Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Apple-Geräte angreifbar

Forscher finden Sicherheitslücken im Betriebssystem von iPhone und iPad

Kommunikation und Medien
Corporate Communications
Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:
Jörg Feuck
Tel. 06151 16 - 20017
Fax 06151 16 - 23750
feuck@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 23. August 2016. Ein internationales Team von Cybersicherheitsforschern unter Beteiligung der TU Darmstadt hat schwerwiegende Sicherheitslücken im Betriebssystem iOS gefunden, mit dem das iPhone und das iPad betrieben werden. Die Sicherheitslücken machen eine Vielzahl von Angriffen auf die Handys und Tablets von Apple möglich.

„Viele Menschen denken, dass das geschlossene Betriebssystem von Apple sicherer ist als das offene Android-System. Wir wollten die Sicherheitstechnologien von iOS deswegen unter die Lupe nehmen“, erklärt Ahmad-Reza Sadeghi, Professor für Systemsicherheit am Profilbereich Cybersicherheit der TU Darmstadt. In den letzten iOS-Versionen habe Apple immer wieder neue Technologien, speziell zum Schutz der Nutzerprivatheit, eingeführt. „Unser Ziel war es herauszufinden, ob wir die Erkennung von Sicherheitslücken automatisieren können, was bei einem geschlossenen System wie iOS nicht trivial ist.“

Gemeinsam mit Forschern der North Carolina State University und der University Politehnica of Bucharest untersuchten Sadeghi und sein Team die „Sandbox“ des iOS Systems, eine Schnittstelle zwischen den Apps und dem Betriebssystem. Jede Drittanbieter-Anwendung bekommt dort ein festgelegtes Profil zugewiesen, in dem geregelt ist, auf welche Informationen die App zugreifen und welche Aktionen sie ausführen darf.

Um diese Profile auf Sicherheitslücken zu untersuchen, die bösartige Drittanbieter-Apps ausnutzen könnten, wurden die binär-kodierten Sandbox-Profile aus dem Betriebssystem extrahiert und dann in eine für Menschen lesbare Form umgewandelt. So konnte ein Modell für jedes einzelne Profil erstellt und mit Hilfe von selbstentwickelten vollautomatischen Tests auf Sicherheitslücken untersucht werden.

„Wir haben bedenkliche Sicherheitslücken gefunden“, so Sadeghi. Mithilfe von Drittanbieter-Apps könnten viele Nutzerdaten ausgespäht werden. Die möglichen Angriffe können zur Folge haben:

- Umgehen der iOS-Datenschutzeinstellungen für Kontakte;
- Zugriff auf den Nutzernamen und die Medienbibliothek;
- Sperren des Zugangs zu Systemressourcen, beispielsweise kann der Nutzer nicht mehr auf das Adressbuch zugreifen;
- Apps können Informationen miteinander teilen, obwohl sie dazu keine Berechtigung haben;

TECHNISCHE UNIVERSITÄT DARMSTADT

- Preisgabe sensibler Informationen, zum Beispiel wann Fotos aufgenommen wurden, durch den Zugriff auf Metadaten von Systemdateien;
- Sperren von Speicherplatz, der auch nach dem Deinstallieren der bösartigen App nicht wieder freigegeben wird.

„Apple hat schnell auf unsere Erkenntnisse reagiert und die Problemlösungen mit uns diskutiert“, so Sadeghi. In der nächsten Version von iOS wolle Apple Sicherheitslücken schließen. „Trotzdem sind wir immer noch der Meinung, dass Apple sich von der Zusammenarbeit mit der akademischen Forschung zu sehr abschottet und keine Kooperationen anstrebt.“

Aus der internationalen Zusammenarbeit der Cybersicherheitsforscher entstand das Paper “SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles”, das bei der renommierten ACM Conference on Computer and Communications Security (CCS) Ende Oktober in Wien vorgestellt werden wird.

MI-Nr. 60/2016, Braun/feu