Transfer

Sichere Authentisierung mit Handys?

Roland Portmann, Leiter Kompetenzzentrum Informations- und Softwaresicherheit, HTA Luzern, roland.portman@hta.fhz.ch

Die moderne Informationsgesellschaft verwaltet eine unüberschaubar grosse Informationsmenge. Viele dieser Informationen sind nicht öffentlich, d.h. der Zugriff darauf muss auf eine definierte Personengruppe eingeschränkt werden. Dies erfordert, dass sich diese Personen gegenüber den verarbeitenden Informationssystemen eindeutig authentisieren müssen. Dies geschieht heute vielfach noch mit einem Benutzernamen und einem Passwort, einem nun fast 50 Jahre alten Verfahren.

Die Authentisierung mit Passwort funktioniert nicht

Den Zugriff auf Informationen an das Wissen eines Geheimnisses (Passwort) zu binden ist ein uraltes Verfahren. Schon Cäsar versuchte mit einem einfachen Chiffrierverfahren geheime Informationen zu schützen. Den Zugriff auf IT-Systeme an ein Geheimnis zu binden war daher naheliegend. In der Praxis funktioniert dieses Verfahren jedoch nicht:

- Auch die besten Awareness-Kampagnen können nicht verhindern, dass Mitarbeiter nicht korrekt mit den Passwörtern umgehen. Man schreibt die Passwörter auf (man ist vergesslich), man gibt sein Passwort seinem Arbeitskollegen (man muss ja effizient sein), man wählt zu einfache Passwörter (man muss sich das Passwort ja merken können). Die Gefahr für ein solches Fehlverhalten steigt mit der Anzahl der Passwörter, die ein Benutzer kennen muss.
- Der Gewinn an Sicherheit durch regelmässig zu ändernde Passwörter ist nicht garantiert. Damit steigt die Gefahr, dass die Passwörter aufgeschrieben werden. Viele Authentisierungs-Systeme erlauben zudem sehr ähnliche Passwörter (z.B. eine inkrementierte Zahl im Passwort) zu verwenden.
- Die Passworteingabe kann auf vielfältigste Art ausspioniert werden, sei es innerhalb des IT-Systems (Keylogger, Netzwerk-Analyse, Trojaner) oder durch Zuschauen bei der Eingabe. Dieses Zuschauen wird üblicherweise mit Videokameras unterstützt. Bei den Phishing-Attacken leitet man den Benutzer mit irgendwelchen Tricks auf falsche Server und kommt so zu den Passwörtern.
- Wenn die obigen Methoden nicht funktionieren, fragt man den Benutzer einfach nach dem Passwort. Erfahrungen in Penetrationtests zeigen, dass man durch geschicktes Fragen in den meisten Fällen zu den gewünschten Passwörtern kommt.

Die obigen Angriffsmethoden sind allgemein bekannt. Trotzdem hoffen viele Verantwortliche, die Problematik mit einer Schulung der Mitarbeiter lösen zu können. Praxiserfahrungen zeigen, dass in vielen Projekten mit dem implementierten Passwortschutz keine ausreichende Sicherheit erreicht wird.

Authentisierung mit Besitz

Zunehmend wird heute in grösseren IT-Umgebungen die Authentisierung an den Besitz eines Gegenstandes gebunden. Dieser Gegenstand, meistens in der Form einer Smartcard, speichert ein für die Authentisierung notwendiges Geheimnis in nicht auslesbarer Form und stellt mittels kryptologischen Methoden eine sichere Authentisierung sicher. Die Smartcard ist meistens noch mit einem PIN geschützt, so dass der Verlust der Smartcard nicht zu einem Sicherheitsrisiko wird. In vielen Projekten werden im innerbetrieblichen Umfeld Multifunktions-Smartcards eingesetzt. Neben der Authentisierung in der IT-Umgebung werden diese Smartcards beispielsweise auch für den Zutrittschutz eingesetzt und können als Zahlungsmittel im Betriebsrestaurant verwendet werden. Diese Mehrfachverwendung vermindert das Risiko, dass eine Smartcard ausgeliehen oder unbeaufsichtigt am Arbeitsplatz liegengelassen wird. Insbesondere die Verwendung der Smartcard als Zahlungsmittel innerhalb des Betriebes wird zu einem vorsichtigeren Umgang mit der Smartcard führen, da auf der Smartcard eigenes Geld gespeichert ist.

Die Verwendung von Smartcards für die Authentisierung erfordert in der Regel, dass Zertifikate erstellt werden müssen, d.h. dass eine Public Key Infrastructure (PKI) aufgebaut

werden muss. Negative Berichte über Probleme in grösseren PKI-Projekten lassen Bedenken aufkommen. Erfahrungen zeigen, dass mit dem in Microsoft-Active-Directory-Umgebungen mitgelieferten Zertifikatsdienst Zertifikate für die Authentisierung ohne grossen betrieblichen Aufwand erzeugt werden können. Werden Zertifikate ausschliesslich für die innerbetriebliche Authentisierung verwendet, bleibt auch der betriebliche Aufwand klein. Deshalb ist eine Smartcard-basierte Authentisierung durchaus auch im KMU Umfeld realisierbar.

Das Handy als Smartcard

Für eine Smartcard-basierte Authentisierung muss der Rechner mit einem Smartcard-Leser ausgerüstet werden. Dies ist bei fest installierten Arbeitsplätzen kein Problem, vielfach aber bei mobilen Rechnern, da diese keinen Kartenleser besitzen. Ein möglicher Lösungsansatz ist, dass man Smartphones bzw. Handys für Authentisierungszwecke einsetzt. Ein solcher Einsatz ist durchaus möglich und hätte einige Vorteile:

- Die in Handys eingesetzte SIM-Karte unterstützt alle kryptologischen Operationen einer Smartcard. Damit lassen sich Smartcard-basierte Authentisierungsmechanismen implementieren.
- Jedes moderne Handy kann über Bluetooth oder anderen Technologien mit einem Laptop-Rechner kommunizieren und unterstützt zusätzlich eine Kommunikation über GSM-Verbindungen. Damit stehen für eine sichere Authentisierung zwei unabhängige Kommunikationskanäle zur Verfügung. Dies erlaubt eine sichere Authentisierung auch dann, wenn ein Kommunikationskanal kompromittiert ist.
- Ein Handy besitzt eine eigene Tastatur. Auch damit könnten allfällige Bedrohungen durch auf Rechnern installierten Keylogger und Trojaner gemindert werden. Allerdings sind durchaus auch Keylogger für Handys vorstellbar.
- Jedermann hat ein Handy, ein Handy ist persönlich und wird nicht ausgeliehen. Viele Leute haben fast eine emotionale Beziehung zu ihrem Handy.

Damit erscheint das Handy als ein geradezu ideales Gerät für eine Authentisierung zu sein.

NFC als Enabler Technologie?

Gegenwärtig ist der Setup von Kommunikationsverbindungen zwischen Handy und Laptop-Rechner noch recht mühsam. Die im Augenblick in der Entwicklung stehende Technologie «Near field communication» (NFC) könnte dieses Problem lösen. Diese Technologie baut auf der RFID-Technologie auf und erlaubt eine Kommunikation zwischen zwei Geräten ohne einen Setup. Das Handy muss nur in die Nähe des Laptop gebracht werden. Es sind die ersten Handys mit einer NFC-Schnittstelle auf dem Markt erhältlich. Vermutlich werden auch bald Laptops erhältlich sein, die diese Technologie direkt eingebaut haben. Dies könnte zu einem Durchbruch für die Authentisierung mit einem Handy führen.

NFC kompatible Handys könnten durchaus auch als Authentisierungsgeräte für weitere Anwendungen eingesetzt werden:

- Authentisierungen im e-Banking.
- Dynamischer Zutrittschutz in Gebäude: Nach einer erfolgreichen Authentisierung und Autorisierung könnte ein nur einmal gültiges Zutrittstoken über eine GSM-Verbindung oder ein SMS auf das Handy geladen werden. Dieses Zutrittstoken könnte von einem normalen RFID-Leser erkannt und verarbeitet werden.
- Authentisierungen beim bargeldlosen Einkaufen.

Das Handy hat unser Leben schon stark verändert. Es ist durchaus auch möglich, dass man Handys in Zukunft nicht nur für das Telefonieren, als Agenda und als Spielzeug verwendet, sondern auch als Gerät, mit dem sicherheitsrelevante Vorgänge gesichert werden können. Die technischen Voraussetzungen dazu sind weitgehend vorhanden.

An der Fachhochschule Luzern wurden verschiedene Forschungsprojekte initiiert, die den Einsatz von Handys für die Authentisierung und andere Sicherheitsapplikationen untersucht. So wurde beispielsweise im Rahmen eines Industrieprojektes gezeigt, dass die SIM-Karte in einem Handy die gleichen Funktionen wie eine Smartcard übernehmen kann. ■

FACHHOCHSCHULE ZENTRALSCHWEIZ
HTA
HOCHSCHULE FÜR TECHNIK+ARCHITEKTUR LUZERN

Fussnoten

1 Anstelle einer Smartkarte können auch andere Devices wie beispielsweise spezielle USB-Sticks verwendet werden.
2 Meistens in der Form eines privaten Schlüssels.