Gerald Steilen, GBV Verbundzentrale

GBV Shibboleth Informationsveranstaltung

Möglicherweise sind Sie bereits mit Shibboleth vertraut oder haben schon einmal davon gehört. Wenn Sie sich für Shibboleth interessieren und noch grundlegende Information zu diesem Thema wünschen, dann laden wir Sie herzlich zu einer Informationsveranstaltung der VZG nach Göttingen ein. Die Veranstaltung wird keine technische Ausrichtung haben.

Ort: Göttingen
Datum: 13. Februar 2007
Uhrzeit: 11:15h - 16:00h

Fragen und Ihre Anmeldung richten Sie bitte an steilen@gbv.de.

Ausgangslage

Sicherlich ist Ihnen die Situation vertraut: Ihre Institution möchte zu schützende Angebote, wie lizenzierte Datenbanken, interne Informationen usw. bereitstellen. Nun sollen Nutzer allerdings möglichst leicht auf diese Ressourcen zugreifen können.

Meist kommt dann eine IP-Kontrolle zum Einsatz, d.h. es wird überprüft, von welchem Computer aus der Nutzer Angebote aufrufen möchte. Ist die IP in eine Positivliste eingetragen, wird der Zugriff erlaubt. Bei dieser Methode wird nicht überprüft, wer Nutzer ist, sondern nur woher er kommt. Somit hat man gleich eine Reihe von Problemen, die nicht ohne weiteres zu lösen sind. Die IP des anfragenden Rechners lässt sich beispielsweise mit relativ wenig Aufwand mit den richtigen Werkzeugen ohne Spezialkenntnisse fälschen. Das mag viele noch nicht überzeugen, obwohl dem sicherlich kein Systemadministrator widersprechen würde. Dann mag viel schwerer ins Gewicht fallen, dass eigentlich berechtigte Nutzer nicht unabhängig vom geographischen Ort ihres Internetzuganges die Ressourcen nutzen können. Recherchen in Datenbanken mit IP-Kontrolle sind vom heimischen Schreibtisch aus i.d.R. nicht möglich bzw. für bestimmte Dienste müssen bestimmte PCs genutzt werden. Andererseits ist der Wartungsaufwand für große Netzwerke erheblich. Jedem fallen hier sicherlich noch mehrere Probleme ein, die man selbst schon mal als ärgerlich empfunden hat.

Nächste Möglichkeit: Es werden für die zugangsbeschränkten Ressourcen Benutzername-Passwort-Kombinationen vergeben. So kann man von jedem Internetzugang aus diese Angebote nutzen. Dass diese Accountdaten weitergegeben werden können, mag hier ebenfalls noch nicht einmal als größerer Nachteil angesehen werden. Aber sicherlich wird kaum jemand darüber erfreut sein, zusätzlich zu EC-Kartengeheimnummer, Handy-PIN oder des Onlinebanking-Passwortes noch von seiner Bibliothek, dem Forschungsinstitut oder von einem CIP-Pool-Verwalter mit einer Reihe von geheimen Zugangsdaten beglückt zu werden.

Single Sign-On

Okay, Problem erkannt, Gefahr gebannt? Eine Single Sign-On (SSO) Lösung muss her! Ein

Nutzer soll nach einer einmaligen Authentifizierung („Wer bin ich?“) auf alle Ressourcen zugreifen können, für die er eine Berechtigung besitzt. Technisch wäre es denkbar Benutzerdatenbanken zu synchronisieren oder eine zentrale Benutzerdatenbank aufzubauen. Während ersteres Systemadministratoren wegen unnötiger Redundanz gerne vermeiden und es auch technisch schwierig ist, zeitnah Änderungen in den Benutzerdaten von einem System auf alle anderen zu verteilen, ist letzteres aus datenschutzrechtlichen Gründen nicht erstrebenswert oder gar unmöglich.

Shibboleth

Genau hier setzt Shibboleth an: Von der Grundidee geht Shibboleth davon aus, dass ein Nutzer immer einer Heimateinrichtung angehört, d.h. eine Institution seine Benutzerdaten verwaltet. Das kann eine Bibliothek, ein Uni-Rechenzentrum oder das Studentensekretariat sein. Daher ist es völlig ausreichend, wenn diese Heimateinrichtung die Benutzerdaten exklusiv pflegt (= Identity Prover). Weiter wird davon ausgegangen, dass die Heimateinrichtung vertrauenswürdig ist und man sich sozusagen „auf ihr Wort verlassen kann“. Das bedeutet: Möchte ein Benutzer eine geschützte Internetressource verwenden, beispielsweise eine Datenbank einer Bibliothek oder eines Verlages, so wird der Benutzer gefragt: „Wo kommst Du her?“ (**W**here **a**re **y**ou **f**rom? = WAYF). Nachdem der Benutzer das einem speziellen Server (WAYF-Server) mitgeteilt hat, wird er ggf. von seiner Heimateinrichtung gebeten sich mit einem Login zu authentifizieren. Somit kann der Anbieter der Ressource (Service Provider) bei der Heimateinrichtung nachfragen „Kennst Du den?“. Wenn das bejaht wurde, wird der Service Provider anhand von Nutzermerkmalen (Attributen) den Zugriff auf die gewünschte Ressource gewähren (autorisieren) oder verweigern. Gelangt der Nutzer anschließend zu Angeboten eines anderen Service Providers muss der Benutzer sich nicht mehr authentifizieren, weil die Kommunikation zwischen dem Identity Provider und dem Service Provider nun im Hintergrund ablaufen kann.

Föderation

Was hier technisch stark vereinfacht geschildert wurde, setzt letztlich ein regelbasiertes Vertrauensmodell zwischen Identity Provider und Service Provider voraus, um sich auf Zusagen des jeweils anderen verlassen zu können. Alle notwendigen Regeln, die Überwachung der Regeln und Sanktionen bei Verstößen werden in einer Föderation vertraglich festgelegt. Alle Beteiligten, die auf die oben beschriebene Weise authentifizieren und autorisieren möchten, müssen zwingend derselben Föderation angehören.

Vorteile

Welche Vorteile bringt Shibboleth also? Nun hier kann man sehr klar die Vorteile für die einzelnen Akteure benennen. Für den Benutzer bedeutet es, sich nur einmal authentifizieren zu müssen, um verschiedene geschützte Angebote nutzen zu dürfen (SSO). Außerdem können die geschützten Ressourcen nun unabhängig vom geographischen Ort genutzt werden. Schließlich wird der Datenschutz gestärkt, da Nutzerdaten einerseits nicht mehr jedem Anbieter übermittelt werden müssen, andererseits die Daten dezentral verwaltet werden. Anbieter können die zu schützenden Angebote mit vergleichsweise geringem Aufwand absichern und benötigen keine eigene Benutzerverwaltung mehr. Zuletzt bringt es allen Institutionen auf Grund der leichten Steuerbarkeit des Zugriffs auf zu schützende Angebote Erleichterungen. Mitglieder einer anderen Institution können so geschützte Angebote, entsprechende Rechte vorausgesetzt, ebenfalls nutzen. Schließlich wird auch die Einbindung neuer Angebote stark vereinfacht.

Praxis

Diese noch nicht sehr alte, aber bereits ausgereifte Technik, wird bereits in einigen Ländern flächendeckend eingesetzt. In Europa sind es die Schweiz, Finnland und Großbritannien, in Übersee Australien und die USA. In den genannten Ländern partizipieren wegen der geschilderten Vorteile selbstverständlich auch Verlage. Zur Zeit wird in Deutschland eine Föderation nach Schweizer Vorbild beim Deutschen Forschungsnetz (DFN) gegründet. Die Initiative geht auf die UB Freiburg i. Br. zurück, da hier Erfahrungen im Vascoda-Teilprojekt AAR (Anm. 1) gesammelt und diese Technik bereits für Baden-Württemberg umgesetzt wurde. Flankiert werden die Bemühungen auch von der DFG, die in Zusammenarbeit mit anderen europäischen wissenschaftlichen Fördereinrichtungen (Anm. 2) die Authentifizierung und Autorisierung europaweit auf einen einheitlichen und kompatiblen Standard bringen möchte (Anm. 3).

Wie man sich leicht vorstellen kann, ist bei solchen Projekten der organisatorische Aufwand erheblich und sie benötigen einen entsprechend langen Vorlauf. Da die Verbundzentrale des GBV bei der Gründung der Föderation beteiligt ist und in Zukunft auch für den GBV die Authentifizierung und Autorisierung mittels Shibboleth anstrebt, wird im Februar die oben angekündigte Veranstaltung stattfinden. Sie ist ausdrücklich nicht technisch ausgerichtet! Es soll vielmehr darum gehen, Verständnisfragen zu erörtern und ein Problembewusstsein zu schaffen.

Weiterführende Links:

Wikipedia:
http://de.wikipedia.org/wiki/Shibboleth
http://de.wikipedia.org/wiki/Single_Sign_On
Offizielle Shibboleth Homepage
http://shibboleth.internet2.edu
Projekt Verteilte Authetifizierung, Autorisierung und Rechteverwaltung
http://aar.vascoda.de

Anmerkungen:

1 http://aar.vascoda.de
2 http://www.dfg.de/forschungsfoerderung/wissenschaftliche_infrastruktur/lis/projektfoerderung/internationale_zusammenarbeit/knowledge_exchange.html
3 http://www.bs.dk/content.aspx?itemguid={3338A3A9-97B3-4C82-B37D-1FCAA2CA105D}