

Authentisierung in Unternehmensnetzen

Problemstellung und Lösungsansätze

>>>

Authentisierung - Agenda -



Inhalt

- Problemstellung
- Was ist starke Authentisierung
- Biometrie
- Was sind Token?
 - > **X.509-Zertifikate**
 - > **Single Sign On**
 - > **Einmalpassworte (OTP)**
- Fragen

Authentisierung - Problemstellung -



Die aktuelle Entwicklung zeigt:

- Der Diebstahl von Identitäten ist inzwischen ein Markt für die organisierte Kriminalität. Es gibt regerechte Preislisten:

Goods and services	Percentage	Range of prices
Bank accounts	22%	\$10-\$1000
Credit cards	13%	\$0.40-\$20
Full identities	9%	\$1-\$15
eBay accounts	7%	\$1-\$8
Scams	7%	\$2.5/week - \$50/week for hosting. \$25 for design
Mailers	6%	\$1-\$10
Email addresses	5%	\$0.83/MB-\$10/MB
Email passwords	5%	\$4-\$30
Drop (request or offer)	5%	10%-50% of total drop amount
Proxies	5%	\$1.50-\$30

Quelle: Symantec's Global Internet Security Threat Report
(Juli – Dezember 2007)

Authentisierung - Problemstellung -



Dazu haben wir jede Menge „alter“ Probleme

- Passwörter werden aufgeschrieben, die Zettel liegen unter Tastaturen oder kleben am Monitor.
- Passwörter „wandern“, sie werden an Kollegen oder Dienstleister weitergegeben.
- Angreifer können per „social engineering“ von Angreifern in der Regel leicht ergaunert werden.
- Eine Verbesserung an einer Stelle (z.B. schwerere Passwörter) hat Verschlechterungen an einer anderen (z.B. mehr aufgeschrieben Passwörter) zur Folge.

Passwörter alleine bieten keinen grossen Schutz!

Authentisierung - Starke Authentisierung -



Starke Authentisierung ist, wenn mindestens zwei der folgenden drei Methoden benutzt werden:

- Es wird etwas abgefragt, was ich weiß
(z.B. ein Passwort)
- Es wird etwas abgefragt, was ich bin
(z.B. ein Fingerabdruck)
- Es wird etwas abgefragt, was ich habe
(z.B. ein spezielle Karte oder ein Schlüssel)

Token bieten eine starke Authentisierung, da etwas abgefragt wird, was ich habe (das Token) und was ich weiß (PIN des Token).

Authentisierung - Starke Authentisierung -

Wie macht man es besser nicht:



Theoretische bietet die EC-Karte eine starke Authentisierung (ich brauche Karte und PIN), aber

- Teile der Karteninformation können kopiert werden
- Ausländische Geldautomaten können die Echtheit der Karte nicht prüfen

Authentisierung - Biometrie -



Gilt vielen als der „heilige Gral“ der Authentisierung. Zeigt aber in der Praxis erhebliche Probleme:

- Missbrauch möglich:

news 29.03.2008 14:10

CCC publiziert die Fingerabdrücke von Wolfgang Schäuble

- Überlisten möglich, wenn nicht überwacht
- Teuer und aufwändig
- Datenschutzrechtlich problematisch für Firmen

Biometrische Verfahren (DNA-Test) können sehr sicher sein, eignen sich aber noch nicht für automatisierte Verfahren!

Authentisierung

- Was sind Token -



Was macht ein Token eigentlich?

- Es stellt einen sicheren Speicher dar, auf den ausschließlich über spezielle Token-Applikationen zugegriffen werden kann
 - > **Beispiel Zertifikate: Diese können eine Token-Applikation nur geschrieben aber nie gelesen werden. Über die Applikation kann aber ein Zertifikat für eine Unterschrift genutzt werden**
- Diese Token-Applikationen bestehen aus einer Software auf dem PC, die über spezielle Schnittstellen Sub-Routinen auf dem Token laufen lassen kann.
- Vor dem Nutzen der Token-Applikation muss sich der Benutzer mittels einer PIN gegenüber dem Token legitimieren.

Authentisierung - Was sind Token -

Es gibt das Token in verschiedenen Bauformen:



Authentisierung - Was sind Token -



Typische Anwendungen sind:

- Speicher für X.509-Zertifikate für die Authentisierung
- Speicher für Passworte anderer Anwendungen und für Web-Sites oder die Anmeldung am Betriebssystem
- Erzeugung von Einmal-Passworten

Authentisierung - X.509 -



X.509-Zertifikate

- Häufigste Anwendung von Aladdin eToken ist die Speicherung von X.509-Zertifikaten im Token.
- Wenn das Zertifikat im Token ist, kann es zwar genutzt werden, in keinem Fall ist es möglich das Zertifikat zu kopieren.

WICHTIG: Wird das Zertifikat nur im Token gespeichert und das Token geht kaputt oder verloren, so ist das Zertifikat endgültig weg.

Authentisierung - X.509 -



Nutzung von X.509-Zertifikaten

- Anmeldung an Web-basierten Anwendungen (z.B. Connectra, Web-Server)
- Anmeldung am VPN (z.B. Cisco, Check Point, SSH)
- Verschlüsselung von Daten (z.B. Festplatte, EMail)
- Signierung von Daten (z.B. EMail, Code)
- Es gibt hier noch wesentlich mehr Anwendungen....
Schnittstelle ist PKCS#11

Authentisierung - Single Sign On -



Was ist „Single Sign On“ (SSO)?

- Der Anwender muss sich nicht mehr verschiedene Passwörter merken. Er meldet sich nur am Token an (mit der PIN) und dieses erledigt die Anmeldung an den anderen Anwendungen.
- Beispiel: Das funktioniert in etwa wie beim Browser, der sich Passwörter merkt (es gibt Plugins, die die Browser-Passwörter auf dem Token speichern).
- Ist nur verfügbar auf Windows-Betriebssystemen.

Token-Management - Single Sign On -



Wie funktioniert „Single Sign On“?

- Die Software (getrennt zu installieren) erkennt bestimmte Anmelde-Fenster und trägt dort die auf dem Token hinterlegten „Credentials“ des Benutzers ein. Das geht z.T. so schnell, das der Benutzer das Anmelde-Fenster gar nicht sieht.
- Der Benutzer kann das „Single Sign On“ selber trainieren („wenn das Fenster aufgeht, trage das ein“) oder die Informationen können zentral gepflegt werden („wenn das Fenster aufgeht, trage das Standard-Passwort des Benutzers ein“).

Authentisierung - OTP -



Was ist OTP und wie funktioniert es?

- OTP steht für „One Time Password“ (Einmalpasswort). Es geht um Passworte, die nur ein einziges Mal genutzt werden können.
- Diese Passworte werden in Abhängigkeit von der Uhrzeit (RSA-Tokens) oder einem internen Zähler (Aladdin) erzeugt.
- Diese Methode der Anmeldung kann in jeder Applikation genutzt werden die RADIUS versteht oder die den Token-Hersteller explizit unterstützt.
- Dies ist für Geräte ohne USB-Schnittstelle (z.B. Handys) oder wo keine Software installiert werden kann (z.B. Internet-Cafe).

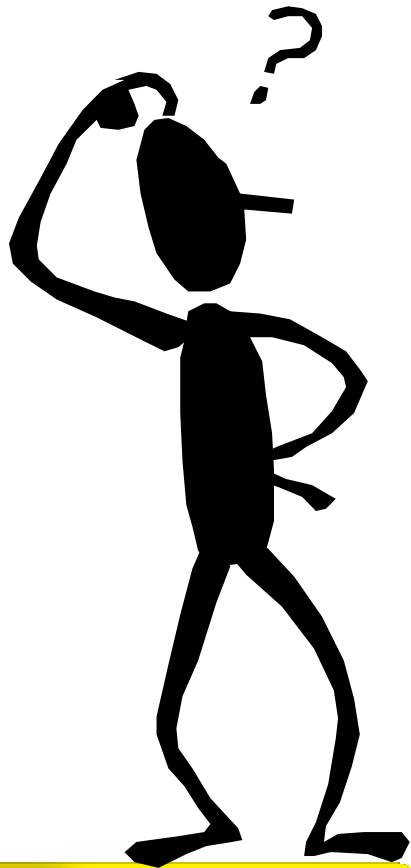
Authentisierung - Weitere Anwendungen -



Es gibt diverse Anbieter, die Token unterstützen. Dazu gehören z.B. Citrix, Cisco, SAP, Adobe.

- Wichtig ist: Stets vorher prüfen, was von dem Anbieter mit welchem Token unterstützt wird. Gerade das Thema ThinClient/Citrix ist da sehr komplex.
- Kann einen erheblichen Mehrwert der Lösung für den Kunden darstellen, führt aber zu erheblichem Klärungsbedarf im Vorfeld.

Authentisierung - Q&A -



Q&A