security
engineering
capability

COMP6445 – Digital Forensics

15th October 2019

INTRODUCTION – Michael Heikkilae

•

IT Industry – 20+ years
NSW Police Force – 12 years

Current Position: Digital Forensics Specialist

Windows user from 1990 to 2018 before migrating to Linux (Arch, Ubuntu Server) / FreeBSD

Vintage computer ~~hoarder~~ aficionado:

- Apple Mac Classic /

COMING UP IN THIS LECTURE...

- Apple property list (.plist) files

- Apple file systems (HFS+ and APFS) and encryption

- Apple T2 SoC

- A brief introduction to *Forensic Explorer*

- Q&A session

.PLIST FILES – WHAT ARE THEY?

Used by Apple MacOS and iOS (among others), property list files store data such as configuration settings and other information used by applications.

Can be in XML[1], JSON[2] or Binary format.

Can be a very valuable source of information and forensic artefacts, including passwords, password hashes and binary data.

[1] Introduced in Apple Mac OS X 10.0 (Cheetah)
[2] Introduced in Apple Mac OS X 10.7 (Lion)

APPLE FILE SYSTEMS

HFS
Hierarchical File System
Introduced in 1985
Maximum volume size of 2TB

HFS+
Hierarchical File System Plus
Introduced in 1998
Can be used with FileVault 2 volume encryption (Mac OS X 10.7 and above)

APFS
Apple File System
Introduced in 2017 with Apple macOS 10.13 (High Sierra)
Native support for full-disk encryption and single or multi-key file encryption

How APFS differs from HFS/HFS+

- Adds support for single or multi-key file based encryption

- Supports point-in-time snapshots

- No support for fusion drives (hybrid magnetic disk and SSD)

- No support for NVRAM (RAM disks)

- Limited or no support by some DF tools

APFS

Originally slow to implement, most industry standard digital forensic tools support APFS, including:

Magnet AXIOM 3.0
BlackBag Macquisition 2018 R1 (Logical only)
BlackBag BlackLight 2018 R1
OpenText EnCase 8.07
X-Ways Forensics 19.7
ADF DEI 1.4
Nuix Investigator 7.6

Still **not** supported by Forensic Explorer (as at 10/10/2019)

ENCRYPTION & APFS

APFS introduces native support for encryption.

By default, encryption is **off** (except in machines with T2 SoC).

Enabling FileVault 2 encrypts APFS volumes at the file system level using XTS-AES-128 (same as Microsoft Bitlocker in Windows 10).

Individual files can be encrypted with their own individual encryption key.

T2 SoC

Introduced in all Apple computers from:

- iMac Pro (December 2017)

- Mac mini (2018)

- Macbook Air (2018 and later)

- Macbook Pro (2018 and later)

T2 SoC

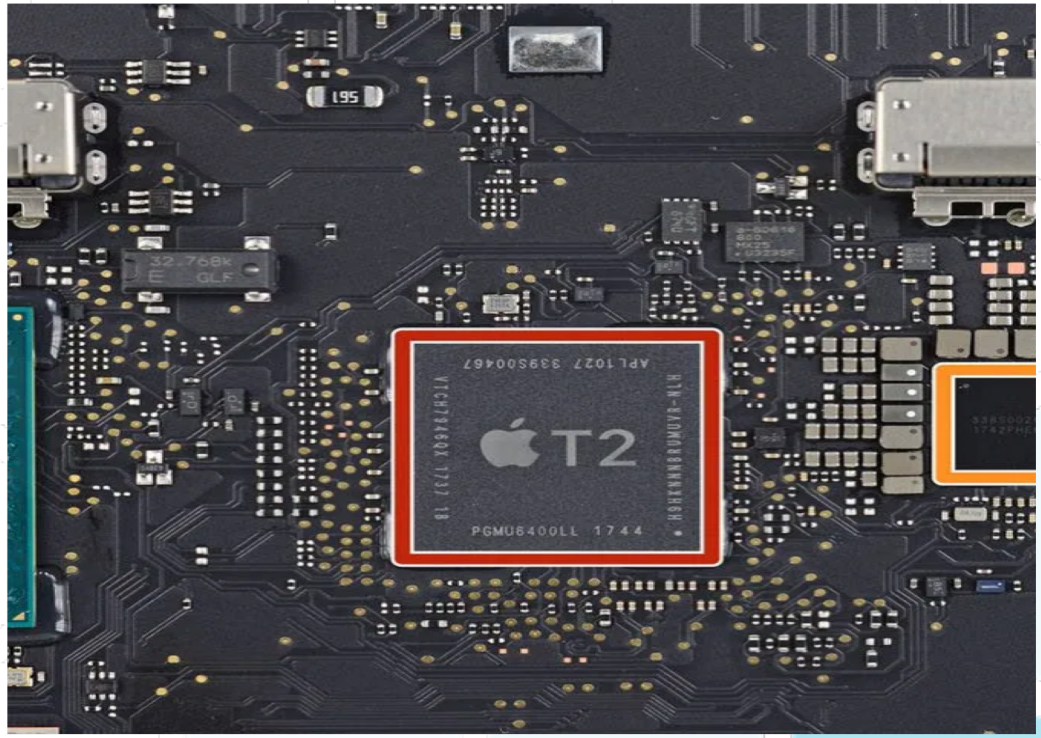
- Custom designed System on Chip

- Integrates SMC, Audio/Video & Disk Controllers

- AES Crypto engine with 256-bit encryption

- Media key stored in T2 chip

- Introduces Secure Boot options



T2, APFS & FILEVAULT 2

- Data on SSDs is encrypted in machines with T2 (cannot be disabled).

- FileVault 2 is disabled by default and encrypted volumes mount automatically.

- With FileVault 2 disabled, disks can be examined in Target Disk Mode.

- Encryption keys are stored on T2 and disks are locked to a machine.

- Enforces limited password attempts (180 attempts in total before drive erasure)

T2, APFS & FILEVAULT 2

- Data on SSDs is encrypted in machines with T2 (cannot be disabled).

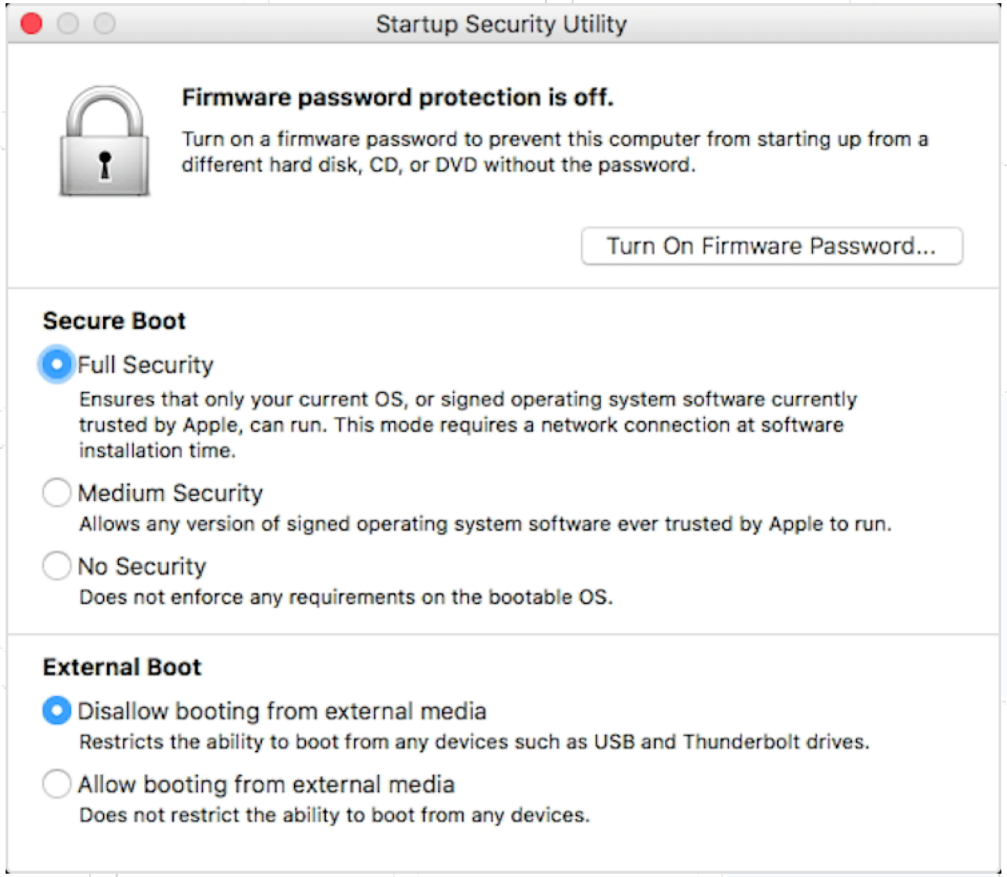
- FileVault 2 is disabled by default and encrypted volumes mount automatically.

- With FileVault 2 disabled, disks can be examined in Target Disk Mode.

- Encryption keys are stored on T2 and disks are locked to a machine.

- Enforces limited password attempts (180 attempts in total before drive erasure)

T2 Secure Boot



AN INTRODUCTION TO FORENSIC EXPLORER

QUESTIONS?

Michael HEIKKILAE
m.heikkilae@unsw.edu.au