Wie sieht es bei sminks mit der Sicherheit aus?

„In der Sicherheitstechnologie sind Bezeichnungen wie „hundertprozentig" oder „unmöglich" unglaubwürdig. Eine hundertprozentige Sicherheit existiert nicht. Ziel der Absicherung eines Systems oder Prozesses muss sein, einen Angriff so kostspielig zu gestalten, dass der daraus zu ziehende Nutzen vergleichsweise gering ist."

Systembedingte Sicherheit

Bei sminks handelt es sich um ein Drei-Parteien-System, bei dem die eigentliche Kontoführung und Transaktion durch dritte Banken ausgeführt wird. Beide Parteien, Sender und Empfänger einer Zahlung, müssen bei sminks registriert sein und ihre jeweiligen Bankdaten hinterlegen. Welche Konten für eine Zahlungen innerhalb des Systems angestoßen werden, wird durch sminks bestimmt und kontrolliert. Die Monetarisierung eines großflächigen Angriffs z.B. durch Datenklau (vgl. Kreditkarte oder EC-Karten Dublette) ist daher nahezu ausgeschlossen.

Das System arbeitet intern mit Forderungen, nicht mit Geldströmen. Das Umleiten oder Abändern einer Forderung ist für einen Angreifer also nutzlos.
Der Zahlende signiert die Forderung, die ihm auf dem Display seines Smartphones gezeigt wird. Eine Abänderung dieser Einblendung ist ohne Kontrolle des Zentralservers nicht möglich, da er eine Kopie der Forderung besitzt und Forderungen grundsätzlich nur innerhalb der Systemstruktur gestellt werden können, nicht von außerhalb.

Sicherheit durch Entwicklungs-Paradigmen

Sminks verwendet in sicherheitsrelevanten Bereichen keine Softwaremodule von Dritten oder Open Source. Angriffe wie Heartbleed oder Lücken wie CVE-2014-0224 zeigen, dass Open Source nicht zwingend sicher ist. Ein System, das z.B. OpenSSL einsetzt, kann aufgrund der Verwendung dieses Moduls kompromittiert werden, ohne dass es direktes Ziel des Angriffs war. Die Verwendung von Modulen Dritter senkt das Sicherheitsniveau auf die Ebene der Schnittstelle(!) zwischen den Modulen. Daher sind einzelne Elemente des Systems sminks monolithisch und Eigenentwicklungen. Die Programmiersprache in allen sicherheits-relevanten Bereichen ist C++.

Sicherheit durch Krypto-Algorithmen

In der Kommunikation zwischen Endgerät und Client Access Point (CAP) kommt RSA2048 und AES512 zum Einsatz (Hybridkommunikation). Sicherheitsrelevante Hashes werden mit SHA256 erstellt und sind salted. Die genannten Algorithmen repräsentieren den aktuellsten Stand der Sicherheitstechnik.

Sicherheit durch Struktur

Ein System dessen Endgerätekommunikation via Internet erfolgt, bietet eine größere Angriffsfläche als Systeme mit eigenständiger Kommunikation (vgl. EC-Karte/GSM). Sminks verwendet daher - und aus Gründen der Skalierbarkeit – ein System mit drei zentralen Komponenten: Endgerät, Client Access Point (CAP) und zentrale Server. Während sich die eigentlichen Server in einem als sicher anzunehmenden, eigenen Netz befinden, agieren die CAPs als Brücken zum Internet. Die Server sind gegenüber den CAPs daher ebenso (wenn auch asymmetrisch) abgesichert, wie die CAPs gegenüber den Endgeräten. Durch die geschickte Verteilung von Schlüsseln ist es für einen Angreifer nicht möglich, einen finanziellen Nutzen aus der Übernahme eines CAP-Rechners zu ziehen.

Sicherheit auf dem Endgerät

In jedem mobilen System ist das Endgerät das schwächste Glied der Sicherheitskette. Ein Sicherheitskonzept muss davon ausgehen, dass es schon in der ersten Stufe eines Angriffes kompromittiert ist. Ein Angreifer erhält durch die Analyse der Software Kenntnisse über die Kommunikation und die verwendeten Verschlüsselungsalgorithmen. Ein Smartphone, das dies hardwareseitig verhindert, existiert für den Consumer-Bereich nicht. Ohnehin muss sich ein Sicherheitskonzept an der unsichersten Hardware orientieren, die es unterstützt.
Sminks verfolgt hier zwei Ansätze: einerseits Schutz des Einzelnen durch eine PIN, die vom CAP validiert wird. Zum anderen Schutz des gesamten Systems, indem auf dem Endgerät keine Informationen gespeichert werden, die eine Übertragung auf andere Geräte ermöglichen. So wird z.B. als Geräte-ID eine zufällige 128 Bit Zahl verwendet. Selbst durch Kenntnis beliebig vieler dieser Zahlen lässt sich nicht auf eine unbekannte Geräte-ID schließen. Bei Geräteverlust oder Diebstahl ist selbst bei invasiver Analyse des Gerätes ein Kompromittieren des Kundenkontos nahezu ausgeschlossen.