Authentifizierung

Universitatea “Transilvania” din Brasov

Agenda

- Wissen und Besitz
- Challenge-Response-Verfahren
- Kerberos
- Chipkarte und Biometrie
- Public-Key Infrastrukturen und Signaturgesetz
- Singl Sign-On

Umgang mit Passwörtern

- Zahlreiche Passwörter

→ schwierig zu merken

→ leichte Passwörter werden gewählt

- Zwang zu komplexen Passwörtern

→ Werden aufgeschrieben und an den Monitor geheftet

Passwörter sind ein Sicherheitsrisiko !

Passwortprobleme

- Mitlesen übers Netz möglich
- Knacken
- Passwortfallen
- Social Engineering
- Hohe Supportkosten
- 40% aller Anfragen bei Help Desk beziehen sich auf vergessene Passwörter
- Administrationsaufwand
- Verteilung / Entzug von Berechtigungen (über ganze Firma)
- Autorisierungen durch verschiedene Stellen welche nicht die gleichen Policies unterhalten

Vorteile von SSO aus Anwendersicht

- Vereinfachte Authentisierung:

→ Nur noch ein Passwort zu merken

→ Passwort kann ausreichend sicher gewählt werden

→ Speicherung auf Hardware-Token möglich

Effizientes Arbeiten:

→ Alle erlaubten Ressourcen stehen automatisch zur Verfügung

→ Einfache Interoperabilität zwischen den einzelnen Anwendungen möglich

- Zertifikatsmanagement

→ Automatische Schlüssel- und Zertifikatserneuerung

Vorraussetzungen

- Zentrales Benutzerverzeichnis

→ User- Informationen

→ Passwörter, Zertifikate

→ Rechte, Privilegien und Rollenprofile

- Public Key Infrastruktur

→ Authentisierung über Zertifikate

→ SSL-Verbindung zwischen allen Komponenten

→ Privilegien mit Zertifikaten verknüpfbar (Attribut Zertifikate)

Aufgaben von SSO-Systemen

- **Authentisierung**

→ **Einmalige Authentisierung des Nutzers**

→ **Mapping der Authentisierungsinformationen auf User-Accounts (Account-Management)**

- **Autorisierung:**

→ **Auslesen von Privilegien und Berechtigungsinformationen aus Verzeichnis**

→ **Weiterleiten der Informationen zu Ressourcen**

- **Session-Management:**

→ **Generierung von Session-Tickets**

→ **Zuordnung der User zu Sessions**

Vorteile von SSO aus Administratorsicht

- Reduzierung des administrativen Aufwandes:

→ Benutzerverwaltung geschieht einmalig und zentral

→ Weniger Supportanfragen wegen vergessener Passwörter

- Erhöhung der Sicherheit

→ kryptongraphisch starke Passwörter für Netzwerk-Ressourcen

→ Sperrung von Nutzern an zentraler Stelle hat Auswirkung auf alle Systeme

→ Verschlüsselte Verbindungen zu allen Ressourcen

Anpassung auf Client-Seite

- Einheitliche Applikations-Schnittstelle für Authentisierung
- SSO- Client-Software für Kommunikation mit Authentisierungs- und Autorisierungsserver
- Zugriff auf Authentisierungsdatenbank zur Änderung und Synchronisation von Benutzerinformationen

Anpassungen auf Server-Seite

- Gemeinsame Programm-Schnittstelle aller Applikationen für Authentisierung
- Schnittstelle zum Autorisierungs- und Authentisierungsserver für die Validierung der Benutzerinformationen
- Gemeinsame Schnittstelle zum Auslesen von Privilegien und Rechten (einheitliches Rollenkonzept)

Lösungsansätze

Zentralisiert, komplex, vollständig:

→ Einheitliche APIs und SPIs aller Anwendungen und Ressourcen

- **→ Zentrales Sessionmanagement**
- **Durch Verwendung offener Standards auch plattformübergreifend in heterogenen Systemen**
- **Aufgesetzt, angepasst, proprietär**

→ S S O nur auf Anwendungsebene

- **→ Bedingt einheitliche APIs (nachträglich angepasst)**
- **→ Proprietäre Schnittstellen**

Zentralisierte Systeme

- Integration in Betriebssystem
- Anmeldung bei zentralem Autorisierungsserver
- Verwaltung der gesamten Session über
- Autorisierungsserver und Session-Tickets
- Interaktion zwischen Ressourcen und Autorisierungsserver
- Verwendung von Zertifikaten
- Dominanz (Abhängigkeit) von einem Betriebssystem
- Anwendungen müssen einheitliche Protokolle unterstützen (z.B. Kerberos)
- Bsp.: Windows 2000

Aufgesetzte Systeme

- Nicht in die Betriebssystemarchitektur integriert, sondern als Anwendung aufgesetzt
- Nachträgliche Anpassung von Client- und Serveranwendungen notwendig
- Proprietäre Schnittstellen und Protokolle
- Zentraler Passwort- Store
- Snap-In von Authentisierungsinformationen (Window-Watching)
- Auf eigene Produktpalette gestützt (PKI, Verzeichnis)
- Meist nur für MS- Plattformen verfügbar
- Bsp.: Novell SSO, IBM Tivoli GlobalSignOn, Entrust SSO

Ist SSO die Lösung ?

- Einsatz in heterogenen Systemen mit hohem Aufwand verbunden
- Nicht alle Plattformen werden unterstützt
- Anpassung der Implementation von nicht „SSO konformen“ Anwendungen (Source notwendig)
- Noch keine Standards vorhanden
- Zertifikatseinsatz bedingt vollständige Integration einer PKI
- Ungesicherte Arbeitsstation ist ein großes Risiko

Ausblick

- Bedarf an SSO-Lösungen wird weiter zunehmen
- Integration von S S O in grosse (gewachsene) Umgebungen ist mit hohem Aufwand verbunden = hohe Kosten
- Einheitliche Applikations-Schnittstelle fehlt oder wird nicht durchweg unterstützt (GSS-API)
- Inkompatible Systeme verhindern Standardisierung
- SSO muss professionell gelöst werden (Komplex)
- Keine Out-of- the-Box Lösung .