ESSE Einführung in Security – VO 10: Sicherheitskonzepte von macOS

Rafael Vrecar, Christian Schanes

INSO – Industrial Software
Institut für Information Systems Engineering | Fakultät für Informatik | Technische Universität Wien

Agenda

Vorbemerkungen

Allgemeines über macOS

Secure Enclave (Prozessor)

Apple File System (APFS)

FileVault

Keychain & Find My

Private Relay

Intelligent Tracking Prevention

Weitere Sicherheitsmaßnahmen

Zusammenfassung

Abschlussbemerkungen

Literaturverzeichnis

Vorbemerkungen

- Apples Software ist im Allgemeinen (Darwin ausgenommen) „Closed Source“
- ⇒ bzgl. Informationen *abhängig* von . . .
  - Apple
  - Researcher:innen, die „Reverse Engineering“ betreiben
- ⇒ Vorlesungseinheit basiert stark auf . . .
  (Details im Literaturverzeichnis)
  - Apples Dokumentation
  - Papers von Researcher:innen
- einige der vorgestellten Konzepte werden auch von anderen Betriebssystemen/Plattformen verwendet

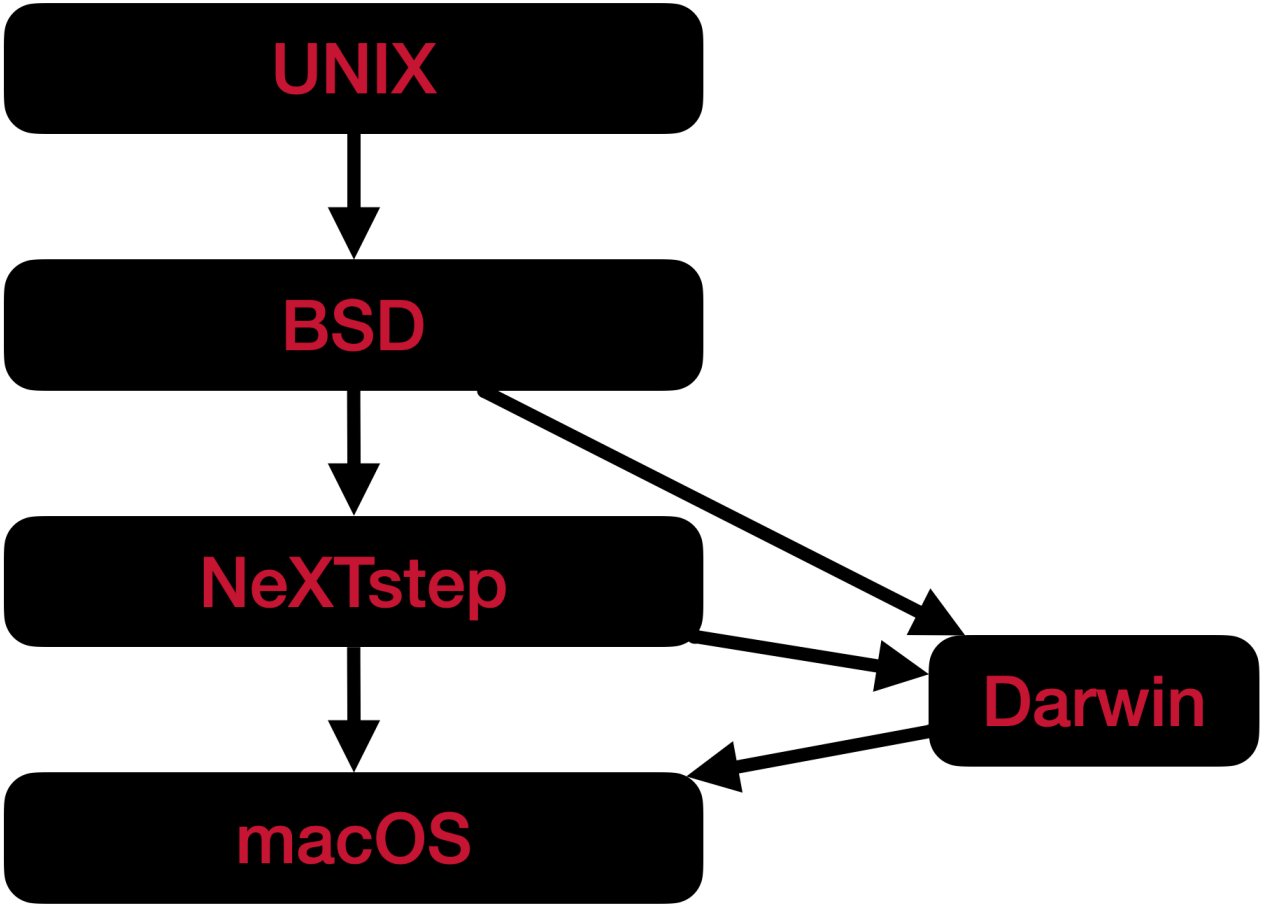
Update-Zyklus & Architektur von macOS

- jährlicher Versionssprung („große“ Features, Designänderungen)
- Point-Releases im Verlauf des Jahres (Security, kleinere Features)
- ∅ **Support:** Geräte erhalten ≈ 7 Jahre aktuelle Version
  + ≈ 3 Jahre Sicherheitsupdates für letzte unterstützte Version[1]
- großteils „Closed Source“, nur auf Apple Geräten unterstützt
  (aber: „Hackintosh“ Community)
- Hybrid Kernel (GNU/Linux: monolithisch, Windows: hybrid seit NT)
- geschrieben in (u.a.): C, C++, Assembler, Objective-C, Swift
- aktuelle Version (Herbst 2023): macOS 14 – Sonoma

[1] Dies sind Erfahrungswerte. Offizielle Supportzeiträume gibt es von Apple nicht.

BSD als Basis von macOS

- „UNIX-basiert“, BSD-Basis ⇒ nicht(!) GNU/Linux

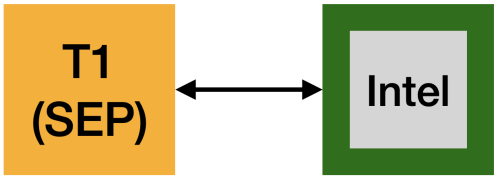


Secure Enclave (Prozessor): Definition & unterstützte Geräte

Abkürzungen: SE . . . Secure Enclave, SEP . . . Secure Enclave Processor

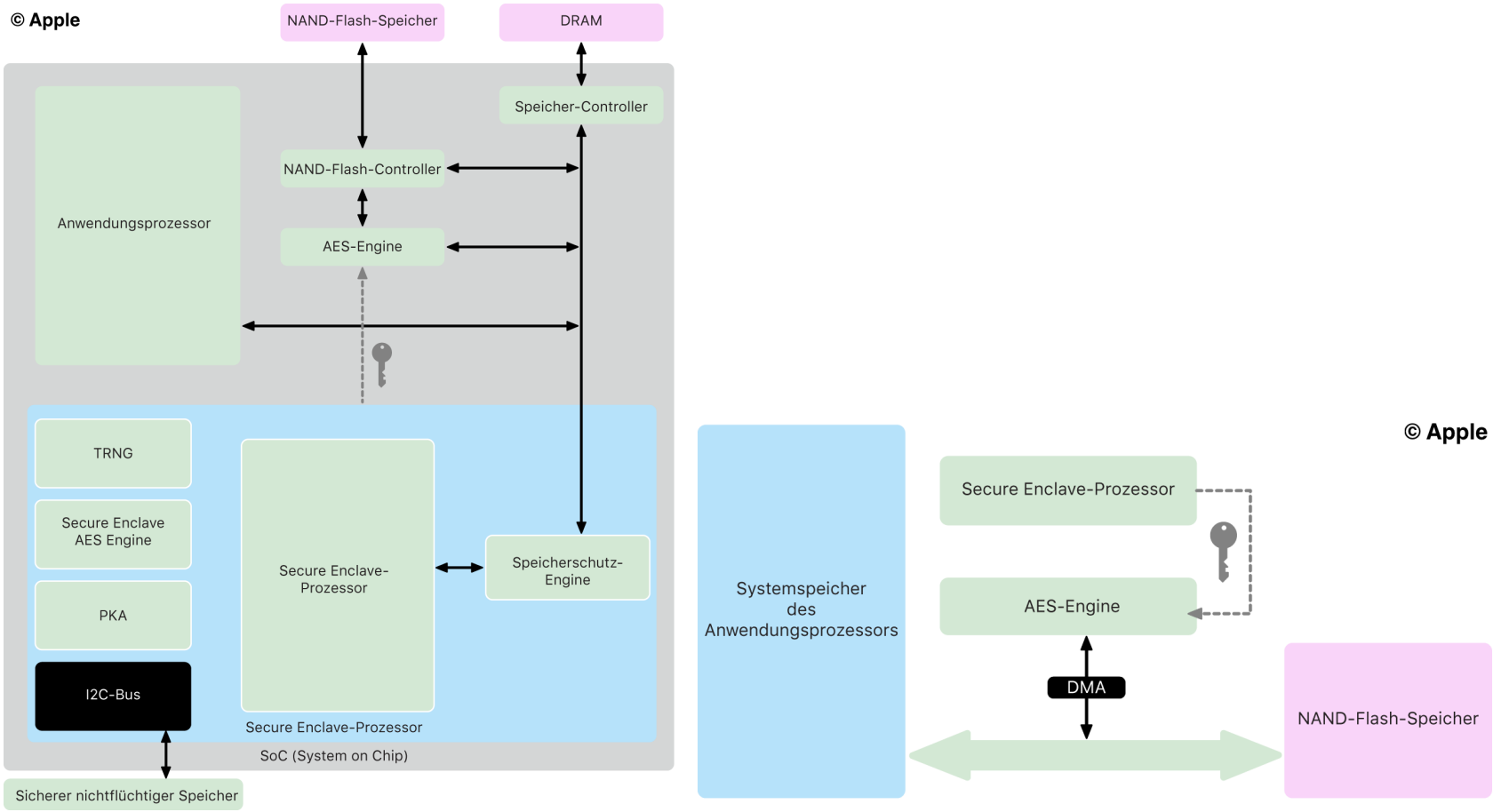
- „Enklave“ $\widehat{=}$ isolierter Bereich, vom Hauptprozessor abgegrenzt
- seit A7 auf Apples Chips enthalten (iPhone 5S, 2013)

- seit MacBook Pro 2016 mit Touch ID als T1 dediziert zusätzlich zu Intel Prozessor, Upgrade (T2) erstmals bei iMac Pro 2017



- in Apple Silicon Macs ebenfalls direkt am Chip (M1 und folgend, seit Herbst 2020)

Secure Enclave (Prozessor): Aufbau (bei Apple Prozessoren)



(Vergleiche `https://support.apple.com/de-at/guide/security/sec59b0b31ff/web`, abgerufen: 23. 11. 2023)

Secure Enclave (Prozessor): Abgrenzung & Speicherschutz

- SEP wird ausschließlich(!) von SE benutzt
- Ziel der Abgrenzung: Verhinderung von **Side-Channel-Attacken**
- niedrige Taktrate soll **Clock- & Power-Attacken** verhindern
- Speicher der SE vom Anwendungsprozessor isoliert (Speicherschutz-Engine)
  - beim Start wird zufälliger Schlüssel generiert
  - Daten, die SE schreibt, werden *verschlüsselt* und ein Message Authentication Code (MAC), genannt „Tag“, zur Sicherung der *Authentizität* (vgl. Vorlesungen 2 & 3) generiert
  - wenn SE Daten entschlüsseln will, wird MAC geprüft
  - MAC gültig $\Rightarrow$ Daten werden entschlüsselt

Secure Enclave (Prozessor): Weitere Bestandteile

- **TRNG** (True Random Number Generator):
  generiert Zufallszahlen, bspw. für die Erstellung eines Schlüssels
- **PKA** (Public Key Accelerator):
  dedizierter Hardware-Block für Operationen der *asymmetrischen* Verschlüsselung
- **AES-Engine**: für Operationen der *symmetrischen* Verschlüsselung zuständig
- **Sicherer nicht flüchtiger Speicher**:
  nur(!) SE kann auf diese Komponente zugreifen, beinhaltet „Entropie“, die zur Generierung von Schlüsseln etc. verwendet wird.

Secure Enclave (Prozessor): Aufgaben

- wie aus den Komponenten ersichtlich wird, zuständig für Verschlüsselung und Schutz von Benutzer:innen-Daten...
- ...insbesondere auch für FileVault
- Biometrie-Informationen (Touch ID auf Macs & i(Pad)OS-Geräten bzw. Face ID auf i(Pad)OS-Geräten) werden ebenfalls mithilfe der SE verschlüsselt aufbewahrt
- durch Abgrenzung vom Hauptprozessor haben Programme von Dritten keinen direkten Zugriff auf Daten der Secure Enclave und operieren auch nicht auf deren Speicher

Apple File System (APFS)

- Standard File System seit macOS 10.13 (2017)
- optimiert für Flash-Speicher
- **Aufbau:** („Container“ $\widehat{=}$ „Partition“, kann mehrere „Volumes“ beinhalten):

```
-- Container 1
-- Container 2
 |---- Volume 1
 |---- Volume 2
 |---- ...
 |---- Volume n
...
-- Container n
```

- Speicherort $\widehat{=}$ „NAND-Flash-Speicher“ auf Folie 7

Aufbau des File Systems bei einer Standard-Installation (1/2)

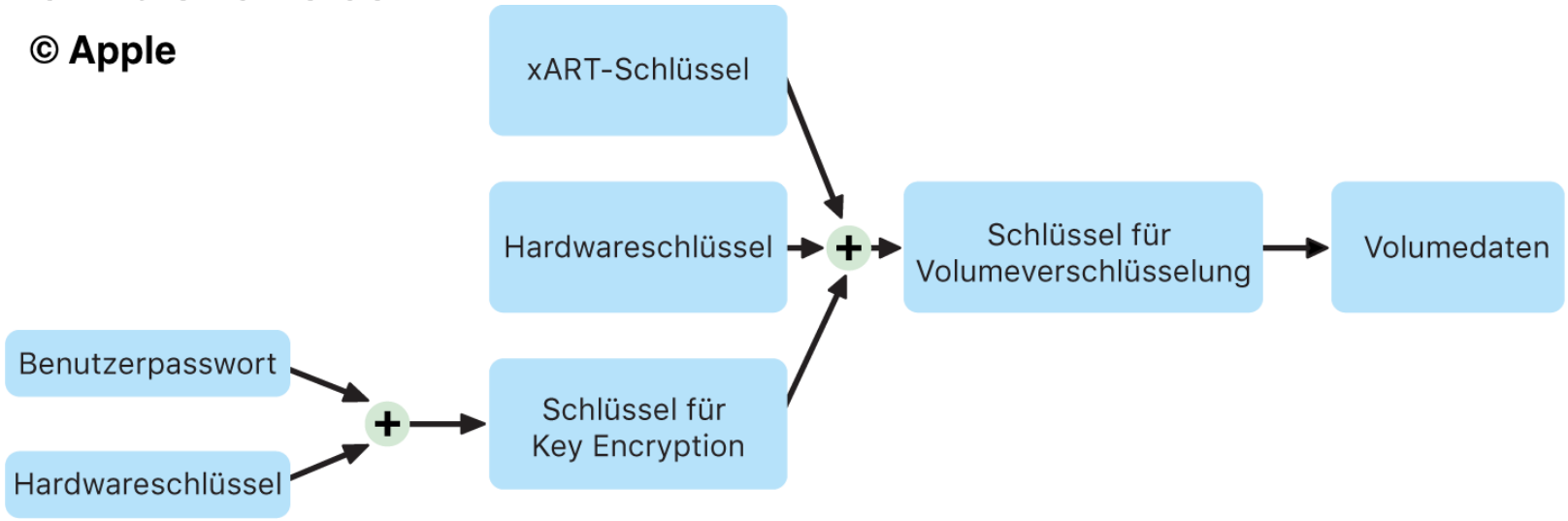
- macOS 10.15 (2019): *„read-only“* **System Volume** d.h. isoliertes Volume, das im Betrieb nicht modifiziert werden kann.
- seit macOS 11 (2020): System Volume dadurch geschützt, dass es signiert wird (kurz **SSV** – Signed System Volume)
  - Kernel überprüft zur Laufzeit, ob Inhalte unverändert
  - falls Integrität gewährleistet
    $\Rightarrow$ Code darf ausgeführt werden, sonst nicht
- System Volume enthält „nativ“ installierte Programme

Aufbau des File Systems bei einer Standard-Installation (2/2)

- **Data Volume** enthält User:innen-Daten, insbesondere auch von dem:der User:in installierte Programme, durch FileVault geschützt!
- **Preboot Volume** enthält Boot-Informationen
- **VM Volume** = Swap File Storage
- **Recovery Volume** enthält recoveryOS, inkl. Festplattendienst- & Terminalprogramm

FileVault: Definition & Funktionsweise

- = Apples Festplatten-Vollverschlüsselung; verwendet AES-XTS
- operiert auf Volume-Ebene
- SE kümmert sich um Schlüsselverwaltung
  (bei Macs mit T2 & Intel oder Apple Prozessor)
- **Funktionsweise:**



(Vergleiche `https://support.apple.com/de-at/guide/security/sec4c6dc1b6e/1/web/1`, abgerufen: 23. 11. 2023)

FileVault deaktiviert ... Was nun?

- Festplatte auch verschlüsselt, wenn FileVault deaktiviert (T2 oder neuer)...
  - ...allerdings nur auf Hardware-UID basierend
  - ...sobald aktiviert, wird durch **Anti-Replay-Mechanismus** verhindert, dass alter Schlüssel verwendet werden kann
  - **Funktionsweise:** siehe vorherige Grafik, allerdings ohne *„Schlüssel für Key Encryption“* und dessen Eltern-Knoten
- erleichtert auch das sichere Löschen der Festplatte
  - Schlüssel werden „weggeworfen“
  - Angreifer:in hat daher nur verschlüsselte Daten, die nicht sinnvoll gelesen werden können

FileVault: unterstützte Geräte & Unterschiede

- vorhergehende Version verschlüsselte nur Home-Verzeichnis
- seit OS X Lion (10.7) in Version 2 (aktuelle Version) verfügbar (Festplatten-Vollverschlüsselung)
- Unterschiede zwischen Macs:
  - Macs ohne SEP oder mit T1 (+ Intel jeweils): Festplatte nicht verschlüsselt wenn FileVault deaktiviert; Schlüsselverwaltung (bei Macs ohne SEP) gänzlich durch Intel-Prozessor
  - Macs mit 1) T2 + Intel oder 2) Apple Chip: Festplatte mit Hardware-UID verschlüsselt wenn FileVault deaktiviert; Schlüsselverwaltung nur(!) durch SEP

Keychain & Find My

- **Keychain:**
  - Passwortmanager mit 2FA-Token-Speicher ab macOS 12
  - verwaltet z.B. Zertifikate, Schlüssel, gespeicherte WLANs
  - Passwörter etc. können über Apple ID mit anderen (Apple) Geräten synchronisiert werden
- **Find My:**
  - sofern Gerät verloren, kann es über Apple ID remote gelöscht werden
  - funktioniert auch wenn offline (dann über Bluetooth, indem zu nahegelegenen Apple Geräten kommuniziert wird)

„Private Relay“ in Safari (iCloud+ ⇒ kostenpflichtig)

- **Idee:** keine Partei (Apple, Website-Provider, …) weiß *gleichzeitig* *wer* man ist & *was* man sich ansieht
- IP-Adresse ist für Netzanbieter *sichtbar* & für 1. Relay (Apple)
- angefragte Website ist für Netzanbieter & Apple *nicht(!) sichtbar*
- 2. Relay (Drittanbieter) generiert *temporäre IP-Adresse*, kennt aber *IP-Adresse von User:in nicht*, dafür kann es *Anfrage entschlüsseln*; . . . danach selber Weg zurück . . .
- Aspekte von VPN oder Tor, Unterschied u.a.: hält sich an Geo-Blocking, unterstützt (vorerst) nur Safari ⇒ Zielpublikum: Endnutzer:innen; keine Vorteile (außer, dass de facto keine Konfiguration notwendig ist) gegenüber VPN(-Angeboten) oder Tor.

„Intelligent Tracking Prevention“ in Safari

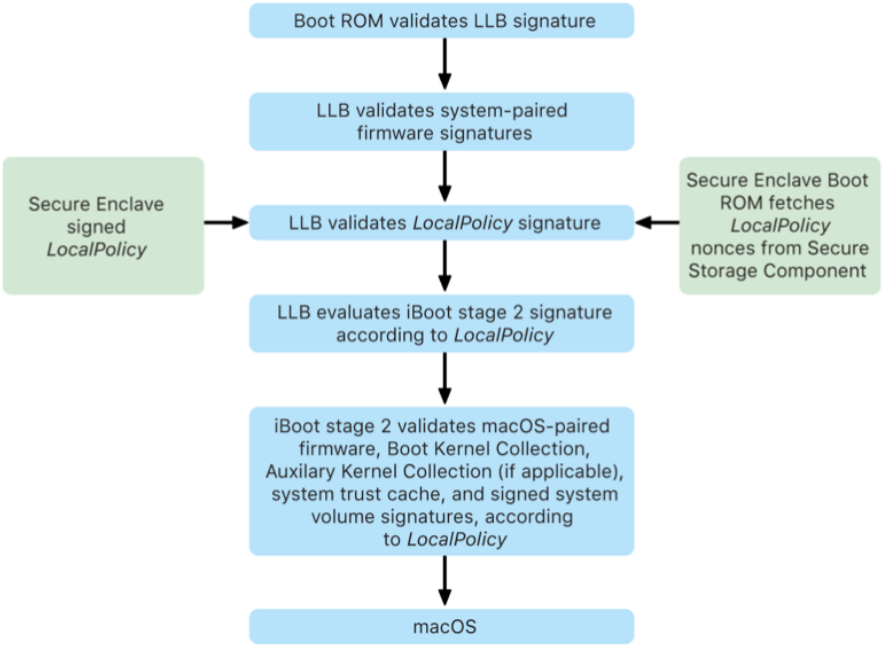
- soll „**Profiling**“ von Dienstleistenden im Internet verhindern
- „on-device Machine Learning“ soll Tracking Technologien blockieren
- Safari legt für User:innen sogenannten „**Privacy Report**“ an, wo blockierte Tracking-Versuche gelistet werden
- soll ebenfalls gegen „**Fingerprinting**“ helfen, indem nur ein *vereinfachtes Profil* mit Dienstleistenden geteilt wird
- Safari keineswegs einziger Browser, der Privacy Maßnahmen setzt; **Beispiel:** Firefox

  (`https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop`) u.a.

XD, ASLR, SIP

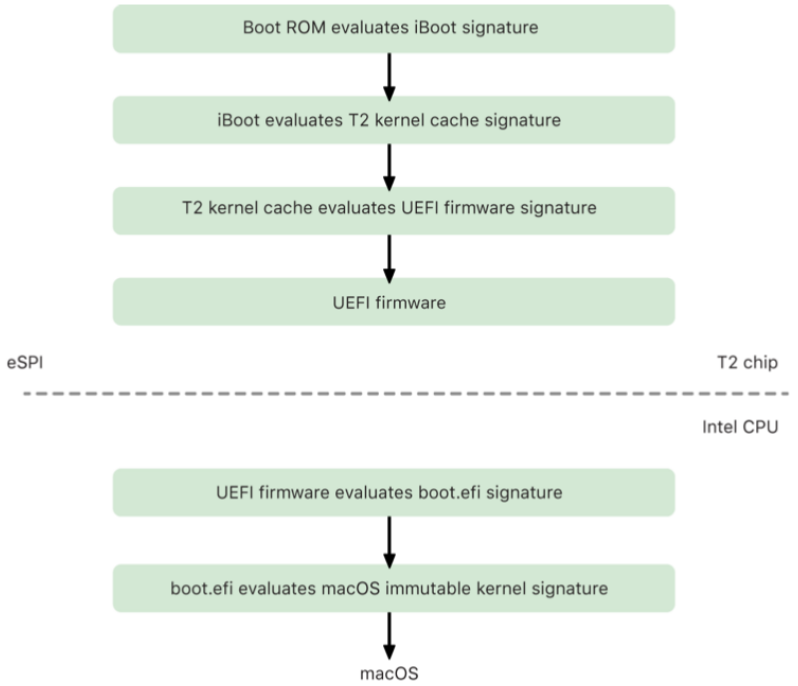
- **XD** (eXecute Disable): einzelne Bereiche im Speicher werden vom Betriebssystem als „nicht ausführbar markiert“, Prozessor verweigert die Ausführung von etwaigem Code, der in diesen Bereichen liegt
- **ASLR** (Address Space Layout Randomization): soll vor **memory corruption bugs** schützen, Programm-Blöcke werden nach Zufallsprinzip im Speicher abgelegt $\Rightarrow$ deutlich unwahrscheinlicher, dass Schadecode an nachfolgender Adresse abgelegt werden kann.
- **SIP** (System Integrity Protection):
  - Mechanismus um spezifische Speicherorte *read-only* zu machen, d.h. während der Ausführung des Betriebssystems können dort befindliche Dateien nur gelesen werden
  - seit OS X 10.11 standardmäßig aktiviert, kann deaktiviert werden

Secure Boot



Boot process steps when a Mac with Apple silicon is started.

© Apple



macOS T2 secure boot chain.

© Apple

(Vergleiche `https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf`, p. 31 & 46, abgerufen: 23. 11. 2023)

Malware & Downgrade erkennen, Systemressourcen-Zugriff

- eingebaute Signatur-basierte Malware Erkennungssoftware („**XProtect**“)
- eingebauter Schutz vor **Downgrade** Angriffen: Zurücksetzen auf ältere Versionen (mit u.U. bekannten Schwachstellen) nicht gestattet
- **Zugriff auf Systemressourcen** (CPU, Speicher, Festplatte, Software, gespeicherte Daten) wird vom Betriebssystem überwacht

Programme installieren, Berechtigungen & Sandboxing

- **Installation von Programmen:**
  - Mac App Store ⇒ App-Review!
    (allerdings nicht alle Anwendungen über App Store beziehbar)
  - **„Gatekeeper“:** aus dem Internet geladene Applikationen werden auf *Authentizität* geprüft
    (Code Signatur mit Developer Certificates)
- **Berechtigungssystem:** einzelne Ressourcen müssen manuell von Nutzer:inne:n freigegeben werden (bspw. Zugriff auf Kamera oder Mikrofon muss jeweils gesondert erlaubt werden)
- **Sandboxing** schützt Daten vor nicht autorisiertem Zugriff durch Anwendungen

Ältere macOS Versionen nutzen . . . gute Idee?

- keine offiziellen Support-Zeiträume $\Rightarrow$ nur Erfahrungswerte
- Support kann abrupt, i.A. ohne Ankündigung, enden
- **Heuristik:** Vorgängerversion sollte i.d.R. sicher zu benutzen sein, Version $n-2$ evtl. schon nicht mehr, aktuelle Version scheint in Apples Update-Policy logischerweise Priorität zu haben
- $\Rightarrow$ **Empfehlung:** 1) aktuellste Version nutzen, sofern keine anwendungsspezifischen Einwände (bspw. endete durch macOS 10.15 Support für 32bit-Anwendungen) & 2) Berichte über Beta-Versionen im Auge behalten, evtl. sinnvoll zwecks Stabilität (wie bei anderen Betriebssystemen auch) erst nach 1. Point-Release upzugraden

Zusammenfassung

- macOS basiert auf BSD (Unix) und hat jährliche Versionssprünge
- Secure Enclave (Prozessor) ist zuständig für Festplattenverschlüsselung (FileVault) und Biometrie Verwaltung
- Passwort-Management, Ortung von eigenen verlorenen Geräten & Schutzmaßnahmen bzgl. Tracking sind direkt ins Betriebssystem integriert
- Code Signatur hilft beim Schutz vor Malware und Downgrade ist nicht erlaubt
- Sandboxing und ein systemweites Berechtigungssystem sollen vor nicht autorisierten Zugriffen auf Daten & Ressourcen schützen

Abschlussbemerkungen

- macOS hat viele Sicherheitsvorkehrungen, nutzen Sie diese!
- Bleiben Sie kritisch und bedenken Sie, dass Apples Sicherheitsmaßnahmen keinesfalls vor Fehlern gefeit sind. ;)
- Behalten Sie im Hinterkopf, dass Apples Code (großteils) nicht offen ist und daher mehr Vertrauen erfordert, da Sie ihn nicht (einfach) überprüfen bzw. selbst kompilieren können.
- Updates installieren ist (i.A.) natürlich (auch bei Apple) eine gute Idee.
- . . . und zuletzt: **Don't be evil!** – Apple hat ein Security Bounty Programm (`https://developer.apple.com/security-bounty/`)

Literaturverzeichnis 1/5

- BSD als Basis von macOS: https://developer.apple.com/library/archive/documentation/Darwin/Conceptual/KernelProgramming/Architecture/Architecture.html, abgerufen: 23. 11. 2023
- macOS Versionsgeschichte: https://support.apple.com/en-us/HT201260, abgerufen: 23. 11. 2023
- Apple Keynotes: https://podcasts.apple.com/us/podcast/apple-events-video/id275834665/, abgerufen: 23. 11. 2023
- The Linux Kernel Archives: https://www.kernel.org/, abgerufen: 23. 11. 2023
- Windows Kernel: https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/windows-kernel-mode-kernel-library, abgerufen: 23. 11. 2023

Literaturverzeichnis 2/5

- Secure Enclave: https://support.apple.com/de-at/guide/security/sec59b0b31ff/web, abgerufen: 23. 11. 2023
- Apple File System (APFS): https://support.apple.com/de-at/guide/disk-utility/dsku19ed921c/mac, abgerufen: 23. 11. 2023
- FileVault 1/3: https://support.apple.com/de-at/guide/security/sec4c6dc1b6e/1/web/1, abgerufen: 23. 11. 2023
- FileVault 2/3: https://support.apple.com/en-us/HT204837, abgerufen: 23. 11. 2023
- FileVault 3/3: Choudary, O., Grobert, F., & Metz, J. (2012). Infiltrate the vault: Security analysis and decryption of lion full disk encryption. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2012/374.pdf, abgerufen: 23. 11. 2023

Literaturverzeichnis 3/5

- Find My Mac: https://support.apple.com/en-us/HT204756, abgerufen: 23. 11. 2023
- Private Relay: https://developer.apple.com/videos/play/wwdc2021/10096, abgerufen: 23. 11. 2023
- Safari Privacy: https://www.apple.com/privacy/, abgerufen: 23. 11. 2023
- Firefox Privacy: https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop, abgerufen: 23. 11. 2023
- Systemsicherheit: https://support.apple.com/de-at/guide/security/sec114e4db04/1/web/1, abgerufen: 23. 11. 2023
- Sicherheit bei Apps: https://support.apple.com/de-at/guide/security/sec35dd877d0/1/web/1, abgerufen: 23. 11. 2023

Literaturverzeichnis 4/5

- macOS Sicherheit – Überblick (1/2): https://support.apple.com/de-at/guide/security/welcome/web, abgerufen: 23. 11. 2023
- macOS Sicherheit – Überblick (2/2): https://www.apple.com/macos/security/, abgerufen: 23. 11. 2023
- Hardwaresicherheit – Überblick: https://support.apple.com/de-at/guide/security/secf020d1074/1/web/1, abgerufen: 23. 11. 2023
- Verschlüsselung & Datensicherheit – Überblick: https://support.apple.com/de-at/guide/security/sece3bee0835/1/web/1, abgerufen: 23. 11. 2023
- iCloud Sicherheit: https://support.apple.com/en-us/HT202303, abgerufen: 23. 11. 2023

Literaturverzeichnis 5/5

- Apple Dokumentation & Support: https://support.apple.com/, abgerufen: 23. 11. 2023
- Apple Platform Security (May 2021): https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf, abgerufen: 23. 11. 2023
- Trusting older macOS versions: https://objectivebythesea.com/v4/talks/OBTS_v4_jLong.pdf, abgerufen: 23. 11. 2023
- Korak, T., & Hoefler, M. (2014, September). On the effects of clock and power supply tampering on two microcontroller platforms. In 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography (pp. 8-17). IEEE.: https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=79126, abgerufen: 23. 11. 2023

Vielen Dank!

https://establishing-security.at/