Keskitetty käyttäjätunnistus yliopistolla

Minna Harjuniemi
Tietotekniikkaosasto

Keskitetty käyttäjien tunnistus on kehittynyt 1990-luvulta sisäänsoittopalvelun unix-käyttäjien tunnistamisesta laajaksi kokonaisuudeksi. Eri tekniikoita käytetään nyt toistensa tukena hyvin monenlaisissa verkkopalveluissa. Vahvojen tunnistustekniikoiden käyttöönotto on yhä tärkeämpää perinteisen salasanavarmistuksen rinnalle.

Kurkistus viime vuosituhannelle

Internetin käytön laajentuessa 1990-luvulla kasvoivat myös yliopiston tarjoamien sisäänsoittopalveluiden käyttäjämäärät. Modeemilla sai kotoa yhteyden yliopiston verkkoon ja sitä kautta ulkomaailmaan. Alkuvaiheissa mikroverkkokäyttäjille oli tarjolla oma soittosarjansa ja unix-käyttäjille omansa. Ensimmäinen käytti omaa tunnistustapaansa, jälkimmäisessä käyttäjäntunnistus perustui yleisesti käytössä olevaan Radius-protokollaan (*Remote Authentication Dial In User Service*).

Hyvin pian kävi selväksi, että kahden erillisen järjestelmän ylläpito oli työlästä ja käyttäjille hankalaa. He eivät aina edes tienneet, mikä tunnus heillä oikeastaan oli ja mihin numeroon pitäisi soittaa. Atk-keskuksessa muokattiin tunnistusta hoitavaa Radius-palvelinta niin, että se pystyi käyttäjätunnuksen perusteella ohjaamaan tunnistuspyynnön joko unix- tai Novell-ympäristöön, ja vähitellen myös muutamaan muuhun samaa protokollaa osaavaan järjestelmään, mm. Windows-verkkoon. Näin saatiin käyttöön ensimmäinen versio keskitetystä käyttäjätunnistuspalvelusta. Myös 1990-luvulla käynnistetty Mappi-sähköpostipalvelu nojautui alusta alkaen samaan tunnistusjärjestelmään.

Vaihtoehtona mainitulle järjestelylle olisi ollut se, että verkkopalveluihin tunnistautumista varten olisi vaadittu erillinen salasana ja työasemaan tai unix-ympäristöön kirjautumiseen toinen. Monessa muussa organisaatiossa on vastaavassa tilanteessa päädytty tähän malliin.

Kohti nykyaikaa

Radius-tunnistuksella pärjättiin varsin pitkälle. Aikojen kuluessa tunnistusta ovat hyödyntäneet sisäänsoittopalvelun lisäksi monet muutkin palvelut: mm. Mappi-sähköposti, Alma-intranet, liikuntatoimiston varausjärjestelmä, HUPNet-vierailijaverkko, lukuisat erityisesti käyttölupahallinnon WWW-lomakkeet sekä opiskelun ja opetuksen tuen tietojärjestelmä WebOodi. Siinä missä sisäänsoiton käyttäjämäärät ovat pudonneet, muiden palvelujen käyttö on ollut kasvussa.

Radius sopii hyvin sellaisten sovellusten tunnistusjärjestelmäksi, joissa riittää, että käyttäjällä ylipäätään on voimassaoleva tunnus ja salasana. Sovellusten monimutkaistuessa on kuitenkin alettu tarvita hienovaraisempaa käyttöoikeuksien hallintaa. On pitänyt pystyä erottamaan opiskelijat ja opettajat, selvittämään käyttäjän laitos tai tunnistamaan, onko kyseessä ns. pääkäyttäjä, jolla on järjestelmään enemmän oikeuksia.

Tähän välineet tarjosi LDAP-yhteyskäytäntö (*Lightweight Directory Access Protocol*), joka on Radiuksen tavoin hyvin standardoitu protokolla. Vuonna 2002 käynnistettiin atk-osastolla hanke *”HSTYA-valmistautuminen ja käyttöönotto vuosina 2002–2007”*. Sen ensimmäiseksi tehtäväksi annettiin LDAP-tunnistuksella lähestyttävän käyttäjähakemiston kehittäminen. Alkuvaiheessa suunnitelmissa oli vielä ensisijaisesti ns. vahvan tunnistuksen eli toimikorttien käyttöönottoon koko yliopistoympäristössä.

Alusta alkaen oli selvää, että LDAP-hakemisto nojautuisi käyttäjien tunnistuksessa jo toimivaksi havaittuun Radius-palveluun, eikä hakemistoon tehtäisi käyttäjille erillisiä salasanoja. Sen perustietosisältö eli käyttäjien nimitiedot ja sähköpostiosoitteet sekä taustatiedot, mm.

laskutustunnus saatiin aikaan varsin nopeasti. Yhtä pian kävi ilmi, että hakemiston sisältö tulee vaatimaan jatkuvaa kehittämistä. Todettiin myös, että hakemistoon ja keskitettyyn käyttäjätunnistukseen liittyvät linjaukset eivät ole ainoastaan tietotekniikkaorganisaation asia, vaan koettiin tärkeäksi keskustella ongelmista erityisesti hallintoviraston muiden osastojen kanssa.

Hallintojohtajan päätöksellä perustettiin vuonna 2004 *Käyttövaltuus- ja rooliryhmä*. Sen tarkoituksena oli määritellä yliopiston henkilö- ja organisaatiotiedot, sekä henkilötietojen osalta mm. roolitiedot (opiskelijat, henkilökunta jne.). Työryhmän piti myös tehdä ehdotus hallinnon tietojärjestelmien käyttövaltuuksien ylläpidon yhtenäistämiseksi. Työskentelyn tuloksena syntyneessä hallintojohtajan päätöksessä (37/2004) esitettiin käyttäjähakemiston edelleen vahvistamista, erillisen organisaatiorekisterin perustamista, hallinnon tietojärjestelmien muuttamista käyttämään LDAP-hakemistoa sekä ohjeiden laatimista hakemiston hyödyntämiseksi. Organisaatiorekisteri (ks. sivu xx) valmistuu lähiaikoina. Myös muut työryhmän ehdotukset ovat saaneet laajalti kannatusta ja edistyneet.

HSTYA:sta tunnistamistekniikkaan

Tietotekniikka-alalle on kuvaavaa se, että monivuotisen kehittämishankkeen, kuten HSTYA-valmistautumisen, alussa ei pystytä täysin arvioimaan, mihin lopulta päädytään. Jo hankkeen toisena vuotena lähdettiin kokeilemaan uutta Shibboleth-tekniikkaa (ks. sivu xx), jossa oli monia yliopistolle erittäin sopivia ominaisuuksia. Näitä olivat mm. parempi tietoturvallisuus, koska salasana kirjoitetaan vain yhteen WWW-osoitteeseen, parempi tietosuoja käyttäjän kyetessä hallinnoimaan tietojensa luovutusta sekä mahdollisuus palveluiden tarjoamiseen myös toisessa organisaatiossa tunnistetuille käyttäjille. Shibbolethin hyödyntämismahdollisuudet ovat hankkeen aikana laajentuneet, ja menetelmä on saamassa jalansijaa myös kaupallisella puolella.

HSTYA-hanke muuttui *Hakemisto*-hankkeeksi (tuttavallisesti *HaHa*), koska pääpainopiste siirtyi nimenomaan hakemistoinfrastruktuurin kehittämiseen ja vahvaan sähköiseen tunnistamiseen liittyvät asiat tuntuivat vielä keskeneräisiltä. Käyttäjähakemisto oli noussut niin olennaiseen osaan yliopiston tietoteknisessä ympäristössä, että syksyllä 2005 päätettiin se vakinaistaa osaksi tietotekniikkaosaston normaalia toimintaa, ja hakemiston osuus hankkeesta lakkautettiin. Hankkeen viimeinen vaihe toteutetaan nyt *Tunnistamistekniikat*-nimellä.

Käyttäjätunnistus nyt

<kuva 1>

Keskitetyn käyttäjätunnistuksen ytimenä on edelleenkin Radius-palvelin. Tunnistusta kaipaava järjestelmä lähettää salasanan tarkistuspyynnön Radius-protokollalla Radius-proxyksi kutsutulle välityspalvelimelle. Pyynnön lähettävä järjestelmä on konfiguroitu hyväksyttyjen palvelinten listalle ja liikenteen salauksesta huolehtii ns. yhteinen salaisuus. Välityspalvelin ohjaa tunnistuspyynnön eteenpäin, vastaanottaa tiedon tarkastuksen onnistumisesta tai epäonnistumisesta sekä välittää vastauksen takaisin tunnistusta pyytäneelle järjestelmälle.

Proxy-palvelin tunnistaa käyttäjätunnuksen perusteella, mihin kohdejärjestelmään tunnistuspyyntö pitäisi lähettää. Jo muutaman vuoden ajan on kuitenkin ollut käytäntö, että jos käyttäjällä on useita käyttölupia, tunnistusjärjestelmä lähettää salasanan tarkistuspyynnön käyttäjän pääkäyttöluvan mukaiseen ”kotijärjestelmään”. Käyttäjä voi halutessaan itse vaihtaa pääkäyttöluvaksi kytkettyä järjestelmää WWW-lomakkeella.

<kuva 2>

Uudemmissa palveluissa käytetään LDAP-hakemistoa. Se lähettää salasanan tarkistuspyynnön aina Radius-palvelimelle, mutta täydentää vastausta tarvittaessa esim. käyttäjään liittyvillä attribuuttitiedoilla, vaikkapa sähköpostiosoitteella. Nämä tiedot ovat aina LDAP-

hakemistossa, ja ne on kuvattu määrämuotoisina etukäteen määriteltyjen sanastojen puitteissa eli ns. LDAP-skeemoina.

Tietyissä palveluissa käytetään Shibboleth-järjestelmää. Tämä lähettää tunnistuspyynnön LDAP-palvelimelle, mutta osaa välittää LDAP-hakemiston tietojen lisäksi informaatiota tarvittaessa muistakin järjestelmistä. Esimerkiksi sähköisessä joustavan opinto-oikeuden JOO-hakemuksessa tarvittavat opintosuoritusmäärät ja suuntautumisvaihtoehtotiedot haetaan suoraan opintojen ja opetuksen tietojärjestelmästä Oodista.

Tiellä vahvempaan tunnistukseen

Keskitetyn käyttäjätunnistuksen merkitys on kasvanut entisestään. Uusia järjestelmiä otetaan käyttöön vuodessa useita, ja käyttäjähakemistoa hyödynnetään, kuten pitääkin, myös muuhun kuin käyttäjien tunnistamiseen, eli tietojärjestelmät hakevat sinne tallennettua tietoa. Tietojen käytöstä sovitaan luonnollisesti aina erikseen, ja niin käyttäjähakemistosta kuin muustakin käyttölupajärjestelmästä on tehty lain vaatimat erilliset rekisteriselosteet.

Yksi tunnus, yksi salasana -ajattelu on tuonut käyttäjälle huomattavia helpotuksia ja se vähentää ainakin salasanojen muistiinkirjoittamisen tarvetta. Samalla kasvavat kuitenkin riskit. Jos käyttäjä hukkaa salasanansa, on väärinkäyttäjälle tie auki esimerkiksi sähköpostiin, UPJWebiin, Almaan suljettuine ryhmähakemistoineen ja kotihakemiston tietoihin, ainakin kunnes käyttäjä vaihtaa salasanansa. Salasanan suojaaminen ja hyvän salasanan käyttö ovat aina olleet tarpeellisia toimia, nyt ne ovat suorastaan ehdottoman välttämättömiä.

Samaan ongelmakenttään liittyy myös kertakirjautuminen ja sen rajat. Esimerkiksi Alman kautta pääsee myös henkilökohtaisiin työvälineisiin yhdellä napsautuksella ilman uutta kirjautumista. Tämä on ilahduttanut ja helpottanut monien käyttäjien elämää. Toisaalta, jos yhteys unohtuu avoimeksi, myös seuraava käyttäjä pääsee kaikkiin samoihin järjestelmiin. Tämän vuoksi kriittisimmissä tapauksissa, kuten UPJWeb-sovelluksessa vaaditaan uutta tunnistautumista, vaikka teknisesti kertakirjautuminen olisikin mahdollista.

Näihin osin pessimistiseltäkin vaikuttaviin uhkakuviin on kuitenkin odotettavissa valoa. Tältä osin ollaan palaamassa alkuperäisen HSTYA-hankkeen juurille, eli Suomen yliopistomaailmassa tutkitaan myös vahvaan tunnistukseen liittyvien tekniikoiden käytettävyyttä ja sopivuutta korkeakouluympäristöön.

Lisätietoa

minna.harjuniemi@helsinki.fi
http://www.freeradius.org/
http://www.openldap.org/
http://shibboleth.internet2.edu/