

Luottamuksenhallinta

Sini Ruohomaa
Helsingin yliopisto
Tietojenkäsittelytieteen laitos
sini.ruohomaa@cs.helsinki.fi

1 Johdanto ja käsitteenmäärittely

Luottamus on tärkeä osa ihmisten välistä kanssakäyntiä. Se toimii vastapainona epävarmuudelle, jonka muiden vapaa tahto saa aikaan. Myös palveluita verkossa tarjoava organisaatio altistuu epävarmuudelle avatessaan osan järjestelmästään ulkopuolisille — kumppaneille tai asiakkailleen. Epävarmuutta ja siihen liittyvää riskiä voi vähentää kontrollikeinoin, kuten tarkalla valvonnalla tai vaatimalla palvelun käyttäjiltä erilaisia vakuuksia. Täydellistä hallintaa ei kuitenkaan voida saada aikaan, ja riskiä pienentävät toimenpiteet voivat myös hankaloittaa palvelun käyttöä liaksi. Täten myös palveluntarjoaja tarvitsee luottamusta jäljelle jääneen epävarmuuden vastapainoksi.

Luottamuksen määritelmät vaihtelevat kirjallisuudessa sovelluksen mukaan. Tätä esitystä varten luottamus määritellään *halukkuudeksi sallia annetun kumppanin tietty toiminta, kun huomioidaan sallimisen tarpeellisuus ja riski sekä kumppanin maine päätöshetkellä*. Luottamus on sidottu tahtoon ja tietoiseen päätökseen luottaa tai olla luottamatta. Maine sen sijaan voi erityisesti ihmisten käytössä painottua tunteisiin ja kehittyä tiedostamatta. Se on *käsitys, jonka toimija on aiemmillä teoillaan antanut pyrkimyksistään ja normeistaan* ([MMH02], mukaillen). Luottamuksenhallinta kerää luottamukseen liittyvää tietoa, analysoi sitä ja tuottaa sen pohjalta tilannesidonnaisia luottamuspäätöksiä. Päätöksillä voidaan tukea palveluntarjoajan ja -käyttäjän vuorovaikutusta. Helsingin yliopiston Tietojenkäsittelytieteen laitoksen Trust Based on Evidence -projekti (TuBE) tutkii luottamuksenhallintaa web-palveluympäristössä.

2 Luottamuksenhallinnan kehitys

Yksinkertaisimmillaan luottamuksenhallinta vaatii paljon tukea ihmiskäyttäjiensä olemassaolevista luottamustiedoista. Luottamuspäätösten politiikka voidaan ilmaista esimerkiksi pääsylistoin (ACL, *Access Control List*), jotka jaottelevat monissa nykyjärjestelmissä käyttäjät erilaisiin luotettavuuden luokkiin. Pääsylistojen kaltaiset mekanismit tallentavat vain päätöksen tuloksen, eivätkä ota huomioon tilanteen muuttumista esimerkiksi joidenkin käyttäjien maineen parantuessa tai heiketessä. Erilaisten politiikkakielten kehitys (esim. PolicyMaker, Ponder ja Kaos [BFL96, DDLS01, UBJ04]) on mahdollistanut luottamustiedon analyysin osittaisen automaation, kun esimerkiksi tietyt toiminnot on voitu sallia ennalta asetetuille käyttäjäryhmille erityisten ehtojen täyttyessä. Ehdot voivat tällöin liittyä esimerkiksi toiminnon riskin tai tärkeyden muutoksiin järjestelmän tilan muuttuessa. Maine kuitenkin ilmaistaan yhä korkeintaan käyttäjien ryhmittelyn ja roolien kautta, eikä sitä päivitetä automaattisesti kokemusten kertyessä.

Mainejärjestelmät keräävät ja analysoivat mainetietoa [RZFK00]. Niiden avulla käsityksen muodostaminen mainejärjestelmän tuntemista käyttäjistä nopeutuu, koska pohjana käytetään omien kokemusten lisäksi muiden käyttäjän kanssa vuorovaikuttaneiden kokemuksia. Omia kokemuksia ei tarvita välttämättä lainkaan, kunhan luottamus mainejärjestelmän levittämän tiedon laatuun on riittävän vahva. Mainejärjestelmät eivät kuitenkaan yleisesti ota kantaa luottamuspäätöksen muihin tekijöihin, kuten toiminnon riskiin, vaan tukevat yhtenä tiedonlähteenä päätöksen tekemistä toisaalla. Päätös delegoidaan nykyjärjestelmissä useimmin ihmiselle, mutta tehtävän voisi siirtää myös luottamuksenhallintajärjestelmälle.

Luottamuksen tutkimus on vähitellen levinnyt puhtaan pääsynhallinnan ja todentamisen ongelmien ratkomisesta käsittelemään laajempia kokonaisuuksia, kuten luottamustiedon ylläpitoa [RK05]. Eurooppalainen SECURE-projekti pyrkii kehittämään laskennallisen mallin luottamukselle, sen muodostukselle, päivitykselle ja levitykselle sekä lopulta rakentaa sovelluskehyksen luottamuksenhallinnan tueksi [CGS⁺03]. Projektin termi ”luottamus” sisältää myös maineen merkityksen. Vaikka luottamus on varsin subjektiivista, eikä luottamussuhde yleisessä tapauksessa ole transitiivinen, mainetiedoista voi hyötyä muikin yhteisö omaa käsitystään kehittäessään.

3 Luottamus TuBE-projektissa

Helsingin yliopistolla vuonna 2004 alkaneen Trust Based on Evidence (TuBE) -projektin tavoitteena on tukea luottamuksenhallintaa web-palveluympäristössä. Tutkimusaihe kattaa luottamussuhteen elinkaaren sen luomisesta luottamuspäätöksiin ja jatkoseurannasta maineen käsittelyyn sekä tarvittaessa suhteen päättämiseen. Luottamuspäätökset vaikuttavat paitsi toiminnon sallimiseen sellaisenaan, myös järjestelmän käyttäytymiseen. Kielteinen luottamuspäätös voidaan joissakin tapauksissa muuttaa myönteiseksi ottamalla käyttöön riskiä pienentäviä varotoimenpiteitä, kuten tarkkailun tehostaminen tai luottamuksen kohteen käytettävissä olevien resurssien rajoitus.

Suunniteltu luottamuksenhallintajärjestelmä ottaa huomioon luottamuksen riippuvuuden arvioitavasta toiminnasta: puolittuntemattoman asiakkaan voidaan sallia esimerkiksi tekevä kyselyjä saatavilla olevista lennoista, mutta lentolippujen tilaaminen laskulla vaatii luottamuksen kehittymistä pidempiaikaisessa asiakassuhteessa. Päätöksessä arvioitava riski ja tärkeys ovat toimintokohtaisia. Lisäksi toimijan maine kehittyy toimintokohtaisesti, sillä esimerkiksi kumppanijohdellin yhteistyökyky yksittäisten huoneiden varaamisessa ei suoraan osoita, että kyseinen hotelli olisi ammattitaitoinen suurkonferenssin pitopaikana.

Luottamuspäätöstä varten selvitetään luottajan ja luottamuksen kohteen identiteetti ja toiminto mahdollisine parametreineen. Päätöksessä käytetään välillisesti myös ajan hetkeä, järjestelmän päätöksenaikaisen tilan muodossa. Toimijoiden tunnistaminen tapahtuu järjestelmän ulkopuolella. Pitkäikäinen identiteetti on tärkeä maineen kehittymisen kannalta, joten mainejärjestelmä toimii parhaiten henkilöllisyyden todentavien, esimerkiksi X.509-standardin mukaisten varmenteiden ollessa käytössä. Edellä mainitut tekijät määrittävät kohteen maineen, toiminnon riskin ja tärkeyden sekä muun kontekstin, joiden perusteella lopullinen päätös tehdään valitun, arvoja vertailevan politiikan avulla. Kontekstia edustavat erilaisia tilanteita ja ylimääräisiä ehtoja varten asetettavat väliaikaispolitiikat, jotka vaikuttavat maine-, riski- ja tärkeysarvoihin.

Web-palveluympäristössä toiminnoksi tulkitaan yksi palvelua pyytävä SOAP-standardin mukainen viesti tai joukko yhteenkuuluvia viestejä. Palvelusovelluksen ja sen käyttäjän välillä on sovelluskääre (engl. wrapper), joka sieppaa viestin ja tekee luottamuspäätöksen edellä mainittujen tietojen pohjalta. Mikäli päätös on myöntävä, viesti välitetään sovellukselle. Kääre vastaa myös tilannetietojen välittämisestä sovellustason tietomurtohälyttimelle (IDS, Intrusion Detection System), jonka analyysin pohjalta tehdään mainepäivityksiä. Tarvittaessa epäilyttävään toimintaan reagoidaan myös välittömästi, kääreelle tehtävän ilmoituksen avulla.

4 Yhteenveto

TuBE-projekti tutkii luottamusta ja sen hallintaa web-palveluympäristössä. Luottamukseen vaikuttaviksi tekijöiksi on eritelty luottaja itse, luottamuksen kohteena oleva toimija ja tämän maine, suoritettava toiminto, toimintoon liittyvä riski ja sen tärkeys sekä konteksti, jossa päätös tehdään. Päätös riippuu myös ajasta, sillä joidenkin edellä lueteltujen tekijöiden arvot voivat muuttua ajan myötä.

TuBE-projektin luottamusmallissa on kiinnitetty huomiota muuttuviin tilanteisiin reagointiin myös jokseenkin verkkaisten mainepäivitysten ulkopuolella. Konteksti on käsitteenä mukana joissakin luottamusmalleissa, mutta sen käyttö päätösten automatisointiin tähtäävässä luottamuksenhallinnassa on ollut vähäistä. Resurssien rajoitus ja muut järjestelmän toiminnan muutokset parantavat niin ikään reaktiomahdollisuuksia. Luottamukseen liitettyinä ne lisäävät pääsynhallinnan joustavuutta.

Kiitokset

TuBE-projektia ovat rahoittaneet TEKES, Nixu ja StoneSoft.

Viitteet

- [BFL96] Blaze, M., Feigenbaum, J. ja Lacy, J., Decentralized trust management. *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, toukokuu 1996, URL <http://ieeexplore.ieee.org/iel3/3742/10940/00502679.pdf>.
- [CGS⁺03] Cahill, V., Gray, E., Seigneur, J.-M., Jensen, C., Chen, Y., Shand, B., Dimmock, N., Twigg, A., Bacon, J., English, C., Wagealla, W., Terzis, S., Nixon, P., Serugendo, G. D. M., Bryce, C., Carbone, M., Krukow, K. ja Nielson, M., Using trust for secure collaboration in uncertain environments. *Pervasive Computing*, 2,3(2003), sivut 52–61. URL <http://ieeexplore.ieee.org/iel5/7756/27556/01228527.pdf>.
- [DDL01] Damianou, N., Dulay, N., Lupu, E. ja Sloman, M., The Ponder policy specification language. *Workshop on Policies for Distributed Systems and Networks (Policy2001)*, HP Labs Bristol, osa 1995, tammikuu 2001, sivut 18–38, URL <http://www.springerlink.com/link.asp?id=1r0vn5hfxk6dxebb>.

- [MMH02] Mui, L., Mohtashemi, M. ja Halberstadt, A., A computational model of trust and reputation. *35th Annual Hawaii International Conference on System Sciences (HICSS'02)*, osa 7. IEEE Computer Society, tammikuu 2002, URL <http://csdl.computer.org/comp/proceedings/hicss/2002/1435/07/14350188.pdf>.
- [RK05] Ruohomaa, S. ja Kutvonen, L., Trust management survey. *Proceedings of the iTrust 3rd International Conference on Trust Management, 23–26, May, 2005, Rocquencourt, France*. LNCS 3477, Springer-Verlag, 2005. Odottaa julkaisua.
- [RZFK00] Resnick, P., Zeckhauser, R., Friedman, E. ja Kuwabara, K., Reputation systems. *Communications of the ACM*, 43,12(2000), sivut 45–48. URL <http://doi.acm.org/10.1145/355112.355122>.
- [UBJ04] Uszok, A., Bradshaw, J. M. ja Jeffers, R., KAoS: A policy and domain services framework for grid computing and Semantic Web services. *Proceedings of the iTrust 2nd International Conference on Trust Management, Oxford, UK*. LNCS 2995, Springer-Verlag, toukokuu 2004, sivut 16–26, URL <http://www.springerlink.com/link.asp?id=7vhae09p5251153c>.