Shibboleth

Juha Ojaluoma
Tietotekniikkaosasto

Shibboleth-tekniikkaa voidaan käyttää käyttäjäntunnistukseen organisaatioiden välillä. Samalla sillä voidaan välittää verkkosovelluksien tarvitsemia tietoja käyttäjästä.

Shibboleth on Internet2-yhteisön projekti, jonka tarkoituksena on mahdollistaa turvallinen käyttäjien tunnistaminen ja heitä koskevan tiedon vaihtaminen eri organisaatioiden välillä. Internet2 on Yhdysvalloissa toimiva konsortio, joka koordinoi 207 yliopiston yhteistoimintaa tietoverkkojen alalla.

Shibboleth perustuu standardeihin ja avoimeen lähdekoodiin. Standardit takaavat sen, että yhteistoiminta myös muiden vastaavat kriteerit täyttävien ohjelmistojen kanssa on mahdollista. Käytettyjä standardeja ovat muun muassa Security Assertion Markup Language (SAML), Secure Sockets Layer (SSL) ja Lightweight Directory Access Protocol (LDAP). Avoimuus kattaa arkkitehtuurin ja ohjelmiston lähdekoodin. Tämä lisää luottamusta ja mahdollistaa kaikkien kiinnostuneiden osapuolten osallistumisen kehitystyöhön.

Turvallinen tapa tunnistautua

Shibboleth tarjoaa turvallisen tavan valvoa pääsyä palveluihin, joiden saatavuutta on rajoitettava käyttäjien ominaisuuksien perusteella. Shibbolethin toiminta perustuu palveluntarjoajan ja identiteetintarjoajan yhteistyöhön. Palveluntarjoaja haluaa suojata jonkin osan Internetissä olevasta palvelustaan ja identiteetintarjoaja tarjoaa käyttäjän tunnistamiseen tarvittavan tekniikan. Kun käyttäjä haluaa käyttää Shibboleth-tekniikalla suojattua resurssia, hänet ohjataan tunnistautumaan identiteetintarjoajalle. Onnistuneen tunnistuksen seurauksena käyttäjä ohjataan haluamaansa resurssiin.

Shibbolethin käyttö on tietoturvallista, koska toimijoiden väliset yhteydet ovat salattuja ja käyttäjä tunnistautuu vain tutulle identiteetintarjoajalle. Kun salasanoja ei ole useita ja kirjautuminen tehdään kotiorganisaatiossa, on helpompaa käyttää monimutkaisempia vaikeasti murrettavia salasanoja. Käyttäjäkunnaltaan rajatuille palveluille riittää pääsynvalvonnassa yleensä tieto siitä, että käyttäjä on esimerkiksi opiskelija tai työntekijä tietyssä organisaatiossa. Näin identiteetintarjoajan ei tarvitse lähettää palveluntarjoajalle mitään käyttäjän henkilökohtaista tietoa. Toisaalta, jos palvelun käyttö vaatii käyttäjästä tarkempaa tietoa, sen vaihtaminen identiteetintarjoajan ja palveluntarjoajan kesken tapahtuu salatulla yhteydellä.

Eri toimijoiden välinen rajapinta on hyvin selkeä. Suurin koitos yhteistyössä on niin kutsutun federaation perustaminen. Siinä määritellään eri toimijat, ja näiden välillä vaihdettavat käyttäjätiedot. Shibboleth mahdollistaa ylläpidon kannalta järkevän arkkitehtuurin, joka on skaalautuva. Vaikka Shibboleth joudutaan erikseen asentamaan, on sen ylläpito jälkeenpäin helpohkoa.

<kuva shib_flow.png>

Käyttäjän pääsy Shibboleth-tekniikalla suojattuun palveluun tapahtuu useimmiten seuraavasti:

1) Käyttäjä pyytää haluamaansa resurssia Internetissä. Resurssi on suojattu ja se haluaa tietää, onko käyttäjällä lupa suojattuun resurssiin.

2) Käyttäjä ohjataan oman kotiorganisaation tunnistautumisjärjestelmään tai sivulle, johon on listattu kaikki organisaatiot, joilla on pääsy palveluun. Käyttäjä valitsee listasta kotiorganisaationsa ja ohjataan edelleen sinne.
3) Käyttäjä kirjautuu normaalisti omassa kotiorganisaatiossa.
4) Käyttäjä ohjataan takaisin alun perin haluamaansa palveluun ja mukana kuljetetaan identiteetintarjoajalta saatu varmennetta. Palveluntarjoaja hyväksyy tämän.
5) Palveluntarjoaja kommunikoi edelleen identiteetintarjoajan kanssa käyttäjää koskevista, palvelussa tarvittavista tiedoista ja päättää saamiensa tietojen perusteella, onko käyttäjällä lupa käyttää palvelua.

Shibboleth yliopistolla

Keväällä 2005 yliopistolla on yksi tuotantokäytössä oleva Shibboleth-identiteetintarjoaja. Tämä kuuluu Haka-federaatioon, jonka tarkoituksena on tarjota siihen liittyneille korkeakouluille mahdollisuus käyttää yhteisiä palveluita oman korkeakoulunsa käyttäjätunnuksilla.

Federaatiossa ajetaan muun muassa *Liikkuvuuden tuki* (LiTu) -hanketta, jossa Shibboleth-tekniikkaa käytetään joustavan opinto-oikeuden (JOO) verkkopalvelussa. Siinä opiskelija voi täyttää sähköisen hakemuksen joustavan opinto-oikeuden saamiseksi toisesta korkeakoulusta. Palvelu on hyvä esimerkki Shibbolethin peruskäytöstä. Shibbolethin avulla käyttäjä voi tunnistautua omassa kotiorganisaatiossaan, joka välittää JOO-palvelulle välttämättömiä tietoja opiskelijasta hakemuksen täyttämiseksi. Tiedot tulevat esitäytettyinä hakemuslomakkeeseen ja opiskelija täyttää loput kentät ja lähettää hakemuksen eteenpäin. Tiedot opiskelijan aikaisemmista suorituksista saadaan suoraan opiskelijarekisteristä eikä hakemuksia vastaanottavien virkailijoiden tarvitse erikseen tarkistaa tietojen oikeellisuutta. LiTu-hankkeessa tuotetun sähköisen JOOPAS-verkkopalvelun käyttäjinä olivat alkuvaiheessa Helsingin kauppakorkeakoulu, joitakin Helsingin yliopiston tiedekuntia sekä Teknillinen korkeakoulu. Nyt käyttö on laajentumassa yliopistossa muihin tiedekuntiin sekä uusiin korkeakouluihin, mm. Tampereen yliopistoon ja Tampereen teknillinen yliopistoon.

Tietotekniikkaosastolla on koekäytetty Shibboleth-tekniikkaa vuodesta 2003. Tieteen tietotekniikan keskus CSC on ollut organisoimassa hankkeita, joissa on testattu tekniikan toimivuutta korkeakoulujen välisessä yhteistyössä. Monet laitokset ja projektit Suomessa ja Euroopassa ovat osoittaneet kiinnostusta Shibboleth-tekniikan käyttöön ja testaukseen yhteistyössä Helsingin yliopiston kanssa. Toistaiseksi hankkeet ovat olleet hieman jäissä johtuen tuoreesta tekniikasta ja rajallisista aikaresursseista.

Shibboleth tarjoaa mielenkiintoisia näkymiä ajatellen hajanaisen infrastruktuurin toiminnan tehostamista ja organisaatioiden välistä yhteistyötä. Julkisia Shibboleth-federaatioita on käytössä korkeakoulujen välillä Yhdysvalloissa, Ranskassa, Belgiassa, Australiassa, Englannissa, Sveitsissä ja meillä Suomessa.

Asennuksesta ja käytöstä

Käyttäjätunnistuksen toteuttaminen voidaan toteuttaa Shibbolethin avulla. Samalla saadaan tarvittaessa tietoja käyttäjästä pääsynvalvonnan tarkentamiseksi tai jonkin verkkosovelluksen käyttöön. Asentamalla Shibboleth-palveluntarjoaja omalle palvelimelle, voidaan käyttäjätunnistukseen tarvittava tekniikka jättää tietotekniikkaosaston hoidettavaksi.

Shibboleth-palveluntarjoaja voidaan asentaa Unix-, Windows- ja Mac OS X -alustoille. WWW-palvelimina voidaan käyttää Apache- (versiot 1.3.x tai 2.0.x) tai IIS (versiot 4.0 ja uudemmat) -palvelimia. Apache-ohjelmisto täytyy olla käännettynä mod_so-moduulin kanssa ja sen on tuettava SSL-suojausta. Näiden vaatimusten lisäksi Shibbolethin käyttö vaatii OpenSSL:n ja muutaman

ohjelmakirjaston käyttöä. Moduulien ja kirjastojen kääntämistä lähdekoodista suositellaan lämpimästi etenkin tuotantokäytössä, koska näin ohjelmapakettien päivittäminen on helpompaa.

Asennus alkaa kääntämällä vaaditut paketit palvelimelle. Shibboleth-paketin mukana tulee Apachen konfigurointitiedostoon (httpd.conf) lisättävät rivit, jotka määrittelevät moduulien sijainnin ja esimerkkiasetukset kuvitellun palvelun suojaamiseksi. Itse Shibboleth-palveluntarjoajan asetukset ovat XML-tiedostoissa ja ne sisältävät toimivat arvot testikäytölle asennuksen yhteydessä. Pienillä muutoksilla palvelu saadaan konfiguroitua turvalliseen käyttöön halutussa ympäristössä.

Shibboleth vaatii sertifikaatin käyttöä. Vaikka WWW-palvelimelta ei vaadita SSL-suojausta, on se käyttäjien turvallisuuden vuoksi erittäin suositeltavaa. Shibboleth voi käyttää omaa tai palvelimen kanssa yhteistä sertifikaattia. Edellytyksenä on, että sertifikaatin on allekirjoittanut taho (CA), jonka identiteetintarjoaja hyväksyy.

WWW-palvelun suojaaminen tapahtuu määrittelemällä halutut vaatimukset samalla periaatteella kuin palvelimen toimintaa hallitaan (.htaccess, Directive, Location, jne). Asetukset voivat näyttää esimerkiksi seuraavilta:

```
<Location /secure>
AuthType shibboleth
ShibRequireSession On
require affiliation employee
#require valid-user
</Location>
```

Ensimmäinen rivi määrittelee Shibbolethin käytettäväksi tunnistusmenetelmäksi. Toinen rivi vaatii istunnon (session) käytön ja kolmas määrittelee vaatimukset resurssin saamiseksi. Tässä tapauksessa vaatimus *affiliation employee* määrittelee palvelun sallituiksi käyttäjiksi yliopiston henkilökunnan. Eli käyttäjästä saatavan *affiliation*- attribuutin on sisällettävä rooli *employee* (ks. kuva, kohta 5). Kommentoitu rivi *valid-user* tarkoittaisi ketä tahansa käyttäjää, kuka on onnistuneesti tunnistautunut identiteetintarjoajalla.

Palveluntarjoaja ja identiteetintarjoja sopivat keskenään välillään vaihdettavista attribuuteista. Näitä voidaan käyttää pääsynvalvonnassa tai sovelluksessa. Sovellus saa attribuutit käyttöönsä HTTP-pyynnön otsikkokenttien avulla. Esimerkiksi edellisessä, affiliation-attribuutti olisi muuttuja *HTTP_AFFILIATION*, jonka arvo olisi *employee*.

Lisätietoja

http://shibboleth.internet2.edu/
http://www.csc.fi/suomi/funet/middleware/haka/
https://www.joopas.fi