Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 103 (2012)
Heft: 4

Artikel: Mobile Security : sind wir bereit für die mobile Revolution?
Autor: Böttcher, Harald
DOI: https://doi.org/10.5169/seals-857288

Mobile Security – sind wir bereit für die mobile Revolution?

Mobile Geräte bieten zahlreiche neue Angriffsflächen

Glaubt man den Analysten, wird der Anteil am Datenverkehr über mobile Endgeräte ab etwa 2015 höher sein als über Desktopsysteme. Das solche Steigerungsraten nicht nur durch mobiles Surfen oder soziale Netzwerke verursacht werden, liegt auf der Hand. Es zeichnet sich ab, dass viele Geschäftsprozesse, die wir heute noch von unseren «stationären» Systemen kontrollieren, zunehmend mobil werden. Sind aber mobile Geräte sicher genug für geschäftskritische Anwendungen?

Harald Böttcher

Die Sicherheit von mobilen Anwendungen und den damit verarbeiteten Daten und Prozessen stellt eine der grössten Herausforderungen der Mobilen Revolution dar. Dies auch vor dem Hintergrund der zunehmenden Industrialisierung der Internet-Kriminalität.

Anatomie von mobilen Endgeräten

Mobile Endgeräte werden oft als kleinere Versionen ihrer PC-Vorbilder angesehen, da moderne Smartphones an die Leistungsfähigkeit der letzten PC- und Notebook-Generation heranreichen. Dabei werden fälschlicherweise oft auch Sicherheitsbetrachtungen aus der PC-Welt unverändert auf mobile Lösungen angewandt. Dieses Vorgehen ist aus zwei Gründen nicht angebracht. Einerseits sind die Betriebssysteme von Smartphones deutlich moderner und daher in ihren «Genen» bereits mit moderneren Sicherheitskonzepten ausgestattet. Andererseits aber bieten die erweiterten Kommunikationstechnologien von mobilen Geräten neue Angriffsflächen für Hacker und Schadsoftware. In diesem Kontext betrachtet werden muss natürlich auch die andersartige Nutzung im Vergleich zu den stationären Computersystemen.

Die ortsunabhängige Nutzung und damit auch die Kontrolle oder eben Unkontrollierbarkeit der Netzwerkinfrastruktur sowie die potenziell höhere Gefährdung für Datenverlust durch Spionage – zum Beispiel durch Überwachungskameras – im öffentlichen Raum oder Diebstahl sind für eine Risikoanalyse gänzlich neue Dimensionen.

Risikoanalyse und Angriffsvektoren

Die für mobile Anwendungen relevanten Risikofaktoren lassen sich wie folgt kategorisieren:

Schadsoftware (Malware)

Schadsoftware ist ein Programmcode, der zumeist in Unkenntnis des Benutzers Daten manipuliert, weiter verbreitet oder gar illegale Operationen wie beispielsweise Bank-Transaktionen ausführt. Drei Typen von Malware werden unterschieden: Viren, Trojaner und Würmer. Die Analogien zur physischen Welt sind hier nicht zufällig, liefern sie doch eine recht präzise Beschreibung über die Art und Weise, wie sich die Malware in die Systeme einschleust.

Viren beispielsweise nutzen ein Wirtsprogramm, in dem sie ihren Programmcode verstecken. Zudem können sich Viren in andere Wirtsprogramme einschleusen.

Trojaner verstecken sich ähnlich wie Viren in anderen Programmen, verfügen jedoch nicht über die Fähigkeit, sich weiter auszubreiten.

Würmer sind eigenständige Programme, die sich durch Netzwerke hindurch in ihren Zielsystemen einnisten.

Die hier genannte Kategorisierung hat auch entscheidenden Einfluss auf die anwendbaren Abwehrmassnahmen zur Erkennung bzw. Verhinderung entsprechender Malware-Attacken.

Netzwerkbasierte Angriffe

Die Zahl möglicher unterschiedlicher Netzwerkangriffe steigt wenig überraschend mit der Anzahl unterschiedlicher Netzwerktechnologien und Protokolle stark an. Zu den, auch vom PC her bekannten, auf dem Internet- bzw. Ethernet-Protokoll basierten Angriffsszenarien kommen hier zusätzliche Netzwerktechnologien wie GSM, GPRS, UMTS aber auch Bluetooth und WiFi hinzu. Auch zu berücksichtigen sind hier Standard Mo-

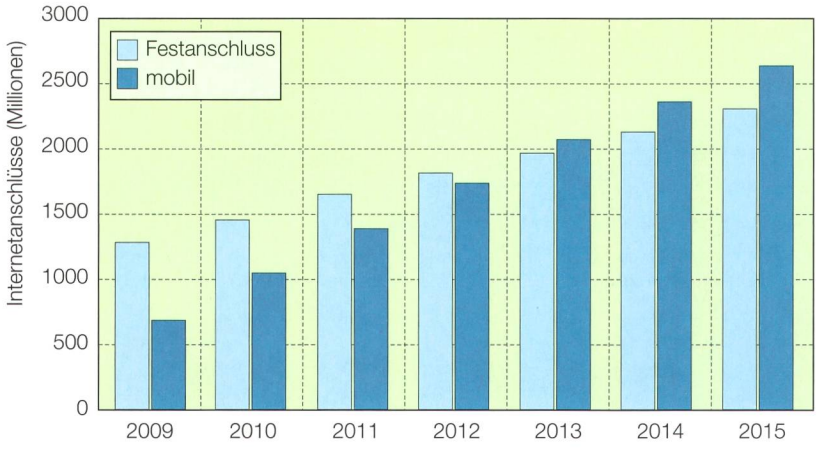

Bild 1 Entwicklung der Internet-Anschlüsse weltweit.

bile Services wie etwa SMS, MMS oder WAP. Wenig bekannt sind in diesem Zusammenhang auch die sogenannten System-SMS, die von den Mobilfunkbetreibern für Netzwerkhandshakes sowie zur Verteilung von Einstellungen der Endgeräte verwendet werden. Da die SMS-Technologie auf die Anfänge der Mobilfunktechnologie zurückgeht, ist sie sicherheitstechnisch nicht mit modernen Technologien wie etwa UMTS vergleichbar.

So vielfältig wie die zugrundeliegenden Netzwerktechnologien sind auch die Namen der bekannten Angriffsstrategien. Man spricht hier z.B. von Spoofing, Phishing, SMiShing, Pharming, Vishing etc. Eine detaillierte Beschreibung dieser Strategien würde den Rahmen dieses Artikels sprengen. Wichtig in diesem Zusammenhang ist letztlich das Ziel dieser Angriffe, nämlich sich aktiv oder passiv in den Kommunikationskanal zu hängen, um Daten mitzuhören oder gar zu manipulieren. Bedauerlicherweise greifen selbst Verschlüsselungstechnologien nur bedingt, da viele der genannten Angriffe darauf abzielen, sich vor oder nach der Verschlüsselung in den Datenstrom einzuklinken – sei dies nun auf Seite der Endgeräte (Man in the Mobile) oder auch auf Seite des Service-Anbieters.

Neben dieser eher technischen Betrachtung von Risikofaktoren gibt es aber auch die eher klassischen Risikofaktoren, die letztlich auf den Diebstahl der «Digitalen Identität» des Benutzers abzielen. Die offensichtlichsten sind sicher der permanente oder temporäre Diebstahl des mobilen Gerätes und damit auch aller auf dem Gerät befindlichen Daten. Besonders gefährlich ist hierbei der temporäre Verlust, sofern es gelingt, in der zur Verfügung stehenden Zeit unbemerkt eine Kopie der Daten anzulegen.

Schliesslich wäre dann noch das Sicherheitsrisiko Nummer 1 zu nennen: der Benutzer. Sein Verhalten beeinflusst die Gesamtrisikobilanz erheblich. Angefangen bei eher einfachen Vergehen wie der Eingabe von Passwörtern im Blickfeld von anderen Personen oder auch Überwachungskameras bis hin zum aktiven Aushebeln der in die Gerätesoftware eingebauten Schutzmechanismen durch «Jailbreaking» oder «Rooting» (Kasten).

Abwehrmassnahmen

Zur Risikominimierung ist daher ein beachtliches Portfolio an Schutzmassnahmen notwendig. Mit nachträglich installierter Virenscanner-Software und Personal Firewalls, wie wir sie von den «stationären» Systemen her kennen, können mobile Systeme nicht abgesichert werden. Ausgeklügelte Schutzmassnahmen, die in den Kern der mobilen Betriebssysteme integriert werden, bieten hier einen weitaus besseren Schutz als die «post mortem» Identifikation und Behebung von Sicherheitslöchern durch Virenscanner.

Interessanterweise verfolgen die heute am Markt relevanten mobilen Betriebssysteme weitgehend identische Sicherheitsstrategien, die sich nur in Nuancen voneinander unterscheiden. Wichtigstes Kriterium ist hierbei der Schutz vor Malware sowie restriktive Einschränkungen von Daten und Geräteressourcen für Anwendungsprogramme. Diese Strategie erweist sich auch als ausserordentlich effektiv gegen viele netzwerkbasierte Angriffe. Denn sollte es einem Angreifer tatsächlich gelingen, über einen Netzwerkangriff ins Gerät einzudringen, bleibt das Schadenspotenzial dank stark eingeschränktem Handlungsspielraum der eingeschleusten Schadsoftware sehr gering.

Die nachfolgend beschriebenen Sicherheitskonzepte finden sich bei allen wichtigen mobilen Plattformen, darunter insbesondere iOS von Apple, Geräte mit dem Android-Betriebssystem von Google, Blackberry-Geräte des ehemaligen Smartphone-Marktführers Research In Motion, sowie in den meisten der mittlerweile schon unzählbaren Variationen von Microsofts mobiler Softwaresparte. Die wichtigsten Konzepte werden im Folgenden erläutert.

Technologie	e-Banking	m-Banking (Smartphone)	m-Banking (Tablets)
OTP/SecureID	Keine TRX Signierung	Keine TRX Signierung	Keine TRX Signierung
Card Reader, Challenge/Response Klasse 3/Tastatur + Display			
Optische Geräte, Challenge/Response			
Audio, Near Field, Challenge/Response			
m-Tan, SMS-Challenge/Response			
USB-Lösungen (Smart Card + Browser)			
Software-Zertifikate, Challenge/Response			

Gut geeignet, hohe Sicherheit
Bedingt geeignet, geringere Sicherheit
Ungeeignet, unsicher

Idate Consulting & Research

Bild 2 Mobiltaugliche Transaktions-Signierung: Vergleich aktueller Two-Factor-Authentication-Lösungen (2FA).

Sandboxing

Sandboxing bedeutet, dass Applikationen in einer isolierten Umgebung – der sogenannten Sandbox – betrieben werden, aus der sie nicht unkontrolliert ausbrechen können. Welche Geräteressourcen die Applikation nutzen kann, wird dabei durch ein vorher festgelegtes Berechtigungsprotokoll festgelegt. So muss beispielweise die Bestimmung der geografischen Position des Gerätes oder der Zugriff auf Netzwerkdienste wie z.B. Roaming durch den Benutzer explizit bestätigt werden. Somit sind die Spielregeln für unseren digitalen Sandkasten gesetzt. Damit der Frieden gewahrt bleibt, bedarf es jedoch noch weiterer flankierender Massnahmen. So muss beispielsweise sichergestellt werden, dass kein Sand aus dem Kasten hinausfliesst und – besonders wichtig – dass die bösen Kinder dem Sandkasten fern bleiben.

Übersetzt auf die digitale Welt der mobilen Geräte bedeutet dies:

Hintergrund

Abwehr der Abwehrmechanismen

Es liegt in der Natur des Menschen, sich gegen zu viel Kontrolle zur Wehr zu setzen. So überrascht es auch nicht, das sich schon kurz nach Veröffentlichung des iPhones eine Community gebildet hat, welche für die von Apple auferlegten «Vorschriften» Umgehungslösungen sucht und auch gefunden hat. Für dieses Aufbrechen der Sicherheitsprotokolle hat sich inzwischen der Begriff «Jailbreaking» eingebürgert. Analoge Bestrebungen gibt es auch in der Android-Entwicklergemeinde. Hier hat sich in Anlehnung an den Unix-Superuser «root» der Begriff «rooting» eingebürgert.

Memory Protection

Hier werden, häufig unterstützt durch die Hardware bzw. CPU auf unterster Betriebssystemebene, kritische Ressourcen wie etwa der Arbeitsspeicher oder reservierte Bereiche der Netzwerk- und Bildschirmregister auf unerlaubten Zugriff hin überwacht. Damit kann sichergestellt werden, dass diese Ressourcen nur über die dafür vorgesehen Funktionen des Betriebssystems verwendet werden können und nicht über fahrlässige oder absichtliche Manipulation durch bösartige Programme. Selbstredend müssen jedoch die Betriebssystem-Operationen durch geeignete Mittel wie etwa das Berechtigungsprotokoll geschützt werden. Eben dieses Protokoll wie auch der Code selbst wird durch eine weitere Massnahme geschützt.

Applikations-Signierung

Applikationen können nur dann auf einem mobilen Gerät installiert und gestartet werden, wenn sie mit einem gültigen Zertifikat «unterschrieben» wurden. Neben der zweifelsfreien Identifizierung des Urhebers der Applikation erlaubt dieses Zertifikat unter der Zuhilfenahme von Prüfsummen auch die Erkennung von nachträglichen Modifikationen am Programmcode. Daraus ergibt sich ein wirksamer Schutz vor jeglicher Form von Malware. Die Herausgabe und Verwaltung der hierfür notwendigen Zertifikate und damit die zweifelsfreie Identifikation ihrer Inhaber obliegt dabei den Herstellern der jeweiligen mobilen Betriebssysteme. Spätestens hier werden dann jedoch signifikante Unterschiede zwischen den Plattformen erkennbar. Während Googles Android keine expliziten Vorgaben macht, über welche Kanäle Programmcode verteilt werden kann, verfolgt insbesondere Apple hier eine sehr viel restriktivere Politik. So ist die Verteilung von Programmen ausschliesslich durch den von Apple betriebenen App-Store möglich – und dies auch erst nachdem der Programmcode einer überraschend sorgfältigen Prüfung durch Apple unterzogen wurde.

Alle bisher genannten Verfahren dienen zum Schutz vor Malware. Zur Risikominimierung vor Identitätsdiebstahl bzw. Missbrauch einer digitalen Identität durch Dritte sind komplett andere Verfahren notwendig, wie zum Beispiel Passwörter zum Schutz von Daten oder Zugriff auf Applikationen und Services. Passwörter repräsentieren dabei eine von drei möglichen Identifikations- bzw. Authentisierungsverfahren, die in drei Kategorien unterteilt werden können.

- Informationen, die ausschliesslich dem Inhaber der Applikation bzw. der Daten bekannt sein können. Typischerweise handelt es sich hierbei um Passwörter oder Antworten auf zuvor vereinbarte Fragen.
- Besitz. Typischerweise ein physisches Gerät mit verifizierbaren Eigenschaften, das sich im Besitz der zu identifizierenden Person befindet. Essenziell für dieses Authentisierungsverfahren ist, dass dieser elektronische Pass nicht kopiert und damit unbewusst Dritten zugänglich gemacht werden kann.
- Eigenschaften, die eine zweifelsfreie Identifikation des Benutzers erlauben. Hierzu zählen insbesondere biometrische Verfahren wie Fingerabdruckscannen oder Stimmerkennungsverfahren.

Für sicherheitskritische Anwendungen werden üblicherweise mindestens zwei Verfahren aus unterschiedlichen Kategorien kombiniert. Man spricht hier auch gerne von starker Authentisierung bzw. 2FA (Zwei-Faktoren-Authentisierung)

2FA-Authentisierungslösungen

Starke Authentisierungslösungen werden heute vorwiegend zur Absicherung von Firmennetzwerken von aussen (Extranet) sowie im eBanking eingesetzt. Einfachere Lösungen nutzen hierfür sogenannte OTP (Einmalpasswörter) welche durch ein externes Gerät generiert werden und zusammen mit dem Benutzerkonto und dem Passwort zur zweifelsfreien Identifikation des Benutzers verwendet werden. OTP-Geräte basieren zumeist auf einer zeitgesteuerten Generierung von nicht vorhersagbaren Zahlenkombinationen. Diese Zahlen werden aus einem im Gerät hinterlegten digitalen Schlüssel und der aktu-

Kobil

Bild 3 Ein für den mobilen Kanal optimiertes 2FA-Gerät, auf BlueTooth-Technologie basierend, mit eingebautem Reader für SmartCards und SI-Kartengrösse.

ellen Zeit über eine mathematisch nicht umkehrbare Funktion errechnet. Somit kann aus einer Zahlenkombination kein Rückschluss auf den verwendeten Schlüssel gezogen werden, was ein Kopieren der Geräte praktisch verunmöglicht. Einzig dem Herausgeber des Gerätes und natürlich dem Anbieter des zu schützenden Services ist der digitale Schlüssel bekannt. Letztgenannter benötigt den Schlüssel dann auch zur Verifikation der vom Benutzer verwendeten Zahlenkombination.

OTP-Lösungen sind heute weit verbreitet, da sie einfach umzusetzen sind und die Geräte zur Generierung der OTP-Zahlenreihen kleine Formfaktoren zulassen. Allerdings repräsentieren diese Geräte nicht den letzten Stand der Sicherheitstechnologie und haben ein im Vergleich zu moderneren Challenge-Response-Verfahren ein sehr begrenztes Einsatzspektrum. Eine entscheidende Einschränkung ist, dass bei zeitbasierten OTP-Lösungen keine weiteren Daten vom Server verifiziert werden können und ihr Einsatzgebiet damit auf einfache Authentisierung eingeschränkt ist. Challenge-Response-Verfahren hingegen bestimmen die zur Verifikation errechnete Zahlenkombination (Response) aufgrund einer vom Server generierten Information (Challenge). Damit eröffnen sich völlig neue Möglichkeiten. So können beispielsweise TAN (Transaktionsnummer) oder Kontonummer des Zahlungsempfängers einer Überweisung in eine Challenge integriert werden.

Vergleich der häufigsten TAN-Lösungen

Heute gibt es ein reichhaltiges Portfolio von Lösungen, welche sich neben der physischen Umsetzung der 2FA-Geräte insbesondere durch die Übertragung der Challenge-Response-Informationen sowie durch die systembedingte Datendichte unterscheiden. Die wichtigsten Vertreter sind:

Chipkarten-Lesegeräte mit Tastatur und Bildschirm. Diese Geräte haben zumeist die Form eines Taschenrechners. Die Challenge-Information wird hier durch den Benutzer auf der Tastatur eingegeben. Das Resultat, welches durch die Logik der Chipkarte errechnet wurde, wird auf dem Display angezeigt und wiederum durch den Benutzer in die eBanking- oder Mobile-Applikation übertragen. Diese Verfahren sind sehr sicher, da der Übertragungskanal – der Benutzer – nicht unbemerkt kompromittiert werden kann. Die wichtigsten Nachteile sind: geringe Datendichte und damit «kryptische» Challenge-Daten sowie eine durch die Tastatur und das Display notwendige Grösse der Geräte.

Optische Lösungen, die das Display der eBanking-Applikationen zur Darstellung der Challenge nutzen und durch fotosensitive Geräte, erfasst und umgesetzt werden können. Zumeist sind dies relativ einfache Geräte die hell-dunkel-Sequenzen – auch bekannt als «flickering» – abtasten. Die Übertragung der Response ist wiederum manuell durch den Benutzer. Durch den Verzicht auf eine Tastatur können diese Geräte deutlich kleiner gebaut werden. Allerdings ist die Datendichte noch immer sehr begrenzt und die Zuverlässigkeit der optischen Übertragung fehleranfällig. Abhilfe könnten Geräte mit Bildverarbeitungsfähigkeiten schaffen, die z.B. 2D-Barcodes erkennen und auswerten können. Noch sind solche Geräte jedoch für den Masseneinsatz unverhältnismässig teuer.

SMS-TAN, auch bekannt als Mobile TAN (M-TAN) Lösungen, sind in den letzten Jahren sehr populär geworden, da sie keine speziellen Geräte erfordern, sondern das Mobiltelefon der Anwender nutzen. Über SMS-Nachrichten werden dabei TAN-Codes zusammen mit weiteren Information wie etwa Begünstigtenkonto oder Betrag versandt. Sind die Informationen korrekt, kann der Benutzer die Transaktion mit der TAN bestätigen. Diese auf den ersten Blick sehr elegante Lösung weist jedoch einige Schwächen auf. Neben den Kosten der SMS-Nachrichten sind dies insbesondere Sicherheitsbedenken bei der SMS-Technologie. Für mobile Anwendungen ist das M-TAN-Verfahren sogar gänzlich ungeeignet, da sowohl Transaktion wie auch Verifikation auf demselben Gerät stattfindet. Wenn die Sicherheit dieses Gerätes kompromittiert ist, entspricht dies einem sicherheitstechnischen Kurzschluss.

USB-basierte Lösungen nutzen den USB-Port zur Übertragung der Challenge-Response-Daten. Damit sind sehr hohe Datendichten realisierbar. Diese Geräte enthalten ein Interface zur Aufnahme eines Sicherheitschips in SIM-Karten sowie ein kleines Display zur Anzeige von Transaktionsdaten **(Bild 3)**. Da die Berechnung der TAN auf der Chipkarte erfolgen kann, sind diese Geräte weitgehend von der eBanking-Applikation entkoppelt und damit vergleichsweise sicher. USB-basierte Geräte können dank externer Stromversorgung und Wegfall von Fotosensoren sogar noch kleiner realisiert werden als optische TAN-Geräte. Leider scheiden USB-Lösungen für mobile Geräte aus, da die meisten Smartphones keinen USB-Port besitzen.

Die jüngsten Entwicklungen, speziell auch für Mobilgeräte, nutzen Nahfeld-Übertragungstechniken wie etwa Bluetooth anstelle von USB. Die Arbeitsweise entspricht in etwa der von USB-TAN. Auch die Einschränkungen sind vergleichbar, so gehören Bluetooth-Fähigkeiten nicht zum Standard gängiger Desktop-Computer, was den Einsatz für traditionelles eBanking erschwert.

Résumé

Sécurité mobile: sommes-nous prêts pour la révolution mobile?

Les appareils mobiles prêtent le flanc à un grand nombre de nouvelles attaques

Bien que les appareils mobiles modernes tels que les smartphones et les tablettes contiennent déjà dans leurs gènes une protection étendue contre les logiciels malveillants, cette dernière n'est en aucun cas suffisante en ce qui concerne les transactions commerciales d'une importance cruciale ou les transactions financières. Comme pour les systèmes PC, plusieurs procédés TAN supplémentaires sont nécessaires à la vérification des données des transactions. De façon plus remarquable, un grand nombre de procédés TAN que les banques suisses viennent de déployer pour leurs solutions d'e-banking ne sont pas aptes à la mobilité ou bien ils ne le sont que très partiellement dans le meilleur des cas. Il n'est donc pas surprenant de constater que la banque mobile suisse brille par l'absence généralisée de ses opérations financières. Jusqu'à présent, personne n'a trouvé de solution idoine qui conviendrait aussi bien à l'e-banking traditionnel qu'à son application mobile. Pourtant, la clientèle âprement disputée des jeunes « natifs numériques » exige, à l'heure actuelle, des services financiers mobiles et sûrs. Nous sommes curieux de savoir qui sera le premier à dénouer ce nœud gordien et à obtenir, par la même occasion, un avantage concurrentiel déterminant. No

Angaben zum Autor

Harald Böttcher, El.-Ing. HTL und Betriebsingenieur ISZ/SIB, arbeitet seit 2009 bei der Technology Innovation & Management AG. Als Principal ist er verantwortlich für den Bereich Mobile Solutions.

Technology Innovation & Management AG, 8048 Zürich
harald.boettcher@ti8m.ch