exist?

Real world systems are out of date

Security Updates gradually drop EFI model support

Quiet failures and lack of visibility

Unexplained EFI update regressions

**Successful OS  
Update Does Not  
Mean Successful  
Firmware Update**

# Real world != perfect world

- **Data analysis reveals not all endpoints get EFI updates**
  - Gathered data from various Edu and Enterprise orgs
  - Anonymous data showing:
    - Model ID
    - OS version string
    - OS build string
    - EFI version string
  - Example: “MacBookPro10,1”, “10.12.4”, “16D25”, “MBP101.00EE.B12”
  - Compare against known-good lookup table
  - Measure non-compliant records

**Which model X, with OS version Y,  
has EFI version older than it should be?**

4.2%

**Running incorrect EFI version**

Average Across All Data

42.9%

**Most out of date model**

iMac16,2 / iMac 21" Late 2015

10%

**Highest overall OS deviancy**

macOS 10.12 Sierra

**3.4%**

**OS X 10.10 Yosemite**

Overall OS deviancy

**2.1%**

**OS X 10.11 El Capitan**

Overall OS deviancy

| Mac Model      | % Running Older-Than-Expected EFI Version | Raw Count of Systems Running Older EFI | Total Count of Systems Running Older EFI |
|----------------|-------------------------------------------|----------------------------------------|------------------------------------------|
| iMac16,2       | 43.0%                                     | 941                                    | 2190                                     |
| MacBookPro13,2 | 34.8%                                     | 114                                    | 328                                      |
| MacBookPro13,1 | 28.5%                                     | 39                                     | 137                                      |
| MacBookPro13,3 | 24.8%                                     | 78                                     | 314                                      |
| MacBookPro8,2  | 14.9%                                     | 89                                     | 598                                      |
| MacBookPro8,1  | 11.9%                                     | 59                                     | 498                                      |
| Macmini3,1     | 11.5%                                     | 6                                      | 52                                       |
| Macmini6,1     | 6.7%                                      | 13                                     | 194                                      |
| iMac16,1       | 5.2%                                      | 15                                     | 287                                      |
| MacBookAir6,1  | 5.0%                                      | 29                                     | 586                                      |
| MacBook9,1     | 4.9%                                      | 10                                     | 206                                      |
| Macmini7,1     | 4.8%                                      | 50                                     | 1035                                     |
| MacBookAir4,1  | 4.4%                                      | 6                                      | 138                                      |
| MacBookPro8,3  | 4.4%                                      | 3                                      | 69                                       |
| iMac13,1       | 4.1%                                      | 86                                     | 2119                                     |
| MacBookAir6,2  | 3.6%                                      | 81                                     | 2244                                     |

**Software Secure  
But Firmware  
Vulnerable**

# Does “Supported OS” Mean “Supported EFI”?

- **Apple has a “soft” support deprecation schedule**
  - Only Apple truly knows what this schedule is exactly
  - Roughly “N-2” model
  - Security Updates (`SecUpd<20xx>-<yyy>`) are subsets of current OS update
    - As name implies security patches only + EFI updates
  - Some of this is because issues don’t affect older OS versions
  - But also because Apple just chose not to backport & QA (`ntp`, **Broadpwn**)
- **Security updates also quietly drop certain EFI updates in current OS updates**
  - Not current == Security updates == EFI quietly stops getting updates
  - Only way to be sure of broadest coverage: **run current OS and update immediately**

# EFI coverage by update:

macOS Sierra 10.12.6 Update

El Capitan Security Update 2017-003

Yosemite Security Update 2017-003

43

EFI bundles

Sierra 10.12

31

EFI bundles

El Capitan 10.11

1

EFI bundle

Yosemite 10.10

**A patch for one  
does not mean a  
patch for all**

# One patch to rule them all?

- Apple states in their update notes when **EFI vulnerabilities** are fixed, but it does not give details for exactly which **Mac models** they patch
- We looked at which models of Mac Apple released EFI updates for that addressed 4 high impact public EFI vulnerabilities
  - **CVE-2014-4498** - (Thunderstrike 1)
  - **CVE-2015-3692** - (Thunderstrike 2)
  - **CVE-2015-7035** - (“An attacker can exercise unused EFI functions”)
  - **CVE-2016-7585** - (Ulf Frisk’s DMA attack)

**Mac models that did not  
have EFI updates released  
for each vulnerability**

**47**

Thunderstrike 1

**31**

Thunderstrike 2

**25**

CVE-2015-7035

**22**

CVE-2016-7585

# Some Models Are EFI Orphans

# Do All OS Supported Models Get EFI Updates?

- **Apple has spotty coverage for certain “supported” models**
  - A number of models are supported by current OS and updates
  - The OS updates have not bundled EFI updates for these models
  - Other models were seen with only “factory” EFI, no further updates
    - Factory EFI: low-numbered <model>.<major>.BXX version
    - **MBPXXY.NNNN.B00**
  - This adds to the incorrect assumption that they are fully secure

# Models Lacking EFI Updates

16

Models not receiving  
any EFI updates

18

Models with only  
factory EFI versions

# EFI Firmware Factory

| Mac Model | EFI Versions Observed in the Real World Data |                |               |
|-----------|----------------------------------------------|----------------|---------------|
| IM101     | IM101.00CC.B00                               |                |               |
| IM71      | IM71.007A.B00                                | IM71.007A.B01  | IM71.007A.B03 |
| IM81      | IM81.00C1.B00                                |                |               |
| IM91      | IM91.008D.B00                                | IM91.008D.B04  | IM91.008D.B08 |
| MB51      | MB51.007D.B03                                | MB51.0073.B06  |               |
| MB52      | MB52.0088.B06                                |                |               |
| MB61      | MB61.00C8.B00                                |                |               |
| MBA21     | MBA21.0075.B03                               | MBA21.0075.B05 |               |
| MBP31     | MBP31.0070.B07                               |                |               |
| MBP41     | MBP41.00C1.B03                               |                |               |
| MBP51     | MBP51.007E.B05                               | MBP51.007E.B06 |               |
| MBP52     | MBP52.008E.B05                               |                |               |
| MBP53     | MBP53.00AC.B03                               |                |               |
| MBP55     | MBP55.00AC.B03                               |                |               |
| MM31      | MM31.00AD.B00                                | MM31.0081.B06  |               |
| MP31      | MP31.006C.B02                                | MP31.006C.B05  |               |
| MP41      | MP41.0081.B04                                | MP41.0081.B07  | MP41.0081.B08 |
| MP51      | MP51.007F.B00                                | MP51.007F.B01  | MP51.007F.B03 |

This table lists Mac models from the real world dataset that have only been observed with one, two or three updates with low build numbers. This suggests they haven't been updated from the versions of firmware they were originally shipped with from the factory - making them likely to contain unpatched vulnerabilities.

**Silent Updates Will  
Also Fail Silently**

# Do Failed Updates Generate Alerts?

- **Apple designed the process to be silent to end users**
  - This means it gets one shot to succeed
  - No retries outside of OS/Security updates until next version
  - No error logging or notification happens
  - User will not find out unless they know where to look for EFI version
  - Since EFI is an unknown system to users and many Mac admins it goes ignored
  - Result: EFI is often out of date

**QA Failure?**  
**Incorrect EFI**  
**Firmwares**  
**Released**

# Are You Getting the EFI Updates You Should?

- **Apple sometimes has QA failures**
  - We identified EFI version regression issues with **OS X 10.10 & 10.11**
  - As part of the **Security Update 2017-001** (Mar 27, 2017)
  - For unexplained reasons included EFI bundles were:
    - **Older** than preceding SecUpd **2016-003**
    - **Same** as prior SecUpd **2016-002**
  - Example:
    - **MBP112**
      - SecUpd 2016-002 = **MBP112.0138.B17**
      - SecUpd 2016-003 = **MBP112.0138.B18**
      - SecUpd 2017-001 = **MBP112.0138.B17**

| Mac Model | Security Update 2017-001 (10.11)<br>[Released March 27, 2017] | Security Update 2016-003 (10.11)<br>[Released Dec 13, 2016] | Security Update 2016-002 (10.11)<br>[Released Oct 24, 2016] |
|-----------|---------------------------------------------------------------|-------------------------------------------------------------|-------------------------------------------------------------|
| IM121     | 0047 23B                                                      | 0047 25B                                                    | 0047 23B                                                    |
| IM131     | 010A B09                                                      | 010A B0A                                                    | 010A B09                                                    |
| IM141     | 0118 B13                                                      | 0118 B14                                                    | 0118 B13                                                    |
| IM142     | 0118 B13                                                      | 0118 B14                                                    | 0118 B13                                                    |
| IM143     | 0118 B13                                                      | 0118 B14                                                    | 0118 B13                                                    |
| IM144     | 0179 B13                                                      | 0179 B14                                                    | 0179 B13                                                    |
| IM151     | 0207 B06                                                      | 0207 B08                                                    | 0207 B06                                                    |
| IM161     | 0207 B03                                                      | 0207 B04                                                    | 0207 B03                                                    |
| MB81      | 0164 B14                                                      | 0164 B19                                                    | 0164 B14                                                    |
| MB91      | 0154 B05                                                      | 0154 B09                                                    | 0154 B05                                                    |
| MBA41     | 077 B14                                                       | 077 B15                                                     | 077 B14                                                     |
| MBA51     | 00EF B04                                                      | 00EF B05                                                    | 00EF B04                                                    |
| MBA61     | 0099 B22                                                      | 0099 B23                                                    | 0099 B22                                                    |
| MBA71     | 0166 B12                                                      | 0166 B13                                                    | 0166 B12                                                    |
| MBP81     | 0047 2CB                                                      | 0047 2DB                                                    | 0047 2CB                                                    |
| MBP91     | 00D3 B0D                                                      | 00D3 B0E                                                    | 00D3 B0D                                                    |
| MBP101    | 00EE B0A                                                      | 00EE B0B                                                    | 00EE B0A                                                    |
| MBP102    | 0106 B0A                                                      | 0106 B0B                                                    | 0106 B0A                                                    |
| MBP112    | 0138 B17                                                      | 0138 B18                                                    | 0138 B17                                                    |
| MM51      | 0077 B14                                                      | 0077 B15                                                    | 0077 B14                                                    |
| MM61      | 0106 B0A                                                      | 0106 B0B                                                    | 0106 B0A                                                    |
| MM71      | 0220 B07                                                      | 0220 B08                                                    | 0220 B07                                                    |
| MP61      | 0116 B17                                                      | 0116 B21                                                    | 0116 B17                                                    |

# Can You Downgrade EFI?

- **Firmware updates can not be downgraded**
  - In our testing we were unable to force older versions
  - The `efiupdater` binary only allows higher versions
    - There is a force flag but this just forces setup, not flash
  - If the version of the target EFI bundle is lower it exits
  - Unable to spoof by altering EFI bundle version due to signing
  - Unable to spoof by altering `efiupdater` due to signing
  - This made the EFI updates in SecUpd 2017-001 for 10.10/.11 just stale code

# Mitigations



# What Can We Do About It?

Upgrade to macOS 10.13

Logging and reporting

Run updates out of band

Apple is addressing some things

# Update to macOS 10.13 High Sierra

- **macOS 10.13 includes EFI updates for supported models**
  - APFS requires EFI support - thus EFI updates
  - Includes Mac Pro tower models (MacPro5,1)
    - This model requires a manual update, special case in Install Assistant
  - Some older models saw their first-ever update since 2015
    - iMac (Late 2009) aka iMac10,1
    - MacBook (Late 2009) aka MacBook6,1
    - Mac Pro (Mid-2010) aka MacPro5,1
  - *Apple actually started shipping these EFI updates in 10.12.5*

# What's new with macOS 10.13 High Sierra?

- macOS 10.13 High Sierra contains new tools

- Apple is focusing on EFI integrity with `eficheck`
- No signs of actively updating out of date EFI versions (yet)
- Combined standalone tool and daemon (runs once a week)
  - `/usr/libexec/firmwarecheckers/eficheck/eficheck`
- Gets checksum of current EFI firmware
- Compares to Apple-shipped and code signed whitelist
- Apple ships partial whitelist with 10.13
- Downloads full whitelist if needed
- If checksum not found in whitelist: alert user
- ...the UX is not great yet ☐

 **Xeno Kovah** @XenoKovah

So I hear macOS 10.13 comes out soon. Let's talk about what's up if you ever see this prompt [thread] [https://pbs.twimg.com/media/DKgDB\\_AUMAArRkB.jpg](https://pbs.twimg.com/media/DKgDB_AUMAArRkB.jpg)

 Twitter | Yesterday at 1:49 PM (28kB) ▼



**Your computer has detected a potential problem**

Click "Send to Apple" to submit a report to Apple.



Show Report

Don't Send

Send to Apple

# Logging and Reporting

- Since the OS does not log we must do it ourselves
  - Use endpoint reporting tools
    - **osquery:** `/usr/local/bin/osqueryi "select version from platform_info"`
    - **Puppet:** `/usr/local/bin/facter system_profiler.boot_rom_version`
    - **Chef:** `/opt/chef/bin/ohai hardware/boot_rom_version`
    - **Shell script:**  
`/usr/sbin/system_profiler SPHardwareDataType | awk '/ROM/{print $4}'`
  - Once we have data we can move on to fixing divergent endpoints:
    - Re-install current OS or Security update to re-apply EFI
    - Use **efiupdater** as shown in paper to kick off EFI update
  - <https://blog.kolide.com/check-the-efi-version-of-a-mac-with-osquery-f98c6e3beffa>
  - [https://github.com/trailofbits/osquery-pr/tree/alessandro/feature/macos\\_efigy\\_support](https://github.com/trailofbits/osquery-pr/tree/alessandro/feature/macos_efigy_support)

# Apply Updates Out of Band

- **Don't wait for next OS/Security Update**

- Re-apply the update
- Requires a restart in any case
- If re-applying OS update: use Combo updater
  - Larger but considered best practice
  - Less chance of failures
- Security Update is always Delta
- Other option: create standalone installer for firmware updates only
  - Requires some custom work
  - Will always require a reboot, properly set user expectations
- <https://github.com/grahamgilbert/imagr/wiki/High-Sierra-Notes#firmware>

# Tool and API Releases



# EFIgy - API and Tools to Help Visibility

- **As we discussed visibility to the state of your EFI and its security is hard**
- EFIgy is free RESTful API and open source client that gives you access to the data that we built up during our research
  - Identifies if you are running the most up-to-date EFI version for your Board-ID and OS Build combination
  - Highlight areas of security concern we have spoken about today such as Mac models that are not receiving EFI updates
  - CVE's that a particular EFI version may be vulnerable to
- Supports OS versions 10.10 through 10.13

# EFIGy CLI App

efigy.io

```
EFIgylite API Information:
  API Version: 0.2
  Updated On: Oct 13 2017, 17:42

-----
Endpoint: 127.0.0.1
  # Enumerated system informaton (This data will be sent to the API in order to determine if you are running the latest version of the OS)

  Hashed SysUUID   : 44c3cfc6f15da575636ebb88a78d7c88c54dabdb60ffaddcb8d7c02845955710
  Hardware Version : MacBookPro13,2
  EFI Version      : MBP132.0226.B25
  SMC Version      : 2.37f20
  Board-ID         : Mac-66E35819EE2D0D05
  OS Version       : 10.12.6
  Build Number     : 16G29

[?] Do you want to continue and submit this request? [Y/N]  y

  # Results:

  EFI firmware version check:
    [+] SUCCESS - The EFI Firmware you are running (None) is the expected version

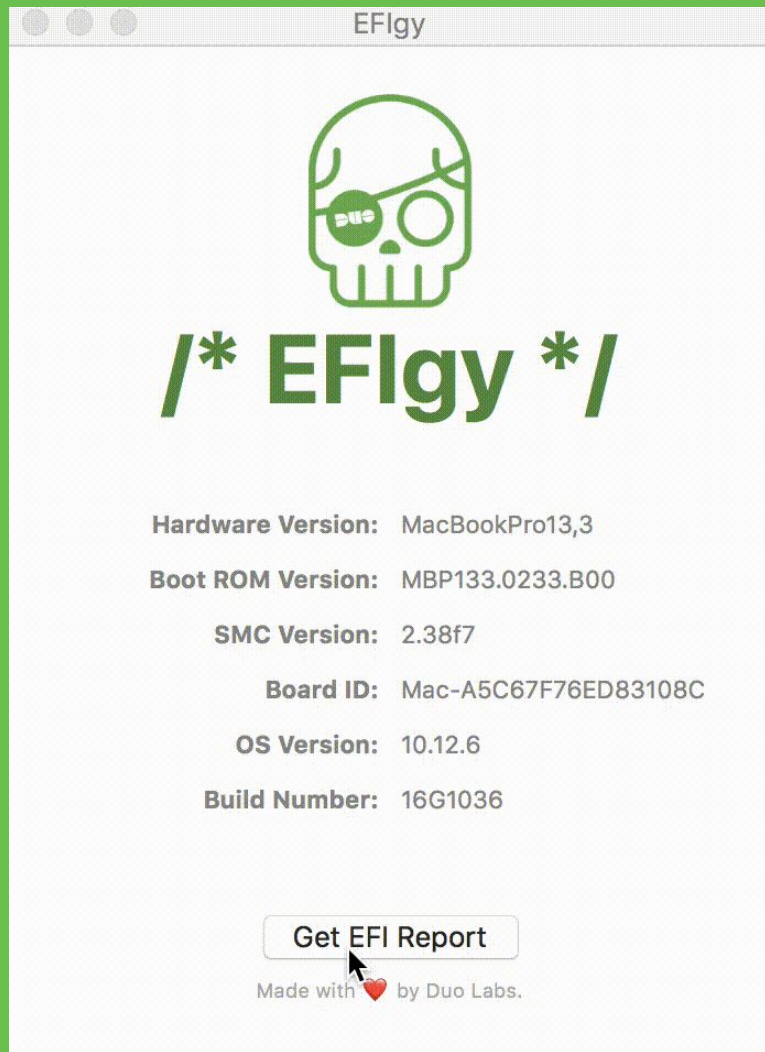
  Highest build number check:
    [+] SUCCESS - You are running the latest build number (16G29) of the OS version

  Up-to-date OS check:
    [+] SUCCESS - You are running the latest major/minor/micro version of the OS

-----
```

# EFlgy GUI App

[github.com/duo-labs/EFlgy-GUI](https://github.com/duo-labs/EFlgy-GUI)



# EFIGy Web App

api.efigy.io

Secure | https://api.efigy.io

Home About

## Check your EFI version

EFI Version Number  How?

Looks like "MBP142.0167.B00"

Mac Model ID How?

Provide models in the form of "MacBookPro5,1" for Mac Pro (Late 2013)

Build Number How?

Looks like "16G29"

NOTE: macOS 10.13 is NOT currently supported. Our dataset currently only covers 10.10, 10.11, and 10.12.

Go

© Duo Labs 2017

Made with  by Duo Labs

**efigy.io**  
**(github)**

# EFlgy API data

Up to date API data and graphs here



Demo  
Time

# Conclusions



# Conclusions

- Transparency is key - vendors should be clear with what they patch
- Systems can be *‘software secure but firmware vulnerable’*
- Not all hardware may be treated equally
- QA is hard! Looking into the firmware being received is a good idea
- EFI is like a full OS in many ways:
  - It affects everything running above it (ring -2 remember!)
  - You should keep it up to date to not undermine the rest of your security
  - It needs to have notifications and alerts for updates like software does
- Apple is taking EFI security seriously and is continuing to lead the way

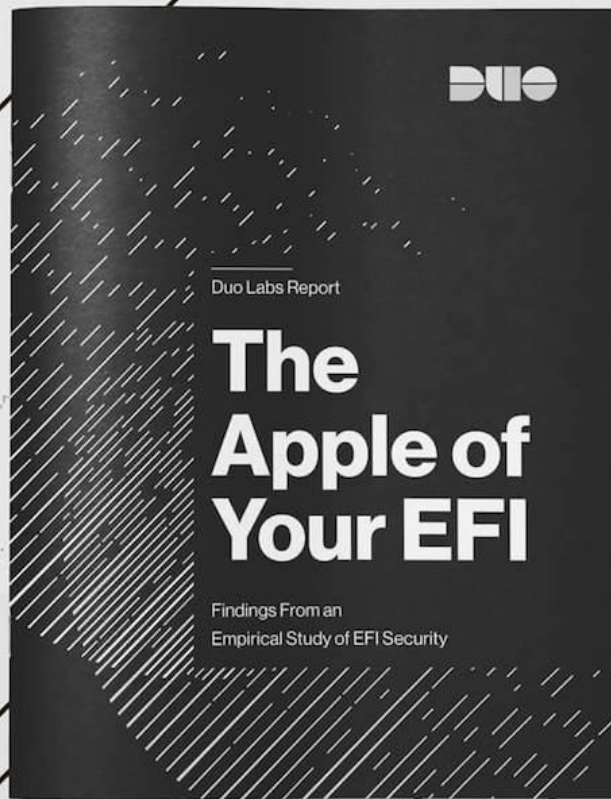
**Lots more information  
in our technical paper**

**<http://duo.sc/2x1AA9R>**

**And Blogpost**

**<http://duo.sc/2ychJhh>**

**EFIgy Tools**  
**<https://efigy.io>**



# Thanks!

If you've got Q's, we've got A's...\*

**Pepijn Bruienne** (@bruienne)

**Rich Smith** (@iodboi)



\* We hope!