

Lupahallinnon historiaa ja nykypäivää

Risto Hietanen

Pirjo Kallström

Timo Klöf

Tietotekniikkaosasto

Yliopiston tietojärjestelmien käyttäjähallinto on kokenut melkoisen muodonmuutoksen 1970-luvun Burroughs-aikakaudelta nykyiseen keskitettyyn käyttöoikeuksien hallintaan, jossa on lähes 65 000 käyttölupaa.

Käyttäjähallinnon periaatteita

Yliopistolla yleisessä käytössä olevilla tietojenkäsittelyjärjestelmillä on keskitetty käyttäjähallinto. Tietotekniikkaosastolla ylläpidetään tietokantaa, johon on talletettu kaikki yliopiston verkossa olevat käyttäjätunnukset. Uusi opiskelija saa tunnuksensa automaattisesti. Kun hänet kirjataan opiskelun tietojärjestelmään Oodiin, lähevät opiskelijan tiedot myös käyttölupajärjestelmään ja hänelle muodostetaan ohjelmallisesti käyttäjätunnus sekä *etunimi.sukunimi@helsinki.fi*-muotoinen postinimi. Tunnus ja sähköpostiosoite aktivoidaan käyttölupapisteessä, jolloin luodaan käyttölupa johonkin yliopiston verkossa olevaan laitteistoon, tavallisesti mikroverkkoon. Vastaavasti yliopiston työntekijän palvelusuhdetiedot saadaan henkilörekisteristä luotaessa hänelle käyttölupaa.

Lupahallinnon varhaishistoriaa

Yliopiston ensimmäinen varsinainen henkilökunnan ja opiskelijoiden käytössä ollut tietokone oli Burroughs-laitteisto. Se oli käytössä vuodesta 1970 vuoden 1987 loppuun. Tuona aikana ei ollut tarvetta henkilökohtaisiin käyttäjätunnuksiin, vaan kaikille tehtäväkokonaisuuksille annettiin projektitunnukset. Ne olivat kuusimerkkisiä, muotoa AA1234 olevia tunnuksia, joissa kirjainosa kuvasi tiedekuntaa, laitosta tai tiettyä toimintoa ja jatkeena oli juokseva numero. Esimerkiksi tietojenkäsittelyopin approbatur-laboratoriolla oli yksi tunnus (JY1023), jota kaikki perusopintovaiheen opiskelijat käyttivät.

Tunnukseen liittyi salasana, joka annettiin opiskelijoiden tietoon. Etäyhteyksiä ei silloin vielä paljon käytetty, vaan pääasiallinen tiedon syöttöväline oli reikäkortti ja myöhemmin kiinteällä yhteydellä varustettu päätelaite. Tietoturvariskeistä ei vielä tiedetty mitään.

Burroughs-järjestelmän tunnuksien ylläpito hoidettiin käsin ja koneen antamista lokitiedoista laskettiin kuukausittaiset käyttötilastot. Käytön kasvaessa laitteiston suorituskyky ei enää riittänyt ja avuksi otettiin itse toteutettu tunnuskohtainen kuukausikiintiöinti. Se yksinkertaisesti sulki kiintiönsä ylittäneet tunnuksent loppukuun ajaksi.

VAX-aikakausi

Kesällä 1987 otettiin käyttöön Digitalin VAX-järjestelmä. Tietokoneen käyttötavat muuttuivat ratkaisevasti. Rakennettiin yliopiston kattava verkko, tuli sähköposti ja sen mukana yhteydet maailmanlaajuisiin verkkoihin (Decnet, DataPak, IBM:n

tutkimusverkko jne.). Keskuskoneesta tuli entistä enemmän omien henkilökohtaisten tietojen käsittely- ja säilytyspaikka. Verkon ja sähköpostin käyttö aiheuttivat tarpeen yksikäsitteisille käyttäjätunnuksille ja sähköpostiosoiteille. Yliopiston tiedekunnat ja laitokset olivat hankkineet myös omia tietokonelaitteistojaan, mutta näillä kullakin oli oma käyttäjäkirjanpituksensa.

VAX-järjestelmän käyttöönoton yhteydessä luotiin uuden toimintaympäristön tarpeita vastaava käyttölupajärjestelmä. Aikaisemmasta poiketen käyttäjätunnukset muuttuivat henkilökohtaisiksi. Tunnukseksi otettiin käyttäjän sukunimestä ja etunimien alkukirjaimista muodostettu korkeintaan 12-merkkinen nimilyhenne, joka oli kahdeksan ensimmäisen merkin osalta yksikäsitteinen. Käyttäjistä haluttiin lisäksi tallettaa myös muuta tietoa, kuten laskutustunnus, nimi- ja osoitetiedot, laitos ja suhde yliopistoon. VAX-järjestelmän sisäinen käyttäjätietokanta salli kuitenkin vain rajoitetun määrän tietoa. Siksi lisätietojen talletus toteutettiin erillisenä VAX-järjestelmän RDB-tietokantana. Sen avainkenttänä oli käyttäjälle annetun tunnuksen kahdeksan ensimmäisen kirjaimen muodostama merkkijono eli ns. ”kasitunnus”.

Käyttölupajärjestelmä laajeni 1990-luvun alkupuolella voimakkaasti, kun siihen liitettiin unix- ja mikroverkkolupien hallinta. Vuonna 1994 keskitetyn käyttölupajärjestelmän piirissä oli jo 31 laitteistoa. Lupatietokantaan oli talletettu 13 300 tunnusta, joille oli myönnetty 28 000 laitteistokohtaista käyttölupaa. Lupatietokanta sai nimekseen *Master*. Yliopiston laitteistokannan kasvaessa siihen alettiin tallettaa myös muiden järjestelmien käyttölupia. Kaikki yliopiston tietokoneiden käyttäjät saivat vähitellen yksikäsitteisen käyttäjätunnuksen, kun ylläpitäjät rekisteröivät uudet tunnukset ensin keskitettyyn lupatietokantaan ja loivat tunnukset sen jälkeen omiin laitteistoihinsa.

Järjestelmän toimintoja lisättiin ja syksyllä 1994 uusien opiskelijoiden tiedot haettiin ensimmäistä kertaa suoraan OPREK-opiskelijarekisteristä. Tällöin heidän käyttäjätunnuksensa ja postinimensä voitiin muodostaa ohjelmallisesti. Osalle opiskelijoista voitiin tehdä käyttöluvat valmiiksi etukäteen. Lupatietokannan ja opiskelijarekisterin välisen yhteyden ansiosta opiskelijalle tuli myös mahdollisuus saada epävirallinen rekisteriote opintosuorituksistaan.

Tietokoneiden käytön nopeaa yleistymistä kuvaa se, että vuoden 1996 loppuun mennessä oli lupatietokantaan rekisteröity 37 laitteistoa, noin 29 000 käyttäjätunnusta ja yhteensä noin 57 000 käyttölupaa. Vuonna 1996 päätettiin asteittain luopua VAX-järjestelmästä ja keskittää voimavarat unix- ja mikroverkkoratkaisuihin. Samalla tuli uusittavaksi myös hyvin VAX-keskeinen lupajärjestelmä.

Oraclen Forms avuksi

Helmikuussa 1997 käynnistyi hanke, jonka tavoitteena oli kehittää uusi käyttölupien hallintajärjestelmä. Perustaksi valittiin uuteen unix-palvelimeen asennettu Oracle-tietokanta. Vanhaan järjestelmään verrattuna tietosisällössä ei tapahtunut kovin suuria muutoksia. Sen sijaan tietokannan rakenne muuttui täydellisesti, kun relaatiomallin oppien mukaisesti tiedot koottiin loogisiksi kokonaisuuksiksi. Käyttölupatiedot muodostivat varsinaisen Masterin. Uusi Oracle-pohjainen järjestelmä otettiin käyttöön 15.12.1997.

Käyttöliittymäksi rakennettiin Oraclen Forms-kehitystyökalulla sähköiset lomakkeet. Niiden avulla myös laitojen ja tiedekuntien vastuuhenkilöille tuli mahdollisuus ylläpitää omien laitteistojensa lupatietoja Master-tietokannassa.

Uudella järjestelmällä voitiin automatisoida eri laitteistojen käyttäjien lisääminen. Uudet käyttöluvut luotiin lupatietojen perusteella automaattisesti unix-laitteistoihin ja mikroverkkoihin. Ratkaisu toi myös mahdollisuuden joustavasti täydentää uusia toimintoja. Näitä ovat olleet mm. radius-tunnistuksen, LDAP-käyttäjähakemiston ja Mappi-postin tarvitsemat lisäykset.

Käyttäjähallinta webiin

WWW-käytön yleistyessä rakennettiin laitosten atk-yhdyshenkilöille verkkopohjaisia työkaluja käyttölupien seurantaan. Yhdyshenkilöt pääsivät jatkamaan laitoksensa käyttölupien voimassaoloa WWW-lomakkeella. Opiskelijat saivat oman lomakkeen käyttölupatietojensa tarkistamiseen ja omatoimiseen käyttöluvan voimassaolon jatkamiseen, joka perustui opiskelijarekisteristä saatuun läsnäolotietoon.

Uuden Oodi-opiskelijatietojärjestelmän käyttöönoton jälkeen vuosituhannen vaihteessa rakennettiin tiivis tietojen vaihto sen ja käyttölupatietokannan välille. Esimerkiksi opiskelijan sähköpostiosoite päivitetään käyttölupatietokannasta Oodiin. Uusien opiskelijoiden perustietoja siirretään Oodista käyttölupatietokantaan ja puuttuvia tai muuttuvia tietoja täydennetään Oodin tiedoilla (mm. asiointikieli ja läsnäolotieto)

Yliopistolle luotu Tietovarasto-järjestelmä mahdollisti palvelusuhdetietojen hyväksikäytön. Vuoden 2003 keväällä myös henkilökunnan käyttölupien omatoiminen voimassaolon jatkaminen oli mahdollista, mikä vähensi atk-yhdyshenkilöiden rutiinitehtävien määrää.

Vuoden 2003 aikana otettiin käyttöön satunnaista lyhytaikaista käyttöä varten kevyttunnukset, joita laitosten atk-yhdyshenkilöt voivat antaa rekisteröimällä luvan tiedot suoraan käyttölupatietokantaan. Näiden tunnusten suosio kuitenkin yllätti, eikä käyttö ole jäänyt lyhytaikaiseksi. Vuoden 2004 aikana oli käytössä 2169 ja seuraavana vuonna 3507 kevyttunnusta. Tunnusten yhteenlaskettu käyttöpäivien määrä oli 253 221 vuonna 2004 ja 524 976 vuonna 2005.

Käyttölupajärjestelmä selvisi ongelmitta vuosituhannen vaihteesta, mutta Oraclen vaihtaminen versiosta 7 versioon 8 osoitti, että vanha käyttöliittymä oli uusittava. Järjestelmän jatkokehitys aloitettiin korvaamalla Forms-pohjaiset lomakkeet uudella WWW-sovelluksella. Itse tietokantaan tehtiin tässä yhteydessä vain pieniä muutoksia. Tietotekniikkaosastolle oli hankittu uusi aikaisempaa huomattavasti tehokkaampi tietokantapalvelin, missä järjestelmän kehitystyö tehtiin. Uusittu käyttölupajärjestelmä otettiin käyttöön keväällä 2004.

Nykypäivää

Keskitetyn käyttölupatietokannan avulla hallitaan eri laitteistojen käyttölupia. Suurin osa laitteistojen luvista luodaan suoraan käyttölupatietokannan perusteella. Tietokanta palvelee useita keskeisiä yliopiston verkkopalveluita, kuten yliopiston Alma-intranetiä, sähköpostia, Mainari-sähköpostihakemistoa, WebOodia sekä keskitettyä käyttäjätunnistusta (LDAP, Radius ja Shibboleth). Siitä tuotetaan myös kuukausittaiset tilastot kustannusten kohdentamiseen.

Vuoden 2005 lopulla oli käytössä 50 031 käyttäjätunnusta, joiden lisäksi 14 235 tunnusta on ns. tunnusvarastossa. Lupajärjestelmän piirissä oli 37 laitteistoa, joihin oli myönnetty yhteensä 63 407 käyttölupaa.

Laitosten atk-yhdyshenkilöt ovat 1970-luvulta alkaen hoitaneet laitostensa käyttölupia ja keskuskoneiden käytön seuranta. Käyttäjämäärän kasvaessa heidän

rutiinitehtäviensä helpottamiseksi on rakennettu erilaisia verkon kautta käytettäviä työkaluja. Vuoden 2005 lopulla perustettiin Almaan atk-yhdyshenkilöiden työryhmäalue, josta kaikki tarpeelliset työkalut löytyvät.

Käyttölupien rekisteröintiä hoitavat tietotekniikkaosaston Keskustan, Kumpulan, Meilahden ja Viikin käyttölupapisteiden henkilökunta. Lupia rekisteröivät lisäksi myös laitosten omien laitteistojen 58 ylläpitäjää.

Tämän vuoden haasteisiin kuuluu käyttölupajärjestelmän kehittäminen siten, että jokaisen käyttöluvan haltijan perustiedot saadaan opiskelijatietojärjestelmästä, henkilöstötietojärjestelmästä tai tänä vuonna luotavasta ulkopuolisten käyttäjien tietokannasta. Lupien käsittelyä kehitetään ottamalla käyttöön sähköistä allekirjoitusta hyödyntävät haku- ja sitoumuslomakkeet, joissa käytetään ns. Tupas-tunnistusta. Käyttölupahallinto tulee myös hyödyntämään yliopiston uutta organisaatiorekisteriä.