Erledigt Überlegung: Mac kaufen, Daten klauen, Verschrotten?

Beitrag von „griven“ vom 28. August 2017, 23:00

Wie soll man das auch ahnen?

Dienste wie iMessage und FaceTime sind bei Apple halt besonders geschützt was durchaus sinnvoll ist denn beide Dienste ermöglichen den Kontakt von Nutzern untereinander wobei eine Ende zu Ende Verschlüsselung zum Einsatz kommt bei deren Entschlüsselung die AppleID eine entscheidende Rolle spielt. Apple hat ein gesteigertes Interesse daran diese Dienste so sicher wie möglich zu halten und dazu gehört eben auch das die AppleID als solche so eindeutig wie möglich einem Nutzer und einem Pool von Maschinen zugeordnet werden kann.

Bei der Installation eines Hackintosh ist aber eben genau das zweite Kriterium nicht unbedingt gegeben wenn man nicht bedacht vorgeht. Bootloader wie zum Beispiel Clover übergeben dem System ohne besondere Einstellungen erstmal immer die Hardware UUID die im System verankert ist und zwar unabhängig vom gewählten SMBIOS erst wenn man im SMBIOS selbst den Wert SmUUID (uuidgen im Terminal) ausfüllt und den Haken bei Inject SystemID entfernt ist man zumindest einigermaßen auf der sicheren Seite. Vielfach wird jedoch bei der Installation mit dem SMBIOS experimentiert und so sammeln sich unter der AppleID schnell unzählige MAC´s verschiedener Bauart mit immer wieder der selben SystemUUID an was zwangsläufig eigentlich ja nicht sein kann.

Wir wissen das für Facetime und iMessage neben der UUID des Systems auch noch die BaseBoardSerial (MLB) und der ROM Wert eine Rolle spielt. Bei jedem Versuch sich an FaceTime und iMessage anzumelden wird neben der UUID des Systems auch der MLB und der ROM Wert an Apple übermittelt zusammen mit den Informationen aus der AppleID wird daraus ein Key zum verschlüsseln und entschlüsseln der iMessage und FaceTime Verbindungen generiert was freilich nur funktionieren kann wenn alle Werte Unique sind und obendrein den von Apple festgelegten Konventionen entsprechen. Apple selbst scheint hier bei der Prüfung der Plausibilität der Werte verschiedene Eskalationsstufen zu kennen denn sehr alte ID´s dürfen in der Regel die Services selbst dann nutzen wenn die übermittelten Werte für sich eindeutig sind aber nicht zu 100% den festgelegten Konventionen entsprechen bei neueren ID´s scheint die Prüfung strikter zu sein hier müssen die Werte dann auch den Konventionen entsprechen damit die Services genutzt werden können.

AppleID´s die schon verbrannt sind werden in Ausnahmefällen auf eine Art Whitelist gesetzt (Anruf bei Apple) wenn man plausibel erklären kann warum und weshalb die ID verbrannt ist ebenfalls scheinen ID´s die für das bezahlte Developer Programm registriert sind hier eine Ausnahme zu bilden...