Werkzeuge zum Knacken der Apple iPhone / iPad Data Protection öffentlich verfügbar

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Im Mai dieses Jahres präsentierten die beiden Franzosen Jean-Baptiste Bédrune und Jean Sigwald auf der Sicherheitskonferenz Hack-in-the-Box in Amsterdam brisante Details zur Funktionsweise der Apple Data Protection. Wenige Tage später veröffentlichte die russische Softwareentwicklungsfirma Elcomsoft mit dem „Acquisition Toolkit" ein Produkt zum Knacken des iOS-Verschlüsselungssystems, welches Strafverfolgungs–behörden und Geheimdiensten zum Kauf zur Verfügung steht.

Die erforderlichen Werkzeuge zum Auslesen von Daten, die mit der Apple Data Protection geschützt sind, stehen aber nicht nur Strafverfolgungs–behörden zur Verfügung, sondern sind seit Mai im Internet als Open Source Tools frei erhältlich und können mit ausreichend technischem Know-How von beliebigen Anwendern zum Knacken des Apple Verschlüsselungssystems eingesetzt werden.

Basis eines solchen Angriffs sind öffentlich bekannte Schwachstellen im BootROM der Apple-Geräte, die auf einem iPhone 4 oder einem iPad der ersten Generation beispielsweise mit Hilfe des Exploits Limera1n ausgenutzt werden können. Dieser Exploit erlaubt das Starten einer Live-Betriebssystemumgebung auf den Apple-Geräten mit Zugriff auf den lokalen Datenträger. Als Live-Umgebung wird in der Regel auf die von Apple bereitgestellte Restore RAMdisk zurückgegriffen, die im Fehlerfall von iTunes zur Wiederherstellung des Betriebssystems auf den Geräten gestartet wird. Da die Restore RAMdisk den Datenträger beim Start transparent entschlüsselt, bietet auch die integrierte Hardwarever–schlüsselung keinen Schutz gegen das Auslesen vertraulicher Daten. Mit entsprechenden Modifikationen kann die Restore RAMdisk zum Starten eines SSH-Servers genutzt werden, auf den von einem angeschlossenen PC aus über die USB-Schnittstelle zugegriffen werden kann. Die notwendigen Werkzeuge zum Starten der Live-Umgebung stellt beispielsweise der Syringe iDevice Exploit Injector des Chronic Dev Team zur Verfügung.

Nach dem erfolgreichen Start der modifizierten Restore RAMdisk kann ein Angreifer über den SSH-Server die Live-Betriebssystemumgebung ansteuern und die lokalen Laufwerke des Apple-Gerätes einbinden. Damit erhält er bereits Zugriff auf alle nicht zusätzlich verschlüsselt gespeicherten Daten. Dazu gehören unter anderem die in den Medien öffentlich bekannt gewordene „crowd-sourced"-Datenbank cache.db (siehe cirosec Pressemitteilung „Apple iOS Update löst die Datenschutzprobleme nicht vollständig" vom 06.05.2011) sowie Kontakte, Kalenderdaten oder alle auf der Bildschirmtastatur eingegebenen Texte, die Apple in der Datei „de_DE-dynamic-text.dat" speichert (siehe Abbildung 1). Diese Angriffsmethode wird von der cirosec bereits seit letztem September auf verschiedenen Veranstaltungen zum Thema iOS-Sicherheit präsentiert.

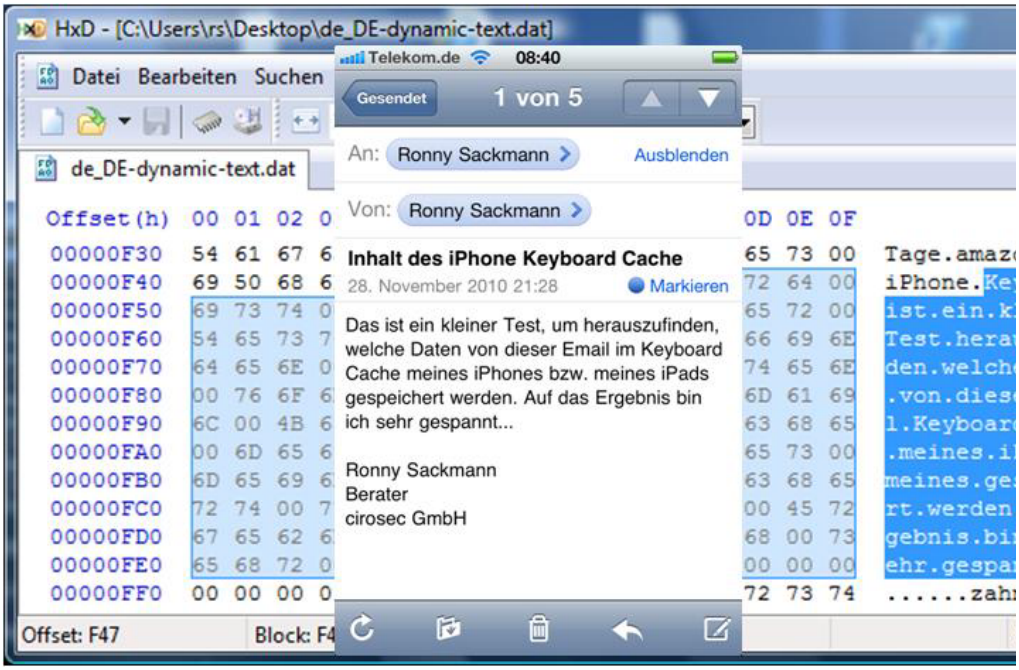

Abbildung 1: Auszug aus dem unverschlüsselt gespeicherten Keyboard-Cache eines Apple Gerätes

Das Ausnutzen der Schwachstelle im Bootloader ermöglicht es ferner, den Kernel der Live-Betriebssystemumgebung so zu patchen, dass Programme den in den Apple-Geräten integrierten AES-Chip direkt ansprechen können. Der dazu erforderliche Exploit ist ebenfalls im Netz frei verfügbar.

Mit weiteren Werkzeugen kann ein Angreifer nun auch die Daten auslesen, die mit der Apple Data Protection geschützt sind. Im einfachsten Fall erfolgt dies unter Verwendung des in den AES-Chip eingebetteten AES-Schlüssels. Hat der Besitzer eine Code-Sperre auf seinem Apple-Gerät gesetzt, fließt dieser zusätzlich in die Berechnung der Schlüssel mit ein. Mit Hilfe von Brute-Force-Methoden kann ein Angreifer diesen Passcode jedoch direkt auf dem Gerät ermitteln. Besonders brisant ist, dass der Angreifer in der Anzahl der Versuche nicht limitiert ist. Die Schutzfunktion „Local Wipe“ nach X falschen Code-Eingaben greift nur im normalen Betriebsmodus, wenn das iOS-Betriebssystem vollständig gestartet ist. Dies ist bei der Angriffsmethode mittels RAMdisk aber nicht der Fall. Auf einem iPhone 4-Testgerät der Firma cirosec lag die maximale Dauer bei einer einfachen PIN als Passcode bei ungefähr 29 Minuten. Mit einem erfolgreichen Brute-Force-Angriff bekommt ein Angreifer Zugriff auf alle in der Keychain gespeicherten Informationen wie Passwörter, Zertifikate und private Schlüssel (siehe Abbildung 2).

Abbildung 2: Entschlüsselte Inhalte der Keychain

Daneben sind aber auch alle mit der Data Protection auf Dateiebene verschlüsselte Daten zugänglich. Abbildung 3 zeigt beispielhaft die standardmäßig verschlüsselten Emails der nativen Mail-Applikation eines Apple-Gerätes.

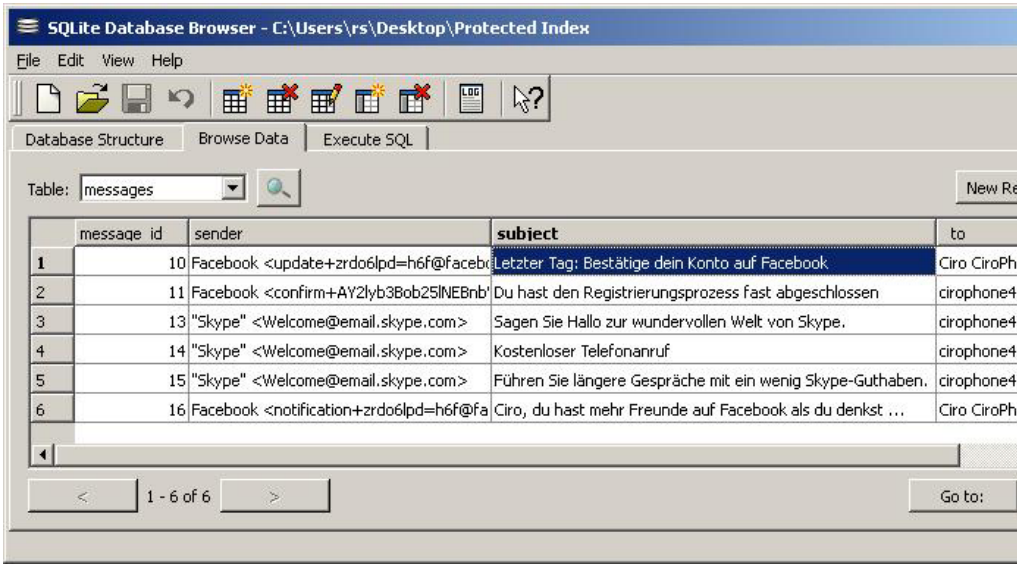

Abbildung 3: Entschlüsselte Email-Nachrichten der nativen Mail-Applikation von Apple

Die Erfahrung von cirosec zeigt, dass bei einer einfachen PIN im Durchschnitt lediglich 10 Minuten physikalischen Zugriffs auf ein Apple-Gerät genügen, um einen Angriff erfolgreich durchzuführen. Der Besitzer hat anschließend keine Möglichkeiten zu erkennen, dass dieser Angriff durchgeführt wurde. Die Abfrage der SIM-PIN kann lediglich einen Hinweis dafür geben, dass das Gerät neu gestartet wurde. Betroffen von dieser Problematik sind derzeit alle Apple-Geräte mit Ausnahme des iPads der zweiten Generation. Dies ist darauf zurückzuführen, dass für das iPad 2 bisher noch keine Schwachstellen öffentlich bekannt sind, die einen derartigen Angriff ermöglichen.

Der Aufwand zur Berechnung des Passcode kann mit der Erweiterung des Zeichenraums erheblich erschwert werden. Geht man bei einer einfachen PIN von einer maximalen Dauer von 29 Minuten aus, so würde die Berechnung unter der Verwendung alphanumerischer Zeichen im Worst Case schon ca. 33 Tage dauern. Erweitert man den Passcode zusätzlich von vier auf fünf Stellen würde ein Angreifer mit einem Brute-Force-Angriff im schlechtesten Fall schon ca. 5 ½ Jahre auf das Ergebnis warten.

Unternehmen, die derzeit betroffene Apple-Geräte im Einsatz haben, sollten sicherstellen, dass ein Passcode auf dem Gerät gesetzt ist und die Komplexität des Passcodes den Sicherheitsanforderungen der gespeicherten Daten gerecht wird. Bei eigenen Applikationen können Entwickler besonders sensitive Daten vor der Ablage mittels Data Protection als zusätzlichen Schutzmechanismus mit einer eigenen Verschlüsselung schützen.

Ronny Sackmann, Berater bei der cirosec GmbH