Aalto-yliopisto
Perustieteiden korkeakoulu

Perustieteiden korkeakoulu
http://sci.aalto.fi/

Väitöstiedote 04.05.2016

Seuraavan sukupolven julkisen avaimen salaustekniikat pääsynvalvonnan toteutuksessa

Väitöskirjan nimi	Enforcing Role-Based Access Control with Attribute-Based Cryptography for Environments with Multi-Level Security Roolipohjaisen pääsynhallintamallin toteuttaminen attribuuttipohjaisilla salausmenetelmillä monitasotietoturvan vaatimusten mukaisesti
Väitöskirjan sisältö	Roolipohjainen pääsynvalvonta (RBAC) on moderni malli kontrolloida pääsyä erityyppisten tietojärjestelmien tietoihin ja toimintoihin. RBAC toteutetaan tyypillisesti esim. käyttöjärjestelmien turvaytimien avulla, mutta tällaiset toteutukset eivät kuitenkaan hyvin sensitiivisissä tapauksissa skaalaudu riittävällä turvatasolla dynaamisiin ja hajautettuihin ympäristöihin, kuten pilvilaskentaan tai esineiden internetiin. Pääsynvalvonnan toteuttaminen salausteknisin keinoin (salaamalla ja/tai allekirjoittamalla digitaalisesti tietoalkiot yksitellen) on myös mahdollista, mutta toistaiseksi melko alkeellista: ensinnäkin perinteisin salausmenetelmien avulla toteutettuna toteutuksesta tulee liian kömpelö, erityisesti avaintenhallinnan osalta ja toisekseen toteutukset ovat kyenneet kattamaan vain pienen osan pääsynhallintamallin kaikista toiminnoista. Tässä väitöskirjassa osoitetaan, että käyttäen seuraavan sukupolven julkisten avainten salausmenetelmien luokkaa, nk. attribuuttipohjaista salausta, voidaan lähes koko RBAC-malli toteuttaa kryptografisesti, esimerkiksi pääsynhallintakäytänteet voidaan koodata suoraan avaimeen ja salakielitekstiin (tai allekirjoitukseen). Merkittävimmät edut seuraavat kryptografisen suojauksen korkeasta luotettavuustasosta, hienojakoisesta kontrollista ja luontaisesta hajautettavuudesta ja ympäristöriippumattomuudesta. Esimerkiksi potilastiedoista olisi mahdollista purkaa ainoastaan käsittelijän sen hetkiseen tehtävään, käyttöaikaan ja rakennukseen liittyvien oikeuksien mukaiset tiedot.
Väitöskirjan ala	Tietojenkäsittelytiede, kryptologia / salaustekniikat
Väittelijä	Mikko Kiviharju, tekniikan lisensiaatti
Väitöksen ajankohta	17.5.2016 klo 12
Paikka	Aalto-yliopiston perustieteiden korkeakoulun AS2-sali, Otaniementie 17, Espoo
Vastaväittäjät	professori Reihaneh Safavi-Naini, University of Calgary, Canada Dr. Konrad Wrona, NATO CI Agency, Haag, The Netherlands
Kustos	professori Kaisa Nyberg, Aalto-yliopiston perustieteiden korkeakoulu, tietotekniikan laitos
Elektroninen väitöskirja	http://urn.fi/URN:ISBN:978-952-60-6774-2
Perustieteiden korkeakoulun väitöskirjat	https://aaltodoc.aalto.fi/handle/123456789/52
Väittelijän yhteystiedot	Mikko Kiviharju, PVTUTKL, PL 10, 11311 RIIHIMÄKI mikko.kiviharju@mil.fi

Väitöskirja on julkisesti nähtävillä Aalto-yliopiston perustieteiden korkeakoulun ilmoitustaululla Konemiehentie 2, sekä ilmoitustaululla Otakaari 1, Espoo viimeistään 10 päivää ennen väitöstilaisuutta.