REGIONALES RECHENZENTRUM ERLANGEN [RRZE]

Security in OS X und iOS

Oliver Kett, RRZE

28.01.2016

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

Agenda

FILEVAULT 2

FileVault 2

- Full Disk Encryption
- verschlüsseln im laufendem Betrieb
- mehrere Benutzer können Autorisiert werden
- seit 10.7, FileVault 1 seit 10.3

FileVault 2: Technik

- Block Device
  - CoreStorage LVM
- CoreCrypto
  - AES-XTS
  - FIPS 140-2 (10.8+)
  - Sollte den meisten Angreifern standhalten
  - Geheimdiensten wahrscheinlich nicht …

FileVault 2: Schlüsselbackup

- iCloud Account
- auf eigenem MDM-Server, etwa Casper
- “hinterlegen an sicherem Ort”
  - ausdrucken, abschreiben, …

- Schlüssel wird mit dem Passwort eines/mehrerer Benutzer verschlüsselt und abgelegt.

POSIX

UNIX

- OS X basiert auf Darwin
  - Darwin basiert zu großen Teilen auf FreeBSD
- klassische UNIX Rechte
  - Probleme beim Desktop Einsatz
- seit 10.0

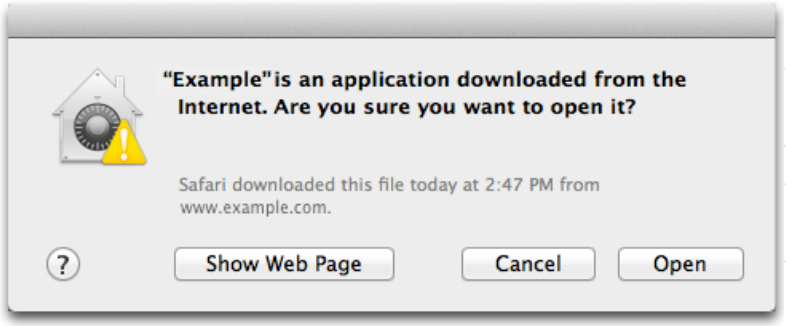
KEYCHAIN

Keychain (Schlüsselbund)

- verschlüsselte Datenbank
  - Benutzernamen und Passwörter
  - Notizen
- bei Login: entschlüsselt im RAM
- APIs, quasi Standard
- für Programm nur lesen/schreiben der eigenen Passwörter möglich
- seit Mac OS 8.6

GATEKEEPER & FILE QUARANTINE

File Quarantine



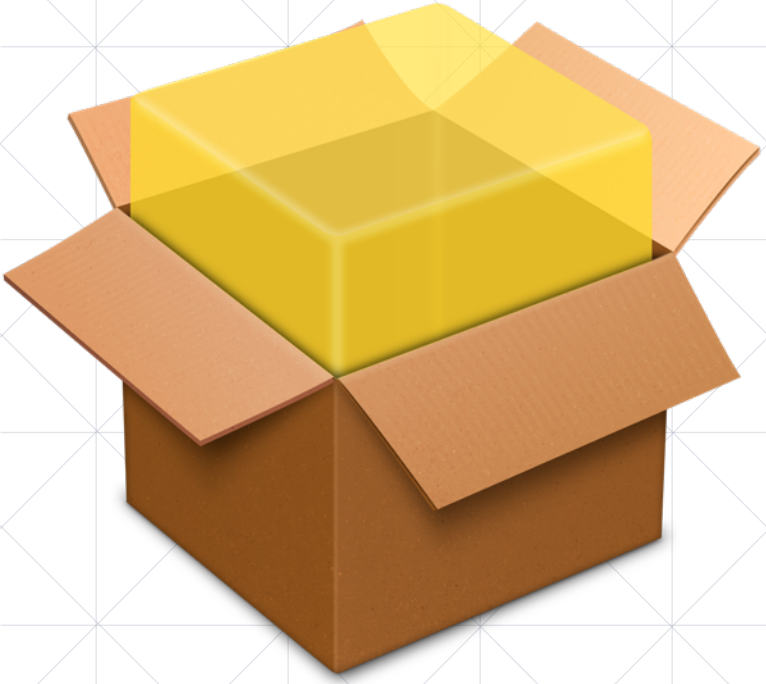
- HFS+ extended Attribute *com.apple.quarantine*
- wird von den meisten Browsern gesetzt
- versehentliches Ausführen von Programmen wird verhindert
- Schadcode kann anhand von Signaturen erkannt werden (XProtect)
- seit 10.5

Gate Keeper

- nur signierte Software wird ausgeführt
  - ctrl-Klick + “Öffnen”
  - “nur App Store” oder “alle” geändert werden
- Signatur muss von Apple beglaubigt sein
- Bedingung für App Store
  - “außerhalb” des App Store optional
- seit 10.7

SANDBOX

Sandbox



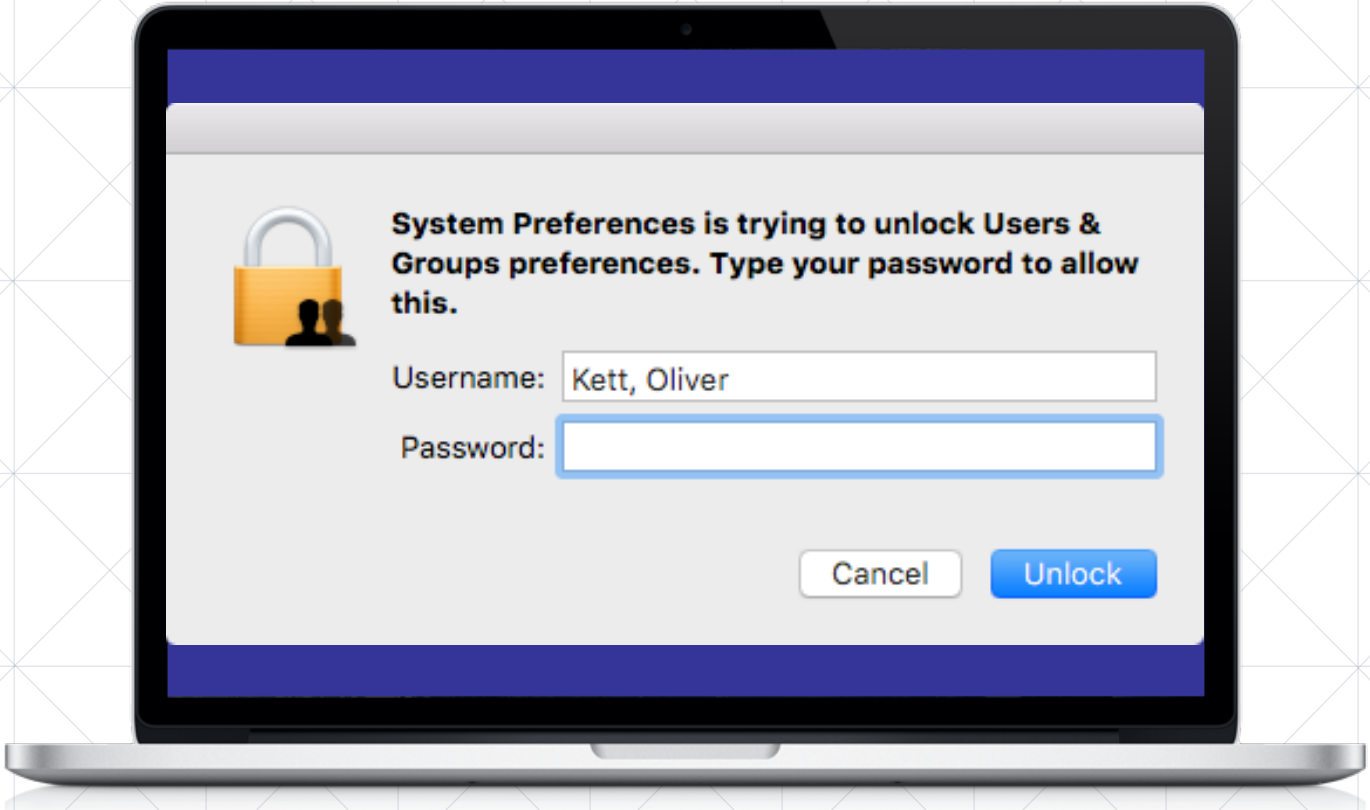
- separiert Anwendungen voneinander
  - Dateisystem (lesen, schreiben)
  - IPC
  - forks / Subprozesse
- ~/Library/Containers
- *sandbox-exec(1)* für beliebige Programme
- Pflicht für App Store
- seit 10.7

klingt doch alles super sicher, oder?

UNIX wurde konzipiert für Multi-User Betrieb auf Großrechnern. Nur Administratoren konnten Änderungen am System durchführen.

OS X ist heute meist Single-User System. Administrator ist dann der einzige “echte” Benutzer auf dem System

Was wird wohl passieren?



SIP TO THE RESCUE!

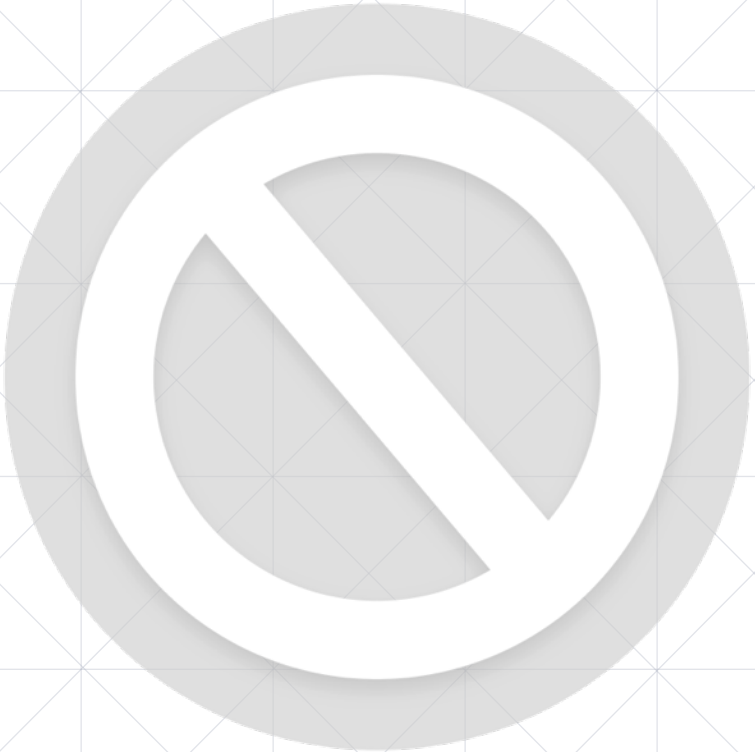
System Integrity Protection

SIP: Dateisystem

- nur lesender Zugriff auf
  - /bin
  - /sbin
  - /usr
  - /System
  - /Applications
    - Apple Apps

SIP: Dateisystem

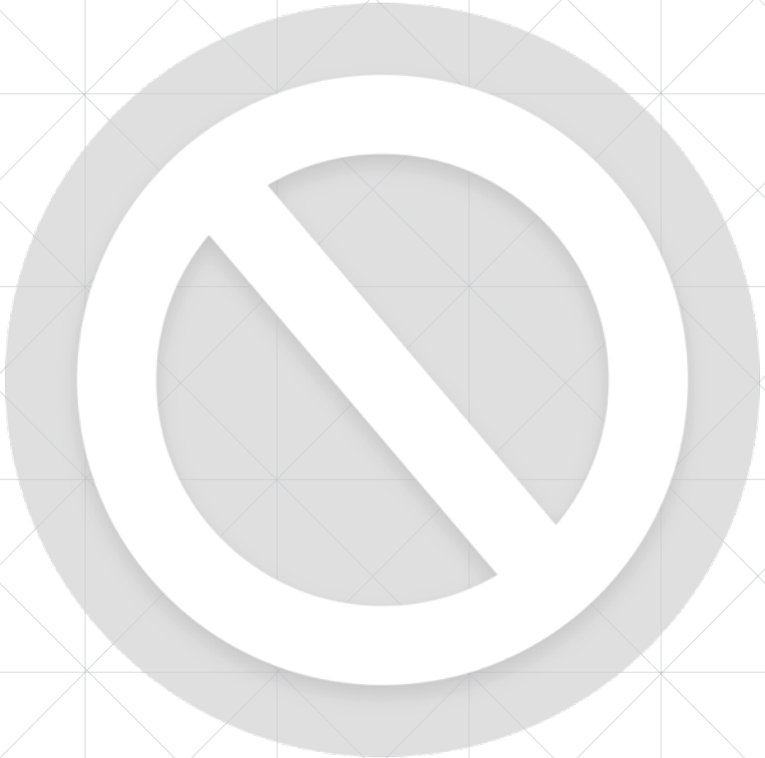
- Zugriff auf
  - /usr/local
  - /Applications
  - /Library
  - ~/Library
- schon lange “best practice”
- /System/Library/Sandbox/rootless.conf



SIP: Dateisystem: Ausnahmen

- /System/Library/Caches
- /System/Library/Extensions
- /System/Library/Speech
- /System/Library/User Template
- /usr/share/man
- …

- Softwareupdate hat spezielles Entitlement und kann überall schreiben



SIP: Dateisystem: noch mehr Ausnahmen

- /System/Library/Sandbox/Compatibility.bundle/Contents/Resources/paths
  - 3rd-Party Treiber
  - VirtualBox
  - jamf
  - gutenprint
  - puppet, facter, …

SIP: Absicherung der Systemprozesse

- DTrace, lldb, …
- auch Anwendungen, etwa Finder
- alle Programme mit FS-Flag “restricted”
- alternativ: Signatur weist spezielles Entitlement auf
- andere Apps nicht geschützt
  - auch nicht App Store Apps

SIP: Kernel Extensions

- /Library/Extensions
- “Developer ID for Signing Kexts”
  - https://developer.apple.com/contact/kext/
- kext-dev-mode obsolet
  - trimforce(8)

SIP: Konfiguration

- NVRAM (PRAM)
  - gilt für alle Installationen
  - Recovery / Install OS
- auch teilweise zu deaktivieren
  - kext
  - fs
  - debug
  - dtrace
  - nvram

SIP soll Manipulation des Betriebssystems verhindern, Anwendungen bleiben (vorerst) ungeschützt.

WWDC 2015:
Security and Your Apps

https://developer.apple.com/videos/play/wwdc2015-706/

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

Regionales RechenZentrum Erlangen [RRZE]
Martensstraße 1, 91058 Erlangen
http://www.rrze.fau.de

Oliver Kett
rrze-mac@fau.de