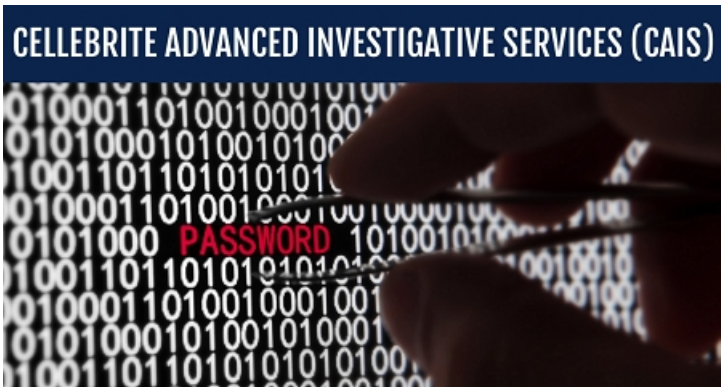
Erstellt am: 30. 3. 2016 - 18:30 Uhr

Wie der FBI-Zugriff auf iPhones funktioniert

Der Wiener Forensikexperte Nicolas Ehrschwendner über manipulierte Bootloader, geklonte Flash-Speicher und nicht-dokumentierte Schnittstellen in der Hardware.

Der überraschende Rückzieher des FBI in der Klage gegen Apple am Montag lässt die Fachwelt rätseln. Laut FBI hatte man doch einen Weg gefunden, in das iPhone des toten Attentäter von San Bernardino einzudringen, ohne Apple zur Produktion eines generellen Nachschlüssels für alle Geräte zu verpflichten. Eine Reihe von Experten tippt dabei auf die israelische Forensikfirma Cellebrite, die auf das Auslesen von Daten aus Mobiltelefonen spezialisiert ist.

Das österreichische Innenministerium bestätigte auf Anfrage, dass Produkte und Dienstleistungen von Cellebrite auch in Österreich seit Jahren eingesetzt werden. Standardmethode ist dabei das Auslesen von Smartphones über die Cellebrite-Hardware mit einem eigenen Betriebssystem. Im Fall des gesperrten iPhones geht es um die Speicherelemente rund um die Passworteingabe. Der Wiener Datenretter und Forensikexperte Nicolas Ehrschwendner erläutert die Techniken der Datenextraktion, die für einen solchen Zugriff des FBI in Frage kommen.



Cellebrite

Aus dem aktuellen Prospekt von Cellebrite

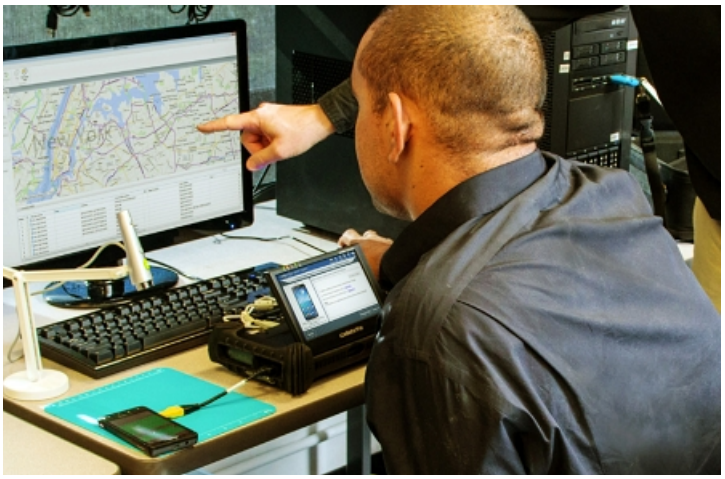
Manipulierte Firmware, eingeschleuster Code

Mit der nun eingestellten Klage hatte des FBI versucht, 1995 erlassene Beschränkungen für staatliche Überwacher mit einem Gesetz aus dem Gründungsjahr der USA 1789 auszuhebeln.

"Bei der Datenrettung werden großteils identische Methoden eingesetzt wie in der Forensik, fixer Bestandteil ist dabei die Manipulation der Firmware in einem Speichermedium. Wir beheben Bugs, schleusen Code ein zur Fehlersuche, legen Sicherheitskopien der Firmware an und spielen die

gegebenfalls wieder auf den Chip zurück", sagte Ehrschwendner.

Um die Manipulation einer solchen "Firmware" - eine Art Basisbetriebssystem für Chips - geht es auch im Fall des Attentäters Syed Farook, dessen Diensthandy durch das Vorgehen des FBI so versperrt wurde, dass es bis jetzt nicht ausgelesen werden konnte. Durch die Entscheidung des FBI, das iCloud-Passwort des Smartphones direkt nach den Attentaten zurücksetzen zu lassen, war der normale Weg zur Datenakquise versperrt. Apple ist es nämlich sehr wohl möglich, ohne Wissen des Eigentümers eine aktuelle Kopie der iPhone-Daten in der iCloud zu erzwingen, im Regelfall geschieht das auf Anordnung eines Gerichts.



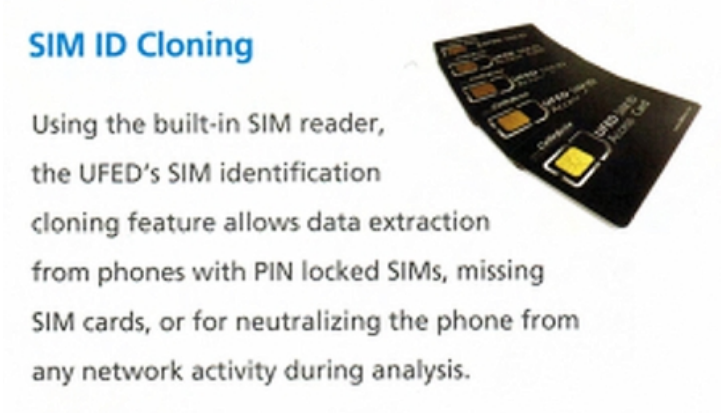
Cellebrite

Links unten ist das Handy, ein sogenanntes UFED von Cellebrite mit Kleinbildschirm daneben, offenbar liest man gerade Geodaten aus.

Bootloader und Diebstahlssicherung

Die Attentate von San Bernardino, bei denen im Dezember 14 Menschen starben, in der Berichterstattung von ORF.at

Da dieser Weg versperrt ist, muss das vom toten Attentäter gesetzte Passwort geknackt werden, das aber ist problematisch, weil auf den iPhones noch eine Diebstahlssicherung existiert. Die veranlasst das iPhone nach zehn fehlgeschlagenen Loginversuchen dazu, alle Daten in den Speichern durch Überschreiben zu löschen. Hier setzt die erste und wohl aussichtsreichste Methode an, nämlich die direkte Manipulation der "Bootloader-Firmware", also des Minibetriebssystems, über das beim Einschalten des Handys das eigentliche Betriebssystem gestartet wird. "Bei diesem Startvorgang lässt sich zum Beispiel eine Firmware einspielen, die eine beliebige Anzahl von Eingabeversuchen erlaubt", sagte Ehrschwendner.



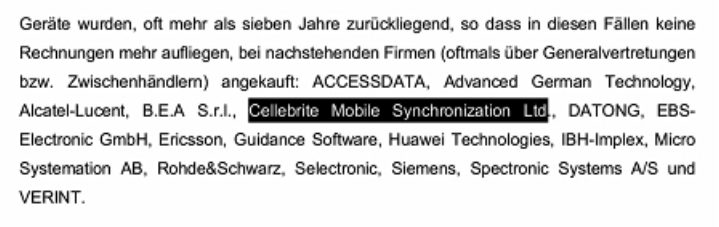
Cellebrite

Aus einem geleakten Cellebrite-Prospekt von 2011

Das Innenministerium sagt

Die Beantwortung der Neos-Anfrage durch das Innenministerium vom April 2015 (https://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_03814/imfname_406204.pdf)

Diese Methode wird in den Set-Ups von Cellebrite standardmäßig eingesetzt und sie ist keineswegs auf iPhones beschränkt. Nach eigenen Angaben verfügt die Firma über manipulierte Bootloader für eine ganze Reihe von Android-Geräten verschiedener Hersteller und bietet sogar eine Hotline an, um das jeweilige Telefon anhand einer Beschreibung seines Aussehens zu identifizieren. Auch das Wiener Innenministerium nimmt solche Dienstleistungen der Firma Cellebrite in Anspruch, das geht aus der Antwort des Innenministeriums auf eine parlamentarische Anfrage der Neos zum Einsatz von Überwachungstechnologie vom April 2015 hervor. In einer Liste von sehr unterschiedlichen Firmen, die das Innenministerium laut eigenen Angaben beliefert haben, findet sich auch der Firmenname Cellebrite. "Das BMI verwendet bestimmte Produkte des Herstellers Cellebrite zur kriminalpolizeilichen Auswertung von gerichtlich beschlagnahmten Mobiltelefonen", bestätigte BMI-Sprecher Karl-Heinz Grundböck auf Anfrage von ORF.at.


Geräte wurden, oft mehr als sieben Jahre zurückliegend, so dass in diesen Fällen keine Rechnungen mehr aufliegen, bei nachstehenden Firmen (oftmals über Generalvertretungen bzw. Zwischenhändlern) angekauft: ACCESSDATA, Advanced German Technology, Alcatel-Lucent, B.E.A S.r.l., Cellebrite Mobile Synchronization Ltd., DATONG, EBS-Electronic GmbH, Ericsson, Guidance Software, Huawei Technologies, IBH-Implex, Micro Systemation AB, Rohde&Schwarz, Selectronic, Siemens, Spectronic Systems A/S und VERINT.

BMI

Die Antwort aus dem Innenministerium auf die Anfrage der Neos zum Thema Überwachung

Geklonte NANDs, Automatisierung

Anleitung auf der Apple-Website zum Setzen eines Passworts im iPhone (https://support.apple.com/en-us/HT204060)

Eine zweite Angriffsmöglichkeit sei das Klonen des verschlüsselten Speichers samt dem Zähler für PIN-Eingaben auf ein externes Speichermedium, in dem Fehlversuche natürlich nicht zu einer Datenlöschung führen. Wenn die Höchstzahl von zehn Fehlversuchen erreicht sei, müssten die verschlüsselten Daten erneut eingespielt werden, so Ehrschwendner weiter. Dieser Vorgang ließe sich auch automatisieren, falls nur ein vierstelliger, rein numerischer PIN-Code gesetzt sei, habe man das Passwort sehr schnell geknackt. Dabei handelt es sich nicht um den PIN-Code für die SIM-Card, den die Mobilfunker vergeben, sondern um eine ebenfalls vierstellige Zahlenkombination für das Apple-Betriebssystem, die vom Besitzer selbst gesetzt wird.

Attingo Datenrettung

Nicolas Ehrschwendner (https://www.attingo.com/)

Wahlweise ist auch ein stärkeres, sechsstelliges Passwort möglich, das aus Buchstaben und Zahlen bestehen kann. "Auch dieser Vorgang gehört zu den gängigen Routinen der Datenrettung. Wenn etwa Flashspeicher und SSD-Laufwerke betroffen sind, bauen wir schadhafte NANDs und andere Speicherelemente aus und lesen sie mit spezieller Hardware ein, um ihren ursprünglichen Inhalt wiederherzustellen", sagte Ehrschwendner abschließend. Dafür würden oft nicht-dokumentierte Befehle und Schnittstellen des Herstellers zum Datenträger genützt. "Es ist keinesfalls

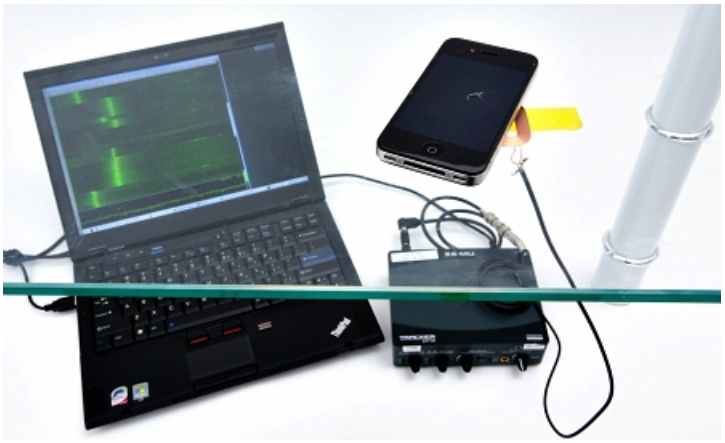
auszuschließen, dass derlei auch für iPhones existiert."

FBI-Vertrag mit Cellebrite am 21. März

Mit welcher Methode das FBI nun auch ohne Apple an die Daten kam, ist derzeit ebenso unbekannt wie Volumen und Inhalt der ausgelesenen Daten. FBI-Chef James Comey begnügte sich damit, die hier geschilderten Ansätze kurz zu dementieren und sprach von einer völlig anderen Lösung, die angeblich zum Einsatz kam. Erst am 21. März hatte das FBI mit Cellebrite einen Vertrag im Auftragswert von 15.000 Dollar abgeschlossen, es kann sich also nicht um einen Großeinkauf neuer Hardware handeln.

Der Vertrag zwischen Cellebrite und dem FBI vom 21. März (https://www.fpds.gov/ezsearch/fpdsportal?q=cellebrite+CONTRACTING_AGENCY_NAME%3A%22FEDERAL+BUREAU+OF+INVESTIGATION%22+PIID%3A%22DJF161200P0004424%22+PIID%3A%22DJF161200P0004424%22&s=FPDSNG.COM&templateName=1.4.4&indexName=awardfull&sortBy=SIGNED_DATE&desc=Y)

Angesichts der Summe kommen dafür eher Dienstleistungen in Frage wie etwa das Auslesen von Handydaten in komplexeren Fällen, mit denen die FBI-Techniker überfordert sind. In etwa so könnte auch die Geschäftsbeziehung des Wiener Innenministeriums zu Cellebrite gelagert sein. Wie nämlich auf Umwegen zu erfahren war, wurden über mehrere Jahre insgesamt "deutlich unter 100.000 Euro" vom Innenministerium an Cellebrite bezahlt.



Eran Tromer

Ein billiges Set-Up zu Mittschnitt und Darstellungen von elektromagnetischen Abstrahlungen von Chips der Universität Tel Aviv.

Sensoren, Soundkarten, elliptische Kurven

Am 1. März hatte ein Forscherteam der Universität Tel Aviv eine Untersuchung über berührungslose Schlüsselextraktion aus Mobiltelefonen, insbesonders solche mit dem Apple-Betriebsystem iOS vorgestellt. Die Angriffsweise ähnelt den Tempest-Attacken der 90er Jahre auf die Abstrahlung von Monitoren, ist aber wesentlich komplexer und macht verblüffend wenig Hardware-Aufwand nötig. Ein billiger Magnetsensor, eine externe Soundkarte sowie ein Laptop genügen, um Verschlüsselungsvorgänge in der Hardware von Handychips zu verfolgen.

"ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels" (https://www.cs.tau.ac.il/~tromer/mobilesc/)

Über den Sensor werden die Abstrahlungen des Prozessors während der Verschlüsselungsprozesses eingefangen, digitalisiert und auf dem Laptop dargestellt. Da die Rechenoperationen und die elliptische Kurvenformel für den betroffenen ECDSA-Schlüssel standardisiert sind, lässt sich messen, in welcher Reihenfolge und wie oft addiert und multipliziert wird. Auf diese Weise sei es gelungen, die ECDSA-Signaturschlüssel aus OpenSSL und CoreBitcoin auf Geräten mit Apples iOS vollständig zu extrahieren, sowie Teile der Schlüssel, die über Apples "CommonCrypto"-Bibliothek generiert wurden, herauszufinden, schreiben die Forscher.

Fazit und Ausblick

Was diese Attacke im Tempest-Stil betrifft, so ist alleine die Extraktion von Schlüsselteilen bereits mehr als die vielzitierte "halbe Miete", um an die Schlüssel zu gelangen. Und das sind keine Passwörter wie in besagtem iPhone, sondern Signaturschlüssel oder Zertifikate, die für ZahluNgsverkehr genutzt werden. Von solchen Methoden wird man in näherer Zukunft noch Einiges hören, denn hier ist Angriffspotenzial vorhanden.

Es ist naturgemäß nicht zu sagen, ob und welcher der hier verkürzt geschilderten Ansätze vom FBI benutzt wurde. Genaugenommen sind die Aussagen des FBI nicht einmal bestätigt, es wurden ja keinerlei Ergebnisse vorgelegt.