Erledigt Wechsel von Clover auf OpenCore

Beitrag von „griven“ vom 17. Dezember 2019, 14:29

Ja bluebyte im großen und ganzen bedeutet es genau das wobei Du den EFI Ordner schon kopieren kannst solange eben die Signatur und die vault.plist mit kopiert werden und im Prozess keine Files verändert werden.

Das create_vault.sh Script erzeugt eine vault.plist Datei in der die SHA-256 hashes aller Files enthalten sind die zu Deiner OC Installation gehören (OC Files, Configs, Extensions usw.) und signiert diese Datei im Anschluss mit RSA Zertifikat und "implantiert" den entsprechenden Key in die OpenCore.efi. Wenn die Optionen RequireVault und RequireSignature in der config aktiviert sind liest OpenCore beim start die vault.plist, natürlich nicht ohne im Vorfeld die Signatur auf Gültigkeit zu prüfen, und gleicht dann die in der Vault.plist abgelegten Hashes mit den Hashes der Dateien auf der EFI ab. Sollte sich vom Zeitpunkt der Erstellung des Zertifikats und der Vault.plist etwas an den Dateien oder an der Vault.plist verändert haben egal ob wissentlich durch den User oder unwissentlich durch Schadprogramme verweigert OpenCore den Systemstart mit einem entsprechenden Hinweis. Aus dem Verhalten ergibt sich natürlich das es nur dann sinnvoll ist beide Komponenten wirklich zu aktivieren wenn man die konfiguration abgeschlossen hat denn ansonsten würde jede Änderung an der config.plist oder irgendeiner anderen Datei im OC Kontext bedingen das die Vault.plist neu aufgebaut und signiert werden muss.

~~In wie weit in dem Zug die OpenCore.efi ebenfalls gegen eine Version getauscht werden muss die noch keinen Public Key enthält kann ich adhoc nicht beantworten würde aber anhand der Dokumentation davon ausgehen das dem so ist weil der Suchbegriff den das Script verwendet um den Key in den EFI Treiber zu schreiben nicht mehr vorhanden ist~~. mhaeuser liege ich da mit meiner Annahme richtig?

Edit: ich lag falsch mit der Annahme der PublicKey bleibt der gleiche sprich die OpenCore.efi muss nicht erneut angepackt werden wohl aber muss die Vault.plist nach jeder Änderung an config oder Files neu erstellt und signiert werden. Danke mhaeuser fürs klarstellen weiter unten

Richtig spannend wird das Thema indes auch erst wenn die SecureBoot implementation komplett ist denn aktuell greift das ganze ja erst wenn OC schon gestartet ist alles was davor passiert (kompromitierte bootX64.efi zum Beispiel) würde so erstmal weitestgehend

unbemerkt durchgehen da aktuell noch eine Instanz fehlt die schon auf dieser Ebene prüft.