Forscher demontieren App-TANs der Sparkasse

Mit Apps, die TANs erzeugen, wollen Banken das Online-Banking auf dem Smartphone attraktiver machen. Doch zwei Forscher der Uni Erlangen kritisieren die Abkehr unter anderem der Sparkassen vom bewährten Konzept der starken Zweifaktor-Authentifizierung. Sie untermauern diese Kritik mit einem konkret demonstrierten Angriff auf die App-Kombination Sparkasse und S-pushTAN. Der leitet eine Überweisung auf ein anderes Konto um und ändert dabei auch gleich den Betrag. Ähnliche Angriffe seien mit hoher Wahrscheinlichkeit auch gegen App-basierte TAN-Verfahren anderer Banken möglich, warnen die Forscher. Der Sparkasse zufolge funktioniert der Angriff mit der aktuellen Version der S-pushTAN-App nicht mehr.

Immer mehr Banken bieten App-basierte TAN-Verfahren an, die mehr Komfort bieten sollen – aber das letztlich auf Kosten der Sicherheit. Dabei nutzt der Anwender eine Online-Banking-App auf seinem Smartphone; eine zweite App auf demselben Gerät fordert über verschlüsselte Kommunikation mit der Bank eine TAN an, die es anschließend anzeigt; ein Klick befördert sie komfortabel in die Banking-App, wo der Anwender den Vorgang abschließen kann. Dadurch funktioniert das Verfahren ähnlich wie die mTAN und hat demgegenüber den Vorteil, dass die Kommunikation mit der Bank kryptographisch gesichert erfolgt und folglich nur schwer angreifbar ist.

Der entscheidende Nachteil dieser komfortablen App-TANs: Der komplette Vorgang einer Online-Banking-Transaktion findet auf einem einzigen Gerät statt. Somit genügt es, in dieses eine Gerät einen Trojaner einzuschleusen. Dass diese Gefahr keineswegs nur theoretisch ist, belegen Vincent Haupert und Tilo Müller von der Forschungsgruppe Systemsicherheit und Softwareschutz mit einer Demonstration.

Durch gezielte Manipulationen im Betrieb der Sparkassen-App fängt ihr Schadcode eine vom Nutzer in Auftrag gegebene Überweisung ab und verändert diese. Die vom Anwender tatsächlich durchgeführte Überweisung sendet dann einen deutlich höheren Betrag an ein anderes Konto. Der Anwender hat dabei keine Chance die Manipulation zu erkennen, da „die angezeigten Daten zu jeder Zeit des Transaktionsprozesses den eingegeben Werten entsprechen“.

Solche Angriffe sind nicht trivial. Man benötigt unter anderem einen speziellen Root-Exploit gegen die auf dem Smartphone eingesetzte Android-Version. Außerdem muss man die Apps analysieren. Zwei bis drei Wochen benötigten die Forscher für diese Analysen. Doch „professionelle Online-Banking-Betrüger könnten das durchaus auch schaffen“, erklärten Haupert und Müller gegenüber c’t.

Die Forscher sehen den erfolgreich demonstrierten Angriff als Nachweis einer konzeptionellen Schwäche aller App-TAN-Verfahren, die nicht auf getrennte Hardware setzen. Für sicheres Online-Banking empfehlen sie deshalb dringend, einen zweiten, unabhängigen Authentifizierungsfaktor einzusetzen, wie ihn ChipTAN-Verfahren bieten. (ju@ct.de)

Immer mehr Banken setzen auf das App-TAN-Verfahren für Online Banking. Dabei erzeugt eine App die TAN und überträgt diese direkt in die Online-Banking-App. Das alles findet auf demselben Gerät statt.

Todesstoß: Erster praktikabler Angriff auf SHA-1

Sicherheitsforscher haben die seit einem Jahrzehnt als angeschlagen geltende Hashfunktion SHA-1 erfolgreich attackiert. Dafür haben sie einen 64-GPU-Cluster zehn Tage lang rechnen lassen.

Die Kryptologen haben eine sogenannte Freestart Collision für SHA-1 entwickelt. Das Verfahren ist aber noch keine echte Kollision, die die Hashfunktion komplett aufbricht. Dem Team zufolge ist die Freestart Collision aber ein wichtiger Zwischenschritt und der Ansatz gibt einen Ausblick, wann es soweit sein könnte. Die Sicherheitsforscher gehen von einer baldigen Kompromittierung aus. Frühere Berichte prophezeiten das für das Jahr 2017.

Schon seit 2005 existieren theoretische Kollisionsattacken auf SHA-1, die die Kryptologen ausgebaut haben. Ihr Ansatz zeigt auf, dass Grafikkarten die Berechnungen besonders effizient stemmen können. Das geht nicht nur schneller als mit CPUs, sondern senkt auch die Kosten.

Aufgrund ihrer Erkenntnisse raten sie dringlich dazu, SHA-1 sobald wie möglich nicht mehr einzusetzen. Zudem sprechen sie sich gegen das Vorhaben des CA/Browser Forums aus, die Verteilung von SHA-1-Zertifikaten bis zum Ende des Jahres 2016 zu verlängern.

Der beteiligte Sicherheitsforscher Marc Stevens war auch Teil des Teams, das bereits MD5 den Todesstoß versetzt hat. Dabei nutzten sie eine MD5-Kollision, um sich selbst ein CA-Zertifikat zu erstellen, das von allen Browsern akzeptiert wurde. (des@ct.de)

BSI will Sicherheit von Routern kenntlich und vergleichbar machen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den Entwurf eines Konzeptes vorgestellt, mit dem Router auf Sicherheitslücken getestet werden sollen. Ziel ist es, einheitliche Kriterien zu etablieren, um die Sicherheit der Geräte messbar und vergleichbar zu machen. Bis zum 30. November können Hersteller solcher Geräte und Internet Service Provider den Entwurf kommentieren und per E-Mail Ergänzungsvorschläge an das BSI schicken.

Endkunden-Geräte haben zwangsläufig Lücken und das Stopfen derselben scheint bei den meisten Herstellern nicht besonders hoch auf der Prioritätenliste zu stehen. Das BSI begründet seinen Konzeptentwurf eben damit, dass die Sicherheit – oder mangelnde Sicherheit – eines solchen Gerätes ein wichtiges Kaufkriterium sei.

Die Vorschläge des BSI sehen eine Prüfung der Aktualität der Firmware, der Router-Firewall, der WLAN-Verschlüsselung und der WPS-Umsetzung vor. Dabei sollen Tester die Funktionsweisen allein anhand des Webinterfaces und anderer dokumentierter Zugriffsmöglichkeiten prüfen – eine Sichtung des Quellcodes der Software ist dem BSI zufolge nicht geplant. Der Test der einzelnen Funktionen schließt dem Konzept zufolge mit einer Punktzahl ab. Am Ende soll ein Gesamtwert die Sicherheit des getesteten Routers widerspiegeln. (fab@ct.de, des@ct.de)

Online-Shops verteilen Exploit-Kit

Unbekannte haben tausende Online-Shops, die auf der Shop-Software von Magento basieren, mit Schadcode infiziert. Besucher von betroffenen Shop-Webseiten bekommen das Exploit-Kit Neutrino untergeschoben, mit dem die Drahtzieher der Angriffe Bezahldaten abgreifen. Magento zufolge bilden alte Sicherheitslücken das Einfallstor, für die es schon Patches gibt; betroffene Shop-Betreiber haben diese aber noch nicht installiert (siehe c't-Link). Die aktuelle Magento-Version soll nicht mehr anfällig sein.

Zudem erklärte Magento gegenüber c’t, dass die Angreifer einige betroffene Seiten über schwache Admin-Passwörter oder Lücken in anderer Software infiltriert haben. Google hat nach Bekanntwerden der Angriffe über 8000 betroffene Webseiten geblockt. Magento zufolge setzen aber nicht alle geblockten Webseiten ihre Shop-Software ein. Die Angreifer scheinen also auch Webseiten zu kompromittieren, die andere Shop-Systeme einsetzen. (fab@ct.de)

c't Sicherheitstipps von Magento: ct.de/y31s

Notizen

Die **Joomla** Version 3.4.5 dichtet drei Lücken ab.

Ein Patch macht das **Akismet**-Plug-in für WordPress sicherer.

In **LibreSSL** klaffen bis hin zur aktuellen Version 2.3.0 zwei Lücken. Die Version in OpenBSD 5.8 soll gefixt sein.