

The background of the slide features a large, faint, circular watermark of the University of Oxford seal. The seal contains the text "UNIVERSITY OF OXFORD" around the perimeter and "DOMINI REGNO" in the center.

# Apple Device Administrator's Meeting

IT Services, University of Oxford  
Hilary Term, 2018

# Agenda

12:30 - Introduction

12:35 - Ben Goodstein: macOS 10.13 and the iMac Pro  
for Administrators

12:50 - Q&A

12:55 - Chris Beard: Meltdown and Spectre: Staying  
Safe

13:10 - Q&A/Discussion

# macOS 10.13 and the iMac Pro

Ben Goodstein, Technical Leader (Apple)  
IT Services, University of Oxford  
@fuzzylogiq - Twitter, Github & Macadmins Slack

# macOS 10.13 & iMac Pro Admin Changes

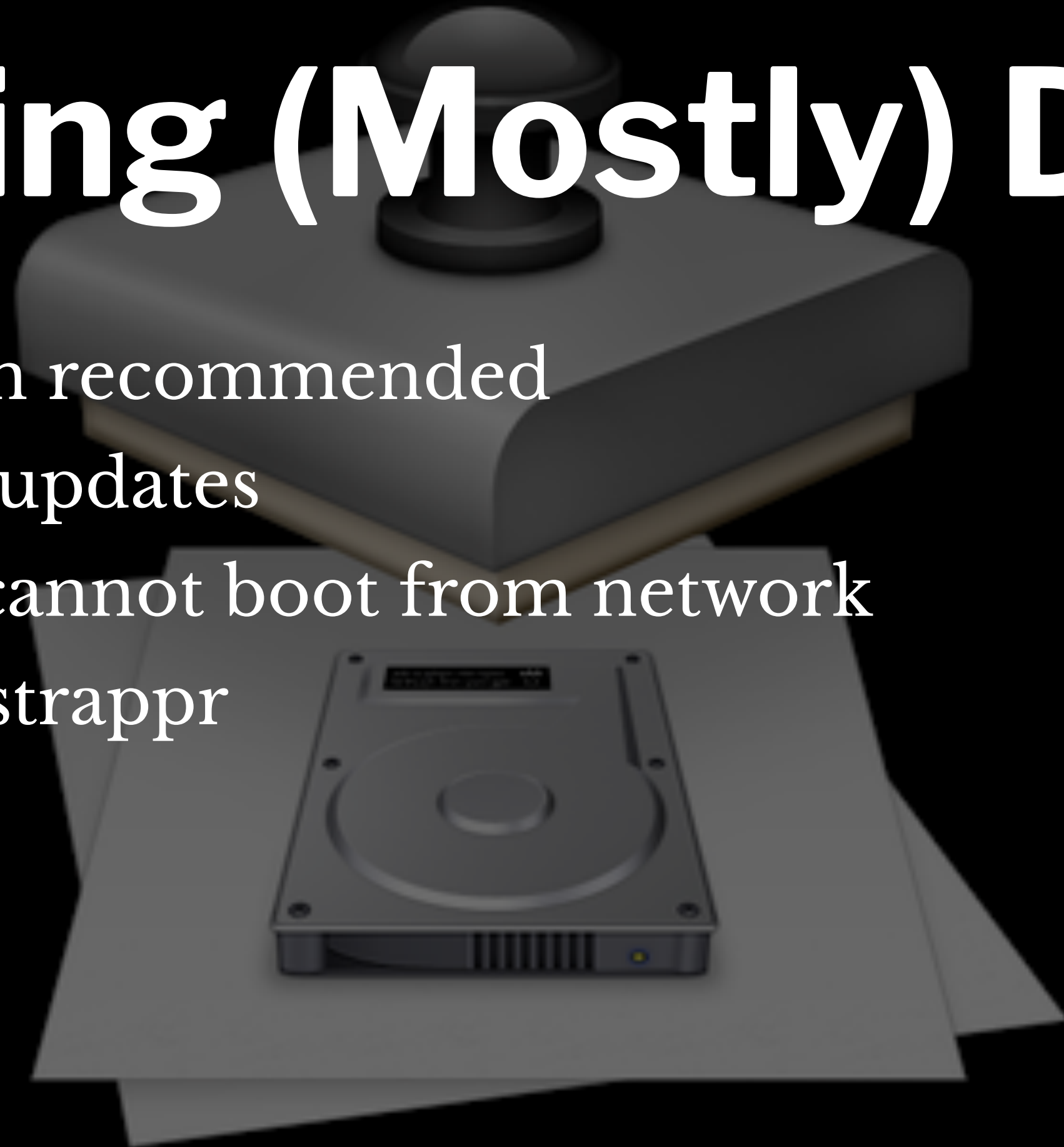
- Imaging (mostly) dead
- APFS - APple File System
- Secure Token - For Encryption
- UAKEL - User Approved Kernel Extension Loading
- UAMDM - User Approved MDM
- Secure Boot





# Imaging (Mostly) Dead

- Installation recommended
- Firmware updates
- iMac Pro cannot boot from network
- DEP/bootstrapp



# APFS - New File System

The background of the slide is a grayscale image of an Apple Internal Hard Disk. The disk is rectangular with a central circular area featuring the Apple logo. At the top, there is a label that reads "Internal Hard Disk". The disk is secured with four screws at the corners. The overall image is slightly faded to serve as a background for the text.

- Not readable by 10.12
- Cannot go back to 10.12 without reformatting as HFS+
- Unknown side-effects of downgrading
- Everything converted except Fusion & HDD

# Secure Token for Encryption

- Allows use to add/remove users from FileVault
- First user created with Setup Assistant to log in
  - or first mobile account (if created by macOS)
- Won't work if created with scripts
- Use `sysadminctl` to check and grant/revoke other accounts

# User Approved Kernel Extension Loading (UAKEL)

- Users must accept kernel extensions in Sys Prefs
- If they don't they won't run (unless installed before upgrade)
- AntiVirus, Tablet Drivers etc.
- Only way to avoid is to enrol in MDM
- But...



# User Accepted Mobile Device Management (UAMDM)

- Introduced in 10.13.2
- Users must accept enrolment into MDM
- Cannot be done remotely
- Only way to avoid is to use DEP
- Will allow you to whitelist kexts



CONFIG

# Secure Boot

- Introduced with the iMac Pro/T2
- Boot only trusted/signed macOS/BootCamp
- Can be managed with Startup Security Utility in Recovery
- Also control whether iMac Pro can boot external
- `systemsetup` can no longer boot to another partition

# References

## Imaging

- <https://support.apple.com/en-us/HT208020>
- <https://scriptingosx.com/2017/10/imaging-is-dead/>
- <https://github.com/munki/bootstrappr>

## Secure Token

- <https://derflounder.wordpress.com/2018/01/20/secure-token-and-filevault-on-apple-file-system/>

## UAKEL/UAMDM

- [https://developer.apple.com/library/content/technotes/tn2459/\\_index.html](https://developer.apple.com/library/content/technotes/tn2459/_index.html)
- <https://derflounder.wordpress.com/2017/08/24/kernel-extensions-and-macos-high-sierra/>
- <https://support.apple.com/en-us/HT208019>

## Secure Boot

- <https://support.apple.com/en-gb/HT208330>
- <https://twocanoes.com/secureboot-imac-pro/>

**Any**

**Questions?**