

Handy anstatt Hardware Token

Moderne Smartphones eignen sich ideal als Lösung für die Zwei-Faktoren-Authentifizierung und bieten gegenüber herkömmlichen Security-Token mehrere Vorteile.

VON HARALD BÖTTCHER

Glaubt man den Analysten von Forrester oder Gartner, so wird das angebrochene Jahrzehnt das Jahrzehnt des Mobile Computing. Es werden Wachstumsraten im zweistelligen Prozentbereich prognostiziert. Gartner geht gar davon aus, dass die Anzahl mobiler Web Devices im Jahre 2013 die der konventionellen PCs übersteigt. Smartphones, welche Mobiltelefone um klassische Handheld- oder PDA-Funktionen ergänzen, sind schon seit längerer Zeit auf dem Markt. Jedoch fehlte es bis anhin an sinnvollen Applikationen, welche das Potential dieser Geräte ausschöpfen. Insbesondere Lösungen, welche das Mobilfunknetz nutzen konnten, waren selten und schlecht akzeptiert. Dies hat sich seit der Lancierung des iPhone und Apples App Store grundlegend geändert. Viele Netzwerkanbieter haben gleichzeitig mit dem Verkauf des iPhone angefangen, kostengünstige Datenservices anzubieten. Zusammen mit den hochauflösenden Displays und der gestiegenen Rechenleistung aktueller Geräte bieten aktuelle Plattformen nun die Grundvoraussetzungen, um auch anspruchsvollere Services nutzbar zu machen.

Die 2F-Authentisierung

Aber sind diese Plattformen auch geeignet, um sicherheitsrelevante Applikationen zu realisieren? Oder kämpfen sie mit denselben Problemen wie Viren, Trojanern etc., die man

vom Desktop her bedauerlicherweise nur zu gut kennt? Lassen sich mit Smartphones eventuell sogar Hardware-Token-basierte Zwei-Faktoren-Authentisierungslösungen (2F-Authentisierung) ersetzen?

Nach wie vor eine der grössten sicherheitstechnischen Herausforderungen ist die zweifelsfreie Authentisierung des User. In ihrer einfachsten Form geschieht die Authentisierung in Form eines User-Login mit mehr oder weniger komplexen Passwörtern. Für kritische Anwendungen wie etwa E-Banking reicht dies aber nicht. Hier braucht es weitreichendere Massnahmen, welche zusätzliche Faktoren beziehungsweise Benutzerattribute überprüfen. Solche Zwei- oder Mehrfaktoren-Authentisierungen basieren auf einer Kombination der folgenden Informationen:

- **Wissen:** PIN-Nummern, Passwörter oder Geburtsdaten etc.
- **Besitz:** Normalerweise ein Schlüssel oder ein Gerät, das nicht kopiert werden kann.
- **Persönliches Merkmal:** Typischerweise biometrische Authentisierung wie Fingerabdrücke, Stimmerkennung usw.

Bis anhin wurden für die 2F-Authentisierung oft spezialisierte Geräte mit LC-Display oder gar Smart-Card-Lesegeräte eingesetzt. Diese können auf Uhrzeitbasis oder nach Eingabe eines Challenge Codes einmalig Passwörter zur Authentisierung generieren. Die Verwaltung, Administration und nicht zuletzt die physische Verteilung dieser Geräte verursacht jedoch erhebliche Kosten.

Smartphones hingegen sind in Unternehmen heute bei vielen

Mitarbeitern ein ständiger Begleiter. Was liegt also näher als Smartcard und Co. durch ein Smartphone zu ersetzen?

Ernstzunehmende Alternative

Die verwendeten Algorithmen in Smartcards basieren auf der Errechnung eines HASH-Code, welcher sich aus einem privaten Schlüssel (auf dem Gerät gespeichert) und der Uhrzeit oder dem Challenge Code zusammensetzt. Selbst einfachste Handys verfügen über die notwendige Leistung für solche Berechnungen und bringen ein Display und eine Tastatur mit. Der einmalige Schlüssel, der zur zweifelsfreien Identifikation des individuellen Gerätes notwendig ist, wird bei der Aktivierung der Software generiert und mit dem entsprechenden Server ausgetauscht. Der Schlüssel selbst wird daraufhin wiederum verschlüsselt und zum Beispiel durch einen PIN-Code geschützt auf dem Smartphone abgelegt. Hier ist es von entscheidender Bedeutung, dass sowohl PIN-Code als auch der generierte Schlüssel nicht über das Netzwerk ausspioniert oder gar kopiert werden können. Sicherergestellt wird dies durch Smartphone-Betriebssysteme, die für jede Applikation eine eigene Umgebung (Sandbox), sowohl zur Laufzeit als auch zur Datenspeicherung, bereitstellt. Durchaus relevant in Bezug auf die Sicherheit ist die Tatsache, dass der Verlust des Mobiltelefons den meisten Anwendern deutlich früher auffallen dürfte als der Verlust eines Security Token. Dies gilt ganz besonders, wenn Services nur gelegentlich genutzt werden, etwa zum Zahlungsverkehr am Ende des Monats.

Smartphones sind somit durchaus eine ernstzunehmende Alternative zu bestehenden Security-Token-Lösungen. Dabei ist bei heutigen Lösungen noch nicht einmal das volle Potential ausgeschöpft. GPS-Informationen des Geräts könnten beispielsweise mit Netzwerkinformationen vom Mobileprovider verglichen werden, um eine «Anwesenheitsprüfung» vorzunehmen oder um sicherzustellen, dass rechtlich geschützte Daten nicht über Landesgrenzen hinweg verteilt werden können. Andere Möglichkeiten wären Unterschriftserkennung für Geräte mit Touchscreen, Stimmerkennung über das vorhandene Mikrofon oder gar die visuelle Authentisierung über eingebaute Kameras. Auch aus wirtschaftlicher Sicht haben Mobile Security Token eine rosige Zukunft. Die potentiellen Einsparungen durch den Wegfall von Beschaffung, Verwaltung und Verteilung traditioneller Security Token sind enorm.

HARALD BÖTTCHER IST ASSOCIATE PRINCIPAL BEI DER BSGROUP TECHNOLOGY INNOVATION.

VERFÜGBARE PRODUKTE UND LÖSUNGEN

ARADIOM	www.aradiom.com
FIREID	www.fireid.com
FIVEBARGATE	www.fivebargate.net
MOBILE-OTP	http://motp.sourceforge.net
DIVERSINET MOBISecure SOFTOKEN	www.diversinet.com
VERISIGN IDENTITY PROTECTION	www.verisign.com