Chaos Computer Club hackt Apple TouchID

21. September 2013

frank, CCC

Hackern des Biometrie-Teams des Chaos Computer Clubs (CCC) ist es gelungen, die biometrischen Sicherheitsfunktionen des Apple TouchID mit einfachsten Mitteln zu umgehen. Dazu genügte den Hackern ein Fingerabdruck, welchen sie von einer Glasoberfläche abfotgoraphierten, um einen künstlichen Finger zu erzeugen. Damit waren sie in der Lage, ein iPhone 5s zu entsperren, welches mit TouchID geschützt war. Damit demonstrierten die Hacker wieder einmal, dass biometrische Daten zur Verhinderung eines unberechtigten Zugriffs vollkommen ungeeignet sind.

Das neue iPhone 5s ist mit einem Fingerabdrucksensor ausgestattet, den Apple als wesentlich sicherer als bisherige Sensoren angepriesen hat. Selbst in technologischer Fachpresse wird seit Tagen über den Gewinn für die Sicherheit diskutiert.

«Tatsächlich hat der Sensor von Apple nur eine höhere Auflösung im Vergleich zu bisherigen Sensoren. Wir mussten nur die Granularität unseres Kunstfingers ein wenig erhöhen», erklärt der Hacker mit dem Pseudonym starbug, welcher durch Experimente die Methode für die Überlistung des Sensors optimiert hat. «Seit Jahren warnen wir immer wieder vor der Verwendung von Fingerabdrücken zur Zugriffssicherung. Fingerabdrücke hinterlassen wir überall, und es ist ein Kinderspiel, gefälschte Finger daraus zu erstellen.»

Das Vorgehen zur Überwindung ist in diesem Video dokumentiert: Hacking iPhone 5s TouchID.

Die Methode entspricht folgenden Schritten und nutzt Materialen, die in nahezu jedem Haushalt vorhanden sind: Zuerst wird der Fingerabdruck eines Benutzers mit einer Auflösung von 2400 dpi fotographiert. Das Foto wird dann am Computer bereinigt, invertiert und per Laserdrucker auf eine Transparenzfolie gedruckt. Dabei sollte eine Auflösung von 1200 dpi bei maximaler Druckstärke nicht unterschritten werden. Auf das Druckbild wird dann hautfarbene Latexmilch oder weisser Holzleim aufgetragen. Durch die Drucklinien entsteht ein Fingerabdruckbild in dem aufgetragenen Material. Nach dem Trocknen kann der gefälschte Finger abgenommen werden. Diesen feuchtet man leicht an, indem man ihn anhaucht. Dann kann man das iPhone damit entsperren.

«Wir hoffen, dass dies die restlichen Illusionen ausräumt, die Menschen bezüglich biometrischer Sicherheitssysteme haben. Es ist einfach eine dumme Idee, etwas als alltägliches Sicherheitstoken zu verwenden, was man täglich an schier unendlich vielen Orten hinterlässt», sagt Frank Rieger, Sprecher des CCC. «Die Öffentlichkeit sollte nicht länger von der Biometrie-Industrie mit falschen Aussagen an der Nase herumgeführt werden. Biometrie ist geeignet, um Menschen zu überwachen und zu kontrollieren, nicht um alltägliche Geräte vor dem Zugriff zu sichern.» Auch Fingerabdrücke in Ausweisdokumenten sind in vielen Ländern seit einigen Jahren eingeführt worden, obwohl von diesen kein Sicherheitsgewinn ausgeht.

iPhone-Benutzer sollten vermeiden, sensible Daten mit ihrem Fingerabdruck zu sichern. Dabei

geht es nicht nur darum, dass der Fingerabdruck so leicht gefälscht werden kann. Auch kann man sehr leicht dazu gezwungen werden, sein Telefon zu entsperren, wenn man festgenommen wird. Einen Menschen dazu zu zwingen, ein sicheres Passwort preiszugeben, ist dagegen um einiges schwieriger als einfach das Telefon vor seine Hände in Handschellen zu halten.

Bedanken möchten wir uns vor allem beim Heise-Security-Team, welches kurzfristig ein iPhone 5s zur Analyse bereitstellen konnte. Weitere Informationen zum Hack werden dort bereitgestellt.

Hacking iPhone 5s TouchID