iPhone X: Face ID soll mit Maske überlistet worden sein

13 November 2017 | **Product Engineering, Software Engineering, User Experience** | **Raphael Reischuk**
Lesezeit: 3 Minutes

Vietnamesische Sicherheitsexperten wollen Apples Gesichtserkennung geknackt haben. Das mag sein, aber es gibt eine Lösung für das Problem.

Mitarbeiter der vietnamesischen IT-Sicherheitsfirma Bkav haben nach eigenen Angaben Face ID geknackt. Die Gesichtsentsperrung hat Apple kürzlich mit dem iPhone X lanciert. Die Sicherheitsexperten haben eine Maske aus vier Teilen gebaut: einem weissen Gerüst aus dem 3D-Drucker, das in einem Metallrahmen steckt, einer handgefertigten Nase aus Silikon samt Make-up sowie 2D-Bildern von Augen und Mundpartie. In jedem Fall müssten die Cyberkriminellen die genauen Masse des Gesichts haben, um die Maske bauen zu können, schreibt Bkav auf seiner Website.

Im folgenden Video zeigt das Sicherheitsunternehmen, wie das iPhone X mit der Maske entsperrt worden sein soll, was offenbar problemlos gelang:

Insgesamt soll die Maske Materialkosten von 150 Dollar verursacht haben. Bkav hatte mit den Arbeiten am 5. November begonnen. Das Unternehmen hatte zuvor unter anderem Schlagzeilen mit dem Überlisten von Gesichtserkennungssystemen in Notebooks gemacht. Ist das Ganze eine Gefahr für Millionen iPhone-X-Besitzer? Nein, sagen die Sicherheitsforscher. Aber in Gefahr seien beispielsweise Chefs von Grossunternehmen, Spione oder Milliardäre – falls der Angriff so wirklich funktioniert. Denn um auf deren Geräte zugreifen zu können, lohne sich der Aufwand.

Es war nur eine Frage der Zeit, bis die ersten Sicherheitsexperten sich Face ID erfolgreich vorknöpfen würden. Denn grundsätzlich lässt sich jedes heute bekannte computergestützte Authentifizierungssystem mit genügend Aufwand brechen. Am Ende entscheidet ein Algorithmus anhand der zur Verfügung stehenden Information, und diese Entscheidung ist im Bereich der Authentisierung eben nur null oder eins, ja oder nein, Zugriff gewährt oder abgelehnt.

Perfekte Sicherheit gibt es nicht
Genau darauf basieren die heute gängigen und praktikablen Sicherheitslösungen: Perfekte Sicherheit gibt es nicht, die Hürde muss nur gross genug sein, um den durchschnittlichen Angreifer auf ein schwächeres Ziel zu verweisen. Beispiel: Im Bereich der symmetrischen

quantensicheren Verschlüsselung braucht es bei richtiger Schlüsselwahl so viel Rechenpower, dass es selbst für Geheimdienste derzeit unmöglich scheint, die Verschlüsselung zu brechen. Möglich ist es allerdings – genügend Ressourcen vorausgesetzt. Informationstheoretisch sichere Verschlüsselung gibt es seit über 100 Jahren, diese kommt aber aus Gründen mangelnder Kompatibilität kaum zum Einsatz.

Analoges gilt für die Authentifizierung: Mit einem umfassenden Scan des Gehirns, der Blutbahnen und der DNA könnten fälschungssichere Authentifizierung ermöglicht werden („by definition"). Allerdings wäre solch ein Verfahren alles andere als praktikabel.

Password-Generatoren bei Madame Tussauds
Folglich ist jede vernünftig nutzbare Authentisierung ein Trade-off. Apple hat mit Face ID diesen Trade-off in beeindruckende Richtungen bewegt, nämlich ein bis dato unerreichtes Mass an Sicherheit bei gleichbleibend guter Usability. Dass auch dieses Verfahren mit viel Aufwand gebrochen werden kann, ist keine Überraschung und Apple bewusst. Bis 3D-Scanner jedoch zu flächendeckenden Passwort-Generatoren bei Madame Tussauds werden, wird es noch einige Zeit dauern.

Ganz zum Schluss: Wer weiss eigentlich, dass der Authentication-Hack tatsächlich authentisch ist? Vielleicht ist der Auth Hack nur ein Fake. Fakt ist, wie Bkav selbst einräumt: In jedem Fall muss die per Maske zu hackende Person einem gründlichen 3D-Scan unterzogen werden. Hier kommen wohl nur Erpressungs- und Foltermethoden in Betracht.

Zum Schluss sei angemerkt, dass der gezeigte Angriff wohl nicht dauerhaft Bestand haben wird. Denn sobald Apple dynamische Features in Betracht zieht, also ein Scan des bewegten Gesichtes von beispielsweise einer halben Sekunde, wird eine statische Maske nicht mehr funktionieren. Davon abgesehen: Das grösste Risiko ist momentan, dass ein Angreifer einem das iPhone X aus der Hand reisst, das Opfer am iPhone anmeldet und uneinholbar davonrennt. Dieses Risiko würde durch einen längeren dynamischen Scan ebenfalls minimiert.