vTEE für mobiles Bezahlen und Pin-on-Glass-Akzeptanz

Von Sam Shawki

Derzeit gibt es drei unterschiedliche Verfahren, um kryptografische Schlüssel auf mobilen Endgeräten zu speichern. Die jüngste Methode, die sogenannte virtuelle Trusted Execution Environment basiert auf den von der EMVCo Ende 2018 gestartete neue Kategorie „Software-Based Mobile Payments" und fungiert wie ein „virtueller Chip". Der Autor sieht hier das Potenzial, Smartphones zu vollumfänglichen Kartenakzeptanzgeräten zu machen. Das setzt freilich eine flächendeckende Ausstattung der Karteninhaber mit kontaktlosen Karten voraus. Red.

Die EMVCo hat Ende Dezember seine Spezifikationssuite erweitert und das Sicherheitsbewertungsverfahren für die neu eingeführte Kategorie „Software-Based Mobile Payments" (SBMP) gestartet. Dieser Schritt unterstützt Neuentwicklungen von Technologieanbietern und fördert die Sicherheitsbasis von mobilen Bezahllösungen. Anwendungen auf mobilen Endgeräten wie Verbraucher-Smartphones laufen in einer per se anfälligen Umgebung, weshalb ein innovativer, mehrschichtiger Software-Sicherheitsansatz nötig ist.

Für das Speichern kryptografischer Schlüssel auf mobilen Endgeräten durch App-Anbieter – zum Beispiel Anbieter von mPoS-Lösungen und Mobile Payment Wallets – existieren derzeit drei alternative Lösungen mit verschiedenen Implikationen hinsichtlich der mit ihnen einhergehenden Datensicherheit und Operabilität:

1. White-Box-Kryptografie: Eine aktuell gängige Lösung zur Speicherung von Bezahlschlüsseln ist die sogenannte „Obfuskation" (Veränderung von Programmcodes), zum Beispiel über White-Box-Kryptografie (WBC). WBC ist ein Software-basierter Mechanismus, der einen sicheren Speicherort für Daten errichtet. Bildlich gesprochen wird der sensible Datenteil hierbei wie die Nadel im Heuhaufen versteckt. Das Problem bei dieser Technologie: Sie in den Code zu implementieren ist arbeitsintensiv. Außerdem ist sie leicht angreifbar und benötigt daher kontinuierliche Updates und Downloads um den „Heuhaufen" zu aktualisieren, bevor er von Angreifern kompromittiert werden kann. Die Folge ist ein hoher operationaler und logistischer Aufwand.

Mittels bestimmter Angriffsszenarien, sogenannter „Fault Injections" oder „Side-Channel-Attacks", können entsprechend geschützte Systeme innerhalb relativ kurzer Zeit vollständig kompromittiert werden. Die dafür benötigten Ressourcen lassen sich inzwischen kostengünstig auf einschlägigen Websites erwerben und erfordern keine weitreichende Kryptografie-Expertise beim Angreifer.

2. Secure Elements und Trusted Execution Environments (TEE): Eine sicherere Lösung als WBC ist die Speicherung von kryptografischen Schlüsseln in einem sogenannten Secure Element. Hierbei handelt es sich um einen vom Gerätespeicher separierten Hardware-Chip. Dieser kann zum Beispiel fest im Gerät beziehungsweise als Chip-Partition verbaut werden oder in eine SIM-Karte eingebettet sein. Um ein entsprechend ausgerüstetes Endgerät kompromittieren zu können, müssen Angreifer physischen Zugriff erlangen. Das Sicherheitselement ist weder für Gerätenutzer noch für App-Entwickler zugänglich und kann von außen ausschließlich vom Gerätehersteller (OEM) kontrolliert werden. Die Entscheidung, ein Secure Element zu verbauen, liegt im Ermessen der OEMs. Einige Betreiber von Betriebssystemen unterstützen Secure Elements allerdings zugunsten der Hardwareunabhängigkeit ihrer mobilen Betriebssysteme nicht mehr.

Sam Shawki, Chief Executive Officer, MagicCube, Santa Clara

Selbst wenn es einem Angreifer gelingen sollte, Zugriff auf ein Sicherheitselement zu erlangen, sind maliziöse Anwendungen schwierig einzuschleusen, da Anwendungsart und -größe strikt limitiert sind. Dadurch ist das Element für Dritte kaum nutzbar, sofern sie keine Kooperation mit der Organisation eingehen, die den Chip kontrolliert. Die Anzahl der Geräte, die über ein Secure Element verfügen, ist gegenüber Geräten ohne diesen Chip allerdings relativ klein. Das gilt insbesondere mit dem Aufkommen von mehr und mehr IoT-Geräten.

Bei der Trusted Execution Environment (TEE) handelt es sich, stark vereinfacht ausgedrückt, um eine „größere" Version eines Hardware-basierten Secure Elements. Die TEE ist ein eigenes Betriebssystem und bietet erheblich mehr Funktionalitäten als ein Secure Element – unter anderem steuert sie viele Gerätetreiber, wie zum Beispiel den Fingerabdrucksensor. Die Kehrseite der Medaille: Ein umfassendes Betriebssystem hat eine komplexe Menge an allgemeinen Programmierschnittstellen (APIs) und weiterhin die Probleme, die eine Hardware-Abhängigkeit mit sich bringt.

»Mit vTee können sich Smartphones als Akzeptanzgeräte qualifizieren.«

3. Virtuelle Trusted Execution Environment (vTEE): Die neueste Lösung, um Bezahltokens und andere kryptografische Schlüssel sicher zu speichern, ist die sogenannte virtuelle Trusted Execution Environment (vTEE). Sprich, eine TEE-Plattform, die ein eigenes Betriebssystem ausführt, das auf einem vollständig emulierten Device mit vom Smartphone entkoppelter Sicherheitsarchitektur agiert.

Die virtuelle Trusted Execution Environment (vTEE) ist in Erwartung der EMVCo-Spezifikationen durch das IoT-Security Start-up Magiccube entwickelt worden. Sie funktioniert wie ein „virtueller Chip" und bietet ein Sicherheitsniveau wie Hardware, ohne selbst auf Hardware zu setzen

Im Unterschied zu den Hardware-basierten Lösungen haben App-Anbieter hier jedoch die vollständige Kontrolle über die Sicherheit (ausschließlich) ihrer Anwendung. vTEE können App-Anbieter auf jedem Endgerät selbst einsetzen und müssen dafür keine besonderen Verhandlungen, beziehungsweise vertragliche und logistische Kooperationen und Verpflichtungen mit Geräteherstellern eingehen.

Eine vTEE benötigt keine separate App, sondern sie wird beim regulären Download einer normalen App mitheruntergeladen. Innerhalb dieser Software bleibt sie inaktiv, bis ihre Dienste benötigt werden. Bei Bedarf ruft die App dann eine einfache API auf, um einen Software-Container zu starten und die erforderlichen Sicherheitsanforderungen bereitzustellen. Dieser virtuelle Chip läuft nun geschützt und kann mit oder ohne Cloud-Kommunikation arbeiten. Eine Verbindung zur Cloud muss nur während des Hochfahrens gegeben sein. Der virtuelle Chip kommuniziert über ein spezielles Protokoll mit einem Server, den Anbieter in ihrem eigenen Rechenzentrum überall auf der Welt unterbringen können. Anders als bei anderen Lösungen, liegt der „Root of Trust" im Backend, nicht in einem Chip auf dem Gerät selbst.

Im Unterschied zu Hardware-basierten Lösungen lassen sich die Software-Container in vTEE-Umgebungen im Falle einer Kompromittierung einfach deaktivieren und mit veränderten Anmeldeinformationen neu ausgeben. Das bedeutet, dass Hacker einen neuen Angriff bei Null starten müssten. Grundsätzlich kann die vTEE aus der Ferne gesteuert und jederzeit als Präventionsmaßnahme gewechselt werden – um die Angreifbarkeit beispielsweise turnusmäßig weiter zu reduzieren. Dafür muss keine App neu installiert oder ersetzt werden.

Die vTEE beim mobilen Bezahlen

Beim mobilen Bezahlen setzen viele Wallets zur Speicherung von Bezahlschlüsseln heute noch auf die angreifbare White-Box-Kryptografie. Diese Mobile Payment Wallets sind deswegen nicht unsicher, sie werden für gewöhnlich als Lösungen bezeichnet, die die Mindestsicherheitsanforderung erfüllen. In Bezug auf ihre betriebliche Nutzerfreundlichkeit sind sie jedoch wenig operational. Denn sie erfordern von den Banken und anderen Anbietern einen sehr hohen Folgeaufwand nach der Einführung, denn Bezahlschlüssel müssen aus Sicherheitsgründen regelmäßig ausgetauscht werden.

Die alternativen Hardware-basierten Lösungen sind sicher. Diese Option ist allerdings nicht auf allen Geräten verfügbar. Selbst wenn das der Fall ist, ist es nicht einfach, den Zugriff auf den Chip oder eine Steuerung aus der Ferne auszuhandeln. Beispielsweise verfügen iOS-Geräte zwar über ein Secure Element, um dies als App-Anbieter nutzen zu können, muss zunächst eine Einigung mit Apple erzielt werden.

Eine zukunftsfähige Alternative bietet das vTEE-Verfahren. Mit dem virtuellen Chip können Banken Bezahlschlüssel auf Telefone aller Hersteller speichern, ohne in langwierige Verhandlungsprozesse einsteigen zu müssen.

Technische Voraussetzungen für PIN-on-Glass geschaffen

Nach Einschätzung des US-Beratungsunternehmens Javelin Research & Strategy hat die vTEE-Technologie das Potenzial, mobile Endgeräte mit einem Sicherheitslevel zu versorgen, das mit dem Einsatz von Hardware-Chips vergleichbar ist. Das hat auch Auswirkungen auf die Zahlungsakzeptanz im Handel, da handelsübliche Smartphones sich mittels dieser Technologie als voll funktionsfähige Zahlungsakzeptanzgeräte qualifizieren können. Die Kartenlesegeräte, beziehungsweise Dongles, mit denen sie dafür verknüpft werden müssen, benötigen dadurch keine Eingabetastatur mehr, wodurch sie in der Massenproduktion erheblich günstiger werden. Die Eingabe der Geheimnummer kann dann per PIN-on-Glass erfolgen, also über das Smartphone-Display des Händlers.

mPoS-Lösungen, die mit Mobilgeräten verknüpft sind, sind in Deutschland bereits seit einigen Jahren erfolgreich im Markt etabliert. Bislang sind diese aber nur in Kombination mit einem sicheren

Kartenlesegerät zugelassen, das über ein nummerisches Eingabefeld für die PIN-Eingabe verfügt und sensible Daten und Schlüssel speichert.

Sobald diese Daten nicht mehr in zusätzlichen Kartenakzeptanz-Devices gespeichert werden müssen, sondern im gekoppelten Smartphone abgelegt werden können, ergeben sich für Einzelhändler darüber hinaus ganz neue Möglichkeiten, Zahlungen sicher anzunehmen: Perspektivisch könnten sie für die Kartenakzeptanz am PoS neben dem handelsüblichen Smartphone oder Tablet überhaupt keine zusätzliche Hardware, sprich Kartenlesegeräte, mehr benötigen. Kontaktlose Zahlungen des Käufers können technisch per NFC-Technologie vom Mobiltelefon des Verkäufers angenommen werden.

Noch keine Lösung regulatorisch zugelassen

Wenn ein solches Verfahren zukünftig Realität wird, setzt es selbstredend eine sehr hohe Abdeckung kontaktloser Karten beziehungsweise mobiler Bezahllösungen voraus, da in jenem Szenario kein Kartenschlitz mehr vorhanden ist, um die Karte zu stecken.

Noch ist keine entsprechende Lösung auf dem Markt, die regulatorisch zugelassen ist. Die Magiccube-Plattform unterstützt dieses Verfahren jedoch bereits und ist damit zukunftssicher, sobald die neuen Standards verfügbar sind.

Voraussetzung für PIN-on-Glass-Verfahren ist eine PCI-Zertifizierung. Im Januar 2018 hat die PCI eine neue Spezifikation herausgegeben, die PIN-on-Glass-Lösungen grundsätzlich möglich macht. Als teilnehmende Organisation des globalen PCI Security Standards Council, das den weltweiten elektronischen Zahlungsverkehr standardisiert, unterstützt Magiccube die Entwicklung eines sicheren Datensicherheitsprozesses im Bereich mPoS. Da das PCI-Council komplette Zahlungslösungen und nicht isoliert Sicherheitstechnologien zertifiziert, ist eine Zulassung möglich, sobald ein App-Plattform-Anbieter eine vollständige Lösung einreicht. Mit der voraussichtlichen EMVCo-Zertifizierung ist davon auszugehen, dass Lösungen mit Magiccube einen erheblich geringeren Aufwand für die Zertifizierung erfordern. ■