HOCHSCHULE MITTWEIDA
University of Applied Sciences

Fraunhofer SIT

Bundeskriminalamt

Betriebssysteme

macOS - Teil1

Autor: Prof. Ronny Bodach

macOS Agenda

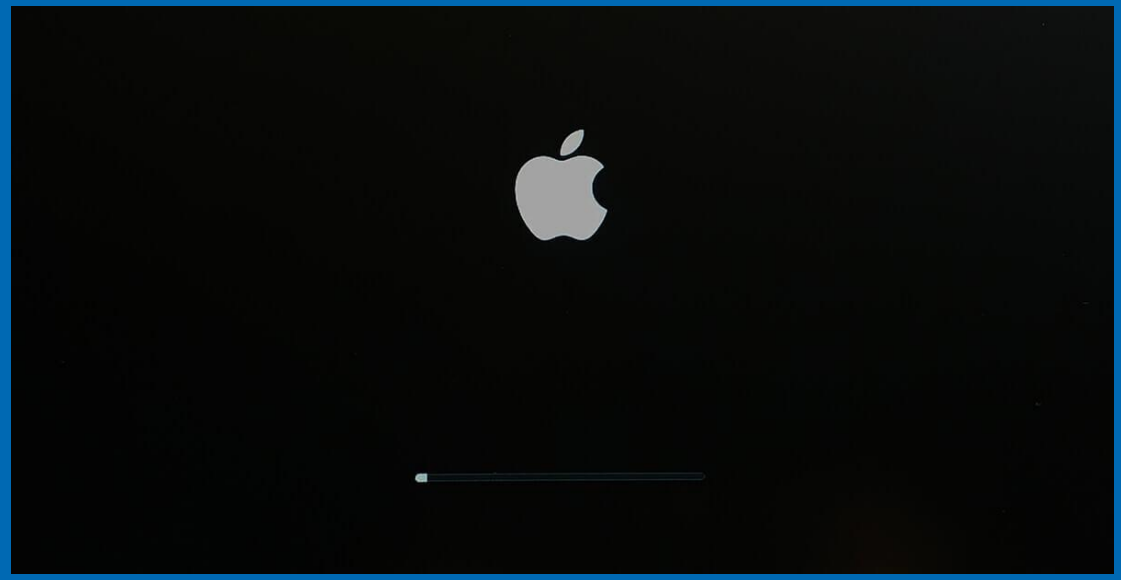
1. Einführung in macOS
2. macOS Bedienung
3. macOS Lab & Image Einbindung
4. Bootcamp Besonderheiten (& Parallels)
5. Mac FHS und Speicherstrukturen
6. Datenformate SQLite und Plist
7. Zuletzt genutzte Elemente & Nutzeraktivitäten
8. Spotlight und erweiterte Metadaten
9. Gelöschte Dateien
10. Schlüsselbund
11. Logdateien
12. Mac Disk Images
13. Time Machine und lokale Backups
14. Kommunikations-Apps
15. Browser Artefakte
16. Cloud
17. iOS Backups

macOS
Agenda

1. Einführung in macOS
   - Historie
   - Aufbau
   - Sicherheitsfeatures

BETRIEBSSYSTEM macOS

Einführung



Betriebssystem macOS

Geschichtliches:

Das auf Unix basierende Mac OS X ist die zehnte Ausgabe des Apple eigenen Betriebssystems für Macintosh Computer. Die ursprünglich auf Motorola Chipsätzen basierten Apple Computer wurden zwischenzeitlich ausschließlich mit Intel Chipsätzen hergestellt. Derzeit wird der Umstieg von Intel auf ARM Technologie durchgeführt.

Im September 2000 wurde die erste OSX Beta (Kodiak) an die Entwickler verteilt.

Bis einschließlich Version 10.7 hieß das Betriebssystem Mac OS X ab 10.8 wurde es nur noch OS X genannt mit der Einführung von 10.12 wurde es erneut umbenannt und heißt nun macOS.

Betriebssystem macOS

Mac OS (X) Versionen:

Mac OS X Public Beta – code name Kodiak	OS X Yosemite – 10.10 (free)
Mac OS X 10.0 – code name Cheetah	OS X El Capitan – 10.11 (free)
Mac OS X 10.1 – code name Puma	macOS Sierra – 10.12 (free)
Mac OS X 10.2 – also marketed as Jaguar	macOS High Sierra – 10.13 (free)
Mac OS X Panther – 10.3	macOS Mojave – 10.14 (free)
Mac OS X Tiger – 10.4	macOS Catalina – 10.15 (free)
Mac OS X Leopard – 10.5	macOS 11.0: Big Sur (2020)
Mac OS X Snow Leopard – 10.6 (requires purchase)	macOS 12.0: Monterey (2021)
Mac OS X Lion – 10.7 – OS X Lion (requires purchase)	macOS 13.0: Ventura (2022)
OS X Mountain Lion – 10.8 (requires purchase)	macOS 14.0: Sonoma (2023)
OS X Mavericks – 10.9 (free)	macOS 15.0: Sequoia (2024)

Betriebssystem macOS

Modellpalette:

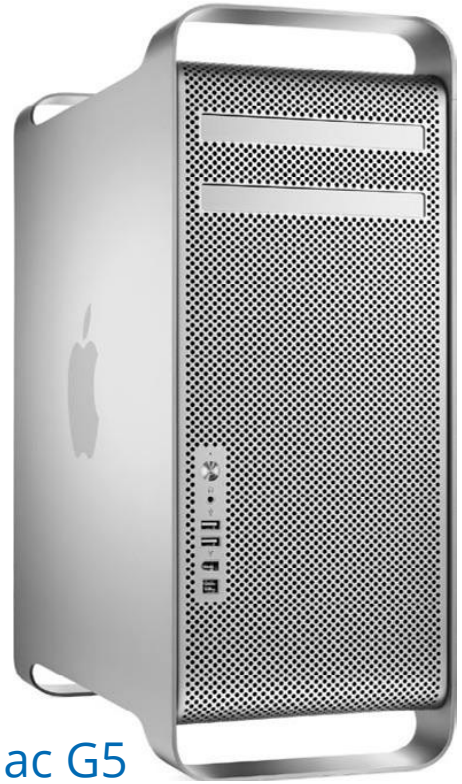
Mac Book Pro 2008

iMac G3

Mac G4

Betriebssystem macOS

Modellpalette:



Power Mac G5

Mac Book Pro

Mac Book Air

iMac 5

Betriebssystem macOS

Modellpalette:

Mac Mini

Apple TV

Betriebssystem macOS

Modellpalette:

Time Capsule

AirPort Extreme

Betriebssystem macOS

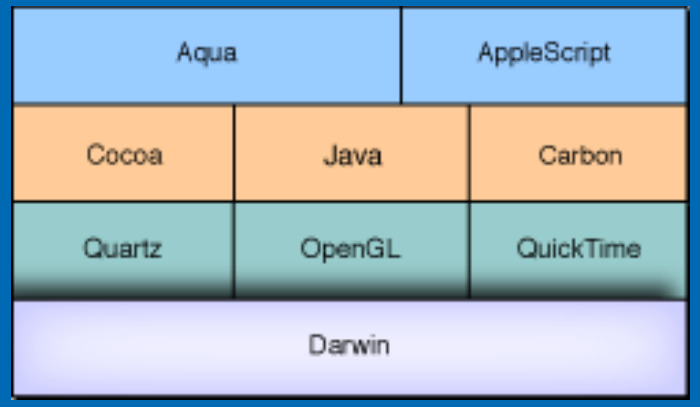
Modellpalette:

Mac Mini M2

Mac Pro M2

BETRIEBSSYSTEM macOS

Aufbau & Grundlagen



Betriebssystem macOS

Grundaufbau von OSX

OSX ist in vier Schichten aufgebaut:

1. **Benutzerebene** - Aqua, die grafische Benutzerschnittstelle (GUI)
2. **Anwendungsprogrammierebene** - Programmierschnittstellen (APIs) wie Cocoa (und früher Carbon), Java
3. **Bereitstellungsebene** - Grafik-Subsystem (Quartz mit Quartz Compositor, OpenGL), Audio/Video (QuickTime) etc.
4. **Basisebene** - Darwin, das Kern-Betriebssystem

Betriebssystem macOS

Grundaufbau von OSX

OSX ist ein Nachkomme von NeXTSTEP und genau genommen eine (proprietäre) Software-Distribution, wobei Darwin, die Basisebene von BSD abgeleitet ist, und damit ein (freies) Unix, das eigentliche Betriebssystem ist.

Durch Darwin (vererbt aus BSD) verfügt OS X über Fähigkeiten wie Speicherplatzschutz, präemptives Multitasking, Mehrbenutzerfähigkeit, erweitertes Speichermanagement und symmetrisches Multiprocessing (SMP). Darwin wurde unter die quelloffene Lizenz Apple Public Source License gestellt.

Betriebssystem macOS

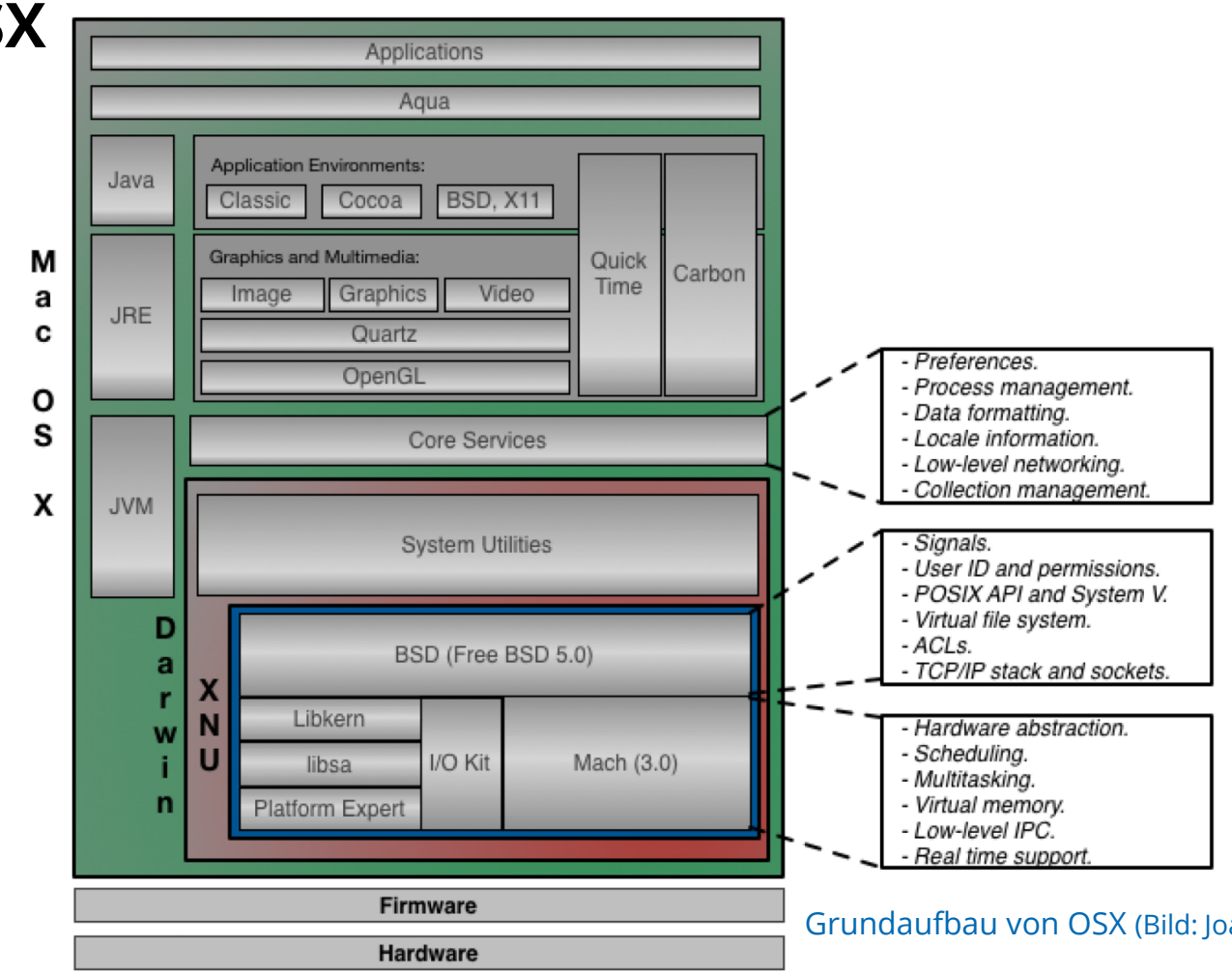
Grundaufbau von OSX

Der Kernel wurde gegenüber NeXTStep vollkommen überarbeitet - während NeXTStep noch einen reinen Mach-Mikrokernel verwendete, setzt OS X bzw. Darwin auf einen sogenannten Hybridkernel: Dabei werden einige Funktionen in den Kernel integriert, allerdings nicht so viele wie bei einem monolithischen Kernel.

Als Basis Kernel wurde weiterhin Mach verwendet und mit Teilen des monolithischen FreeBSD Kernel ergänzt. Der Kernel heißt XNU (X is Not Unix).

Betriebssystem macOS

Grundaufbau von OSX



Grundaufbau von OSX (Bild: Joaquín Moreno Garijo)

Betriebssystem macOS

Unterstützte Dateisysteme:

Mac OS X nutzte das Dateisystem HFS und dessen Erweiterung HFS+. Dieses von Apple entwickelte Dateisystem wurde auch für externe Datenträger verwendet und kann mit einem Windows basierten System nicht gelesen werden.

Mac OS X kann auch das FAT12/16/32 Dateisystem lesen und schreiben. Damit ist es möglich externe Datenträger, wie Speicherkarten und USB Sticks für den Multibetriebssystembetrieb einzurichten.

Seit der Einführung von macOS X 10.12 wurde das Apple Dateisystem HFS+ durch APFS (Apple File System) ersetzt.

Betriebssystem macOS

Unterstützte Dateisysteme:

OS X unterstützt verschiedene weitere lokale Dateisysteme wie NTFS, exFAT, UFS, UDF, sowie ZFS (die beiden letztgenannten nur lesend). Der Schreibzugriff auf NTFS wurde in Mac OS X 10.6 hinzugefügt, ist standardmäßig jedoch abgeschaltet und muss durch einen Eintrag in fstab aktiviert werden.

Unterstützte Netzwerkdateisysteme sind AFP, FTP, NFS, SMB/CIFS und Web-DAV.

Mit der Zusatzsoftware ***MacFUSE*** und entsprechenden Plugins wie NTFS-3G (für Schreib/Lesezugriff auf NTFS-Datenträger bis OS X 10.6) sind weitere Dateisystemtypen unter OS X verfügbar.

Hierbei werden zusätzlich eine Menge für die Forensik relevante Dateisysteme nutzbar, wie durch das Mounten von EWF-Images und BDE-Volumes, etc.

Betriebssystem macOS

Benutzerverwaltung

Dem Ursprung von Mac OS X angelehnt ist das Betriebssystem Multiuserfähig und bietet eine entsprechende Benutzerverwaltung mit Benutzer und Gruppen an.

OSX unterscheidet zwischen:

- normalen Benutzern (user)
- Systemverwalter (admin) und dem
- Superuser (root).

Normale Benutzer können keine Änderungen am System vornehmen oder Software außerhalb ihrer Benutzerordner installieren. Alle von Usern gestartete Programme werden mit den entsprechenden Nutzerrechten des Users ausgeführt.

Betriebssystem macOS

Benutzerverwaltung

Die Benutzer der Gruppe **admin** verfügen über weitergehende Rechte, sie dürfen systemweite Einstellungen vornehmen, Software installieren und verfügen über Schreibzugriff auf diverse Systemverzeichnisse.

Nur nach gesonderten Authentifizierungen können tiefergreifende Änderungen am System vorgenommen werden. Ein nutzbares Root-Benutzerkonto, das dauerhaft über Berechtigungen des Superusers verfügt, gibt es nach einer Systeminstallation nicht. Zwar gibt es einen Benutzer „**root**“, dieser ist jedoch standardmäßig deaktiviert. Kann jedoch explizit aktiviert werden.

Betriebssystem macOS

Zeitstempel

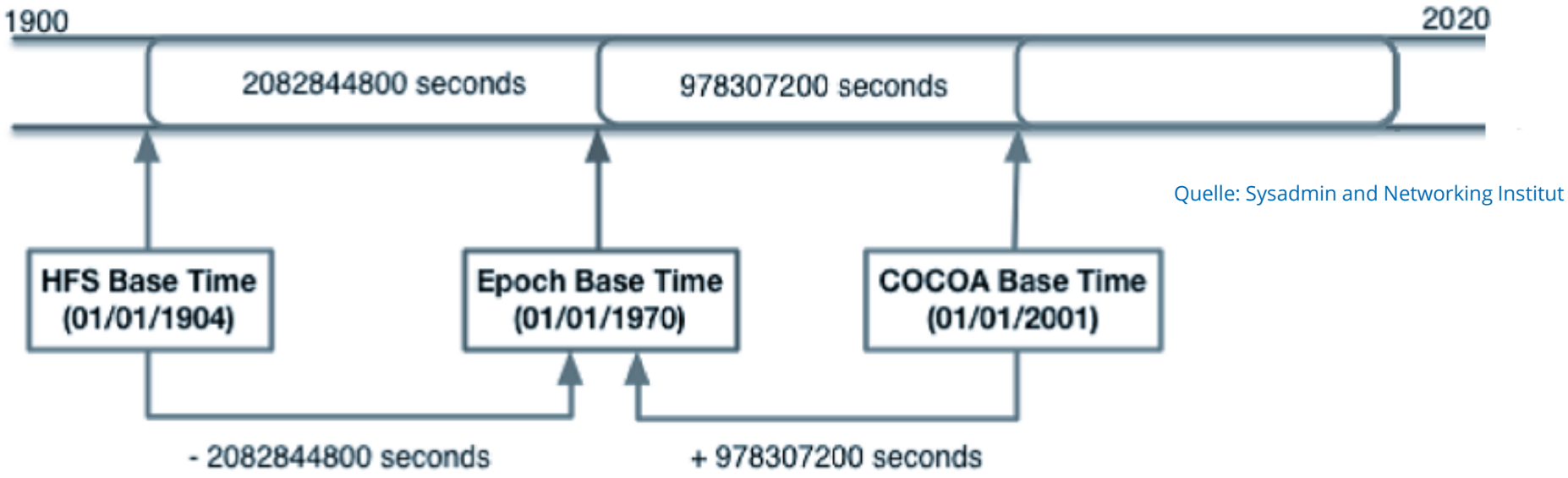
OSX verwendet drei unterschiedliche Zeitstempel:

- **HFS Time**: 4 Byte HexWert, der die Sekunden seit dem 01. Januar 1904 zählt
- **Epoch:** 4 Byte HexWert, der die Sekunden seit dem 01. Januar 1970 zählt
- **Cocoa:** 64 Bit - Integer der die Sekunden seit dem 01. Januar 2001 zählt

Betriebssystem macOS

Zeitstempel

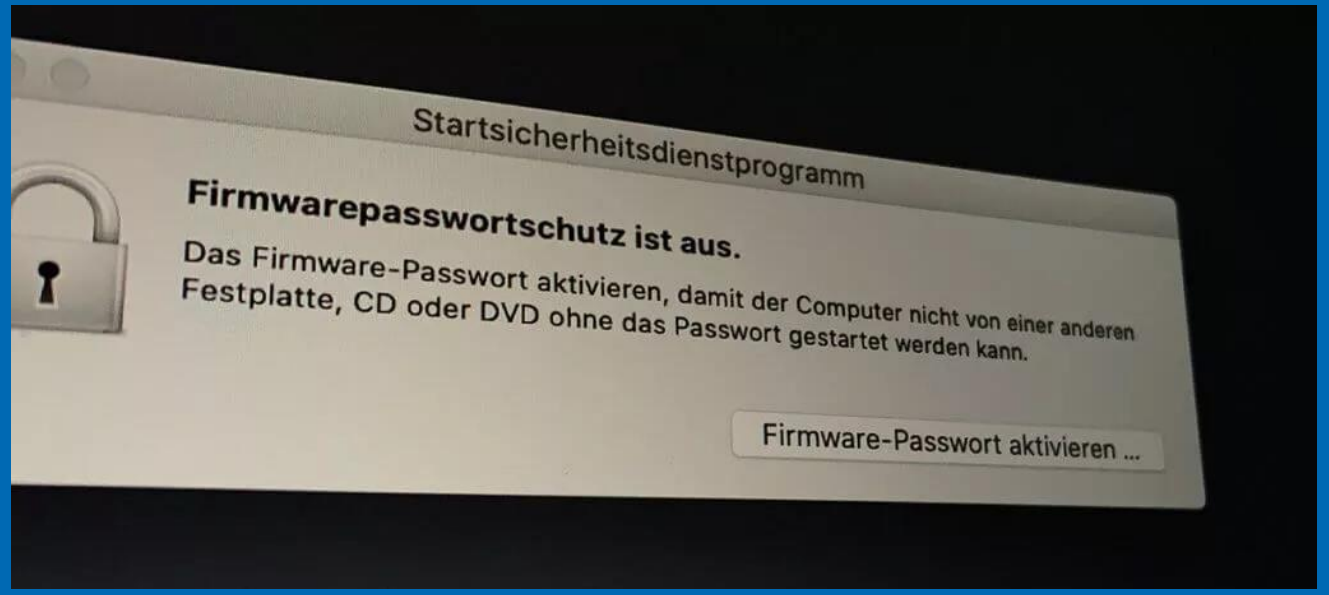
OSX verwendet drei unterschiedliche Zeitstempel:



Quelle: Sysadmin and Networking Institut

BETRIEBSSYSTEM macOS

Sicherheitsfeatures



Betriebssystem macOS

Sicherheitsfeatures - System Integrity Protection (SIP) 1

- Systemintegritätsschutz auch bezeichnet als ***rootless***
- eingeführt in OS X El Capitan (2015) (OS X 10.11)
- Bestehend aus drei Schutzebenen:
  - Schutz von Inhalten und Dateisystemberechtigungen von Systemdateien und –verzeichnissen
  - Schutz von Prozessen gegen Code-Injection, Laufzeitanbindung (wie Debugging) und Dtrace
  - Schutz vor unsignierten Kernel-Erweiterungen ("kexts").

Betriebssystem macOS

Sicherheitsfeatures - System Integrity Protection (SIP) 2

- Kernstück ist Schutz der Systemeigenen Dateien und Verzeichnisse gegen Änderungen durch Prozesse ohne eine bestimmte "Berechtigung", auch wenn sie vom Root ausgeführt wird oder ein Benutzer mit Root-Rechten (sudo)
- Dies geschieht entweder durch Hinzufügen eines erweiterten Dateiattributs zu einer Datei oder einem Verzeichnis oder durch Hinzufügen der Datei oder des Verzeichnisses zu ***/System/Library/Sandbox/rootless.conf***
- Geschützt durch SIP als default:
  - ***/System***
  - ***/sbin***
  - ***/bin***
  - ***/usr***
  - ***/Applications***

Betriebssystem macOS

Sicherheitsfeatures - System Integrity Protection (SIP) 3

Der Systemintegritätsschutz kann nur (ganz oder teilweise) von außerhalb der Systempartition deaktiviert werden. Zu diesem Zweck stellt Apple das Befehlszeilendienstprogramm ***csrutil*** bereit, das über ein Terminalfenster innerhalb des Wiederherstellungssystems ausgeführt werden kann oder einer bootfähigen macOS-Installationsdiskette, die dem NVRAM des Geräts ein Boot-Argument hinzufügt.

Schritte:

1. Command + R beim booten in Wiederherstellungskonsole
2. Terminal öffnen
3. Befehl ausführen: ***csrutil disable***

Nach Änderungen einschalten nicht vergessen!!!

Betriebssystem macOS

Sicherheitsfeatures - Sealed System Volume (SSV) 1

Klassifikation:

- eingeführt in macOS 11 BigSure
- ergänzt das separate schreibgeschützte Systemvolume (ab macOS 10.15 Catalina)
- vertieft den Schutz des Systems gegenüber dem bestehenden Read-only-Volumen der Systemintegritätssicherung (SIP)

Betriebssystem macOS

Sicherheitsfeatures - Sealed System Volume (SSV) 2

Funktionsweise:

- Während der Installation sobald System-Volume installiert werden kryptografische Hashes für jede Komponente auf dem Volume berechnet und zu einem Baum (wie ein Merkle-Baum) zusammengesetzt
- Baum gipfelt in einem einzigen Master-Hash der als Siegel bezeichnet wird
- Hashes werden als Metadaten gespeichert und es wird ein Dateisystem-Snapshot des Volumes erstellt
- Anstatt das System-Volume wie in Catalina schreibgeschützt zu mounten, wird nur der versiegelte Schnappschuss gemountet
- dadurch weiterer robuster Schutz vor Manipulationen und Fehlern durch unveränderliche Systemdateien

Betriebssystem macOS

Sicherheitsfeatures - Sealed System Volume (SSV) 3

Sicherheit:

- Während des Starts prüft macOS BigSur das Seal des Systems
- ist Seal defekt, bootet das Betriebssystem nicht und muss neu installiert werden
- der Wiederherstellungsmodus bietet eine Option, um diese Prüfung zu deaktivieren, so dass es möglich ist, ein System-Volume anzupassen und es unversiegelt zu starten

Betriebssystem macOS

Sicherheitsfeatures - Sealed System Volume (SSV) 4

Hinweise:

Schritte:

1. Command + R beim booten in Wiederherstellungskonsole
2. Terminal öffnen
3. Befehl ausführen: ***csrutil authenticated-root disable***

- Datensicherung von Seal Broken Devices nur mittels ASR Befehl (Apple Software Restore Utility) möglich
- Rückkehr zum versiegelten Volume mittels:

sudo bless --mount / --last-sealed-snapshot

Betriebssystem macOS

Sicherheitsfeatures - FileVault1

- Eingeführt mit Mac OS X 10.3 Panther
- reine Softwareverschlüsselung
- In FileVault 1 oder Legacy FileVault werden nur Home-Ordner in einem Sparsebundle verschlüsselt
- Sparsebundle sind dynamische Dateien (8 MB Default Größe) ähnlich verschlüsselten Container in Truecrypt
- verursacht Probleme mit Time Machine-Backups (werden nur bei Nutzerabmeldung erstellt vs. Suspend)
- vergleichsweise einfach zu knacken bzw. zu entschlüsseln mit Benutzerkennwort

Betriebssystem macOS

Sicherheitsfeatures - FileVault2 ohne Hardwareschutz

- FileVault 2 wurde in Mac OS X 10.7 Lion eingeführt
- ursprünglich ebenfalls Software basiert mit zusätzlichen Maschinenbefehlen für die Crypting Engine auf Intel i CPUs
- Verschlüsselung des gesamten Volumes basierend auf dem Benutzerkennwort mittels überschlüsselten Volume Encryption Key VEK
- Verschlüsselung wird unter Verwendung des XTS-AES-Modus von AES mit einem 256-Bit-Schlüssel durch CPU durchgeführt
- alle Daten die geschrieben werden, müssen verschlüsselt werden, bevor sie auf die Festplatte geschrieben werden
- alle davon gelesenen Daten müssen entschlüsselt werden, bevor sie verwendet werden können

Betriebssystem macOS

Sicherheitsfeatures - Hardwareschutz ohne Filevault2

- Das Unternehmen Apple führte mit dem Apple T2 Security Chip 2017 einige Funktionen zur Erhöhung der Sicherheit entsprechender Geräte ein.
- Der T2 (und auch M1) Chip speichert den VEK Schlüssel der zum Verschlüsseln verwendet wird auf seiner eigenen Hardware.
- Der T2-Chip fungiert als Speichercontroller für die interne SSD, sodass alle Daten, die zwischen dem Intel-Prozessor und der SSD übertragen werden, eine Verschlüsselungsstufe in der Hardware des T2 durchlaufen.
- Alle Macs mit T2-Chips, mit Ausnahme des Mac Pro 2019, verfügen über einen internen Speicher, der eingelötet ist, um das Entfernen schwierig zu machen.

Betriebssystem macOS

Sicherheitsfeatures - Hardwareschutz ohne Filevault2

- Die Sicherheitsfunktionen werden von einer dedizierten Hardware durchgeführt (Secure Enclave mit Secure OS) welche nur über Schnittstellen mit der restlichen Hardware kommuniziert.
- Auf Intel-Macs verlassen sie nie den T2-Chip, sind also nie dem Intel-Prozessor des Mac zugreifbar.
- Wird die Hardware beschädigt oder zerstört, können die Daten auf dem Datenträger nicht mehr durch diesen entschlüsselt werden.
- Der Chip kann auch nicht einfach ersetzt werden, da der einzigartige Schlüssel fehlt.
- Durch diese Funktion kann die Erstellung einer Forensischen Datensicherung stark erschwert oder verhindert werden.

Betriebssystem macOS

Sicherheitsfeatures - FileVault2 mit Hardwareschutz

- wenn FileVault2 auf T2 / M1 Mac aktiviert ist, wird ein VEK in der Hardware abgelegt, der durch einen KeyEncryptionKey (KEK) geschützt wird, der durch das Benutzerkennwort geschützt wird
- dies bedeutet, dass der Benutzer sein Passwort ändern kann, ohne dass das Volume erneut verschlüsselt werden muss
- es ermöglicht zudem die Verwendung spezieller Wiederherstellungsschlüssel, falls das Benutzerpasswort verloren geht

Betriebssystem macOS

Sicherheitsfeatures – Hardwareschutz & Forensic

Der T2 ist die zweite Generation der Apple T-Serie und wurde seit 2017 in verschiedenen Apple Geräten mit Intel Prozessor verbaut.

Mit der Einführung des Apple M1 sind die Funktionen des T2 Chips in den M1 Chip integriert worden, es wird hier also kein extra Chip mehr benötigt.

- **Boot-ROM** - Der Startprozess eines Apple Gerätes mit M1 oder T2 kann nicht manipuliert werden, da der im Boot-ROM gespeicherte Code nicht veränderbar ist. Dieser stellt sicher, dass nur vertrauenswürdige Software im Bootvorgang geladen und ausgeführt wird.
- **Secure Boot** - Bei entsprechender Konfiguration kann verhindert werden das unsignierte Betriebssysteme geladen werden. Es besteht auch die Option das die Signatur bei vorhandener Netzwerkverbindung während der Installation bei Apple überprüft wird.
- **Allowed Boot Media** - Bei entsprechender Konfiguration kann verhindert werden das von einem anderen Gerät gebootet wird.

Betriebssystem macOS

Sicherheitsfeatures - Apple T2 Security Chip

Apple T2 Security Chip ist die zweite Generation der Apple T-Serie und ist ein System on a Chip SoC

Funktionen und Komponenten

- Verschlüsselter Speicher für Passwörter und Schlüssel
- Funktionen zum sicheren Startvorgang
- Schutz und Verarbeitung von Biometrischen Daten
- Audio- und Videoverarbeitung
- Speichercontroller für internes Solid-State Drive
- Hardwarebeschleunigte AES-Engine zur Ver- und Entschlüsselung

Der Apple T2 besitzt weitere Funktionen und Komponenten zur Diagnose, Spracherkennung und zum Monitoring.

Betriebssystem macOS

Sicherheitsfeatures - Apple Silicon M1

Der Apple M1 Chip ist die erste Generation der Apple M-Serie und ist ebenfalls ein SoC. Der M1 Chip wird als der Hauptprozessor von entsprechenden Apple Geräten verwendet. Bei seinem Design wurden viele Funktionen direkt in diesen Chip integriert.

Funktionen und Komponenten

- CPU
- GPU
- Unified Memory
- Cache
- Neural Engine
- Verschlüsselter Speicher für Passwörter und Schlüssel
- Funktionen zum sicheren Startvorgang
- Schutz und Verarbeitung von Biometrischen Daten
- Audio- und Videoverarbeitung
- Speichercontroller für internes Solid-State Drive
- Hardwarebeschleunigte AES-Engine zur Ver- und Entschlüsselung

Der Apple M1 besitzt ebenfalls weitere Funktionen und Komponenten zur Diagnose, Spracherkennung und zum Monitoring.

Betriebssystem macOS

Sicherheitsfeatures – Open Firmeware Passwort

- Firmwarepasswörter sind zum Schutz des BIOS / EFI BIOS gedacht
- Schützen auch vor falschen Bootmedien (DVD/USB)
  - Schützen den Start Manager vor unberechtigter Nutzung Wahltaste/Option (⌥) oder Alt
  - Schützen vor dem Starten des Recovery/Wiederherstellungsmodus Befehlstaste/Command (⌘) + R
- auf Macs mit Apple-Silicon-Chips lässt sich kein Firmware-Passwort mehr setzen

Vielen Dank

Prof. Ronny Bodach

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 58-1011
F +49 (0) 3727 58-21011
bodach@hs-mittweida.de
www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau | Raum 8-205
Am Schwanenteich 6b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de