Luottamuksenhallinta avoimissa palveluverkoissa

Sini Ruohomaa, Lea Kutvonen
Helsingin yliopisto
Tietojenkäsittelytieteen laitos
sini.ruohomaa@cs.helsinki.fi, lea.kutvonen@cs.helsinki.fi

Tiivistelmä

Yritysten välinen yhteistyö avoimessa palveluverkossa on yleistymässä. Luottamuksenhallinta tukee yhteistyötä ja edistää riskien hallintaa tilanteissa, joissa kumppanien väliset suhteet syntyvät ja katoavat varsin nopeasti. Palvelun laadun ja palveluntarjoajan luotettavuuden arvioimiseksi omiin kokemuksiin liitetään maineverkoston kautta myös muiden sen jäsenien kokemuksia, jolloin koko verkosto voi oppia joidenkin jäsentensä virheistä. Luottamuksenhallintajärjestelmä tuottaa paikallisen tiedon ja maineverkostosta saadun kokemuksen pohjalta tilannesidonnaisia luottamuspäätöksiä. Helsingin yliopiston tietojenkäsittelytieteen laitoksen TuBE-projekti (Trust Based on Evidence) tutkii luottamuksenhallintaa web-palveluympäristössä.

1 Johdanto

Luottamus on tärkeä osa ihmisten ja yritysten välistä kanssakäyntiä. Avoimessa palveluverkossa autonomiset toimijat ovat ennalta-arvaamattomia, ja keskitetyn hallinnan puute aiheuttaa haasteita yhteensopivuudelle ja riskinhallinnalle. Palveluita verkossa tarjoava yhteistyöhaluinen organisaatio joutuu avaamaan osan järjestelmästään ulkopuolisille; kumppaneille tai asiakkailleen. Perinteiset tietoturvamekanismit perustuvat järjestelmän sulkemiseen tuntemattomilta ja tunnettujen, "luotettujen" toimijoiden minimaaliseen valvontaan. Tämän lähestymistavan vastapainoksi avoimeksi tarkoitetut järjestelmät tarvitsevat mekanismeja riskin ja luottamuksen tasapainottamiseksi tilanteen mukaan.

Epävarmuutta ja siihen liittyvää riskiä voi vähentää varotoimin, kuten tarkalla valvonnalla tai vaatimalla palvelun käyttäjiltä erilaisia vakuuksia. Täydellistä hallintaa ei kuitenkaan voida saada aikaan, ja riskiä pienentävät rajoitukset voivat myös hankaloittaa palvelun käyttöä liiaksi. Täten myös palveluntarjoaja tarvitsee pehmeitä turvamekanismeja [9], kuten luottamusta, jäljelle jääneen epävarmuuden vastapainoksi.

Luottamuksenhallinnan automatisointi nousee keskeiseksi yhteistoiminnan lisääntyessä ja rutiininomaisia luottamuspäätöksiä vaativien tilanteiden yleistyessä. Helsingin yliopistolla vuonna 2004 alkaneen Trust Based on Evidence (TuBE) -projektin tavoitteena on tukea luottamuksenhallintaa web-palveluympäristössä. Tutkimuksen kohteena on luottamussuhteen koko elinkaari sen luomisesta tilannekohtaisiin luottamuspäätöksiin, jatko-

seurannasta maineen käsittelyyn ja tarvittaessa suhteen päättämiseen.

Yritysten välisessä yhteistoiminnassa luottamuksenhallinta liittyy läheisesti sopimusten neuvotteluun, niiden toteutumisen valvontaan sekä sopimusrikkeisiin reagointiin. Kehitettävä luottamuksenhallintajärjestelmä liittyy osaksi web-Pilarcos-projektissa kehitettyä väliohjelmistoa [13], joka tukee yritysten tietojärjestelmien yhdistämistä suuremmiksi kokonaisuuksiksi, liiketoimintaverkostoiksi. Väliohjelmiston toimintoihin kuuluu myös muun muassa tarjottujen liiketoimintapalveluiden yhteensovitus toimivaksi, mallin mukaiseksi verkostoksi sekä niiden yhteentoimivuuden dynaaminen varmistaminen. Järjestelmään tallennettaviin sähköisiin sopimuksiin sisältyy kuvaus hyvitysprosessista sopimusrikkeen tapahtuessa. Yksi hyvitysprosessin käynnistävä tekijä on luottamuksen puutteesta johtuva toiminnan keskeyttäminen.

Luottamuksen määritelmät vaihtelevat kirjallisuudessa sovelluksen mukaan. Me määrittelemme luottamuksen *halukkuudeksi sallia annetun kumppanin tietty toiminta, kun huomioidaan sallimisen houkuttimet ja riski sekä kumppanin maine päätöshetkellä*. Luottamus on sidottu tahtoon ja tietoiseen päätökseen luottaa tai olla luottamatta. Sen taustalla on kokemukseen perustuva omakohtainen käsitys kumppanin pyrkimyksistä ja normeista, eli tämän maine. Luottamuksenhallinta kerää luottamukseen liittyvää tietoa, analysoi sitä ja tuottaa sen pohjalta tilannesidonnaisia luottamuspäätöksiä. Päätöksillä voidaan tukea palvelun tarjoajan ja käyttäjän välistä vuorovaikutusta.

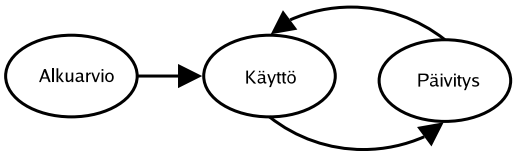
Tämä artikkeli esittelee luottamuksenhallintaa ja sen toteutusta TuBE-projektissa. Luku 2 kuvaa luottamuksenhallinnan taustaa. Luku 3 määrittelee TuBEn luottamusmallin, ja luku 4 kuvaa mallin toteuttavan järjestelmän. Luku 5 havainnollistaa järjestelmän toimintaa osana Web-Pilarcos-väliohjelmistoa tapauskuvauksen kautta.

2 Luottamuksenhallinnan taustaa

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 [2, 4, 15]) 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. Luottamus ilmaistaan kuitenkin yhä korkeintaan käyttäjien ryhmittelyn ja roolien kautta, eikä sitä päivitetä automaattisesti kokemusten kertyessä.

Keskeinen edistysaskel luottamuksenhallinnan tutkimuksessa on ollut luottamuksen dynaamisen luonteen huomioon ottaminen. Tällöin luottamuspäätös rakennetaan aluksi esitietojen varaan, mutta sitä päivitetään käytön aikana saadun kokemuksen perusteella. Kuva 1 esittää tämän palautesyklin luottamuksen käytön ja päivityksen välillä. Luottamuksen kohdet-



Kuva 1: Luottamustiedon elinkaari.

ta ja kokemusta tästä kuvataan mainetiedolla. Mainetiedon lisäksi myös paikalliset riski- ja tärkeysarvotukset voivat muuttua ajan kuluessa, mutta tämä tapahtuu eri mekanismien kautta.

Mainejärjestelmät keräävät ja analysoivat mainetietoa [10]. 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 luottamuksenhallintajärjestelmien kehitys mahdollistaa päätöksenteon siirtämisen niille. Automaatio sopii erityisesti rutiininomaisille päätöksille, joita joudutaan tekemään usein. Rajatapausten ja poikkeuksien käsittelijänä ihminen on yhä varsin korvaamaton.

Luottamuksen tutkimus on vähitellen levinnyt puhtaan pääsynhallinnan ja todentamisen ongelmien ratkomisesta käsittelemään laajempia kokonaisuuksia, kuten luottamustiedon ylläpitoa [11]. Eurooppalainen SECURE-projekti on kehittänyt laskennallista mallia luottamukselle, sen muodostukselle, päivitykselle ja levitykselle sekä lopulta rakentanut sovelluskehystä luottamuksenhallinnan tueksi [3]. Projektin termi “luottamus” sisältää myös maineen merkityksen. Vaikka luottamus on varsin subjektiivista, eikä luottamussuhde yleisessä tapauksessa ole transitiivinen [1], mainetiedoista voivat hyötyä muutkin yhteisön jäsenet omaa käsitystään kehittäessään.

3 Luottamusmalli

TuBE-projektin mallissa uottamuspäätös johdetaan seitsemästä tekijästä: luottaja, luottamuksen kohde, toiminto, kohteen maine, riski, tärkeys ja konteksti. Kukin *luottaja* tekee omakohtaisen päätöksen tiettyyn toimintaan osallistumisesta, ja toistaa prosessin dynaamisen päätöksen luomiseksi aina kun yhteistyössä kohdataan riskinhallinnan kannalta relevantti sitoumuspiste, jota vastaa *toiminnon* käsite. Luottamuspäätös tehdään liiketoimintaverkostoa koottaessa kunkin toimijan osalta, ja verkon toiminnan aikana aina tarpeen mukaan. *Luottamuksen kohde* on luottajan tapaan palveluntarjoaja, joka on liittymässä liiketoimintaverkostoon tai toimii siinä. Luottaja ja luottamuksen kohde voivat molemmat toimia verkostossa sekä palveluntarjoajina että käyttäjinä, ja luottamuspäätökset voivat siten kohdistua sekä palvelun säätelyyn että sen käyttötapaan kuhunkin liittyvien sitoumuksista ja riskeistä riippuen.

Luottamuksen *kohteen maine* on ko-

kemukseen perustuva käsitys, jonka pohjalta ennakoidaan tämän käyttäytymistä jatkossa. Maine kootaan omakohtaisen kokemuksen lisäksi muiden saatavilla olevien toimijoiden kokemuksesta. Tiedon kokoamista käsitellään luvussa 4.2. Maine vaikuttaa myös tilanteesta tehtävään riskianalyysiin.

Riski on taktinen analyysi myöntävän luottamuspäätöksen mahdollisista ja todennäköisistä seurauksista. Analyysi yhdistää hyödyt ja haitat eri lopputuloksista, ja erottelee tuloskategoriat todennäköisyyksineen eri suojattavien kohteiden välille. Analyysin tuloksena voidaan esimerkiksi pitää erittäin todennäköisenä, että seurauksena on pienehkö rahallinen hyöty, lievä isku turvallisuudelle ja positiivinen vaikutus luottajan omaan maineeseen. Riskin sieto ja siten päätöksen tulos riippuu sietopolitiikasta, johon liittyy dynaamisena tekijänä toiminnon tärkeys.

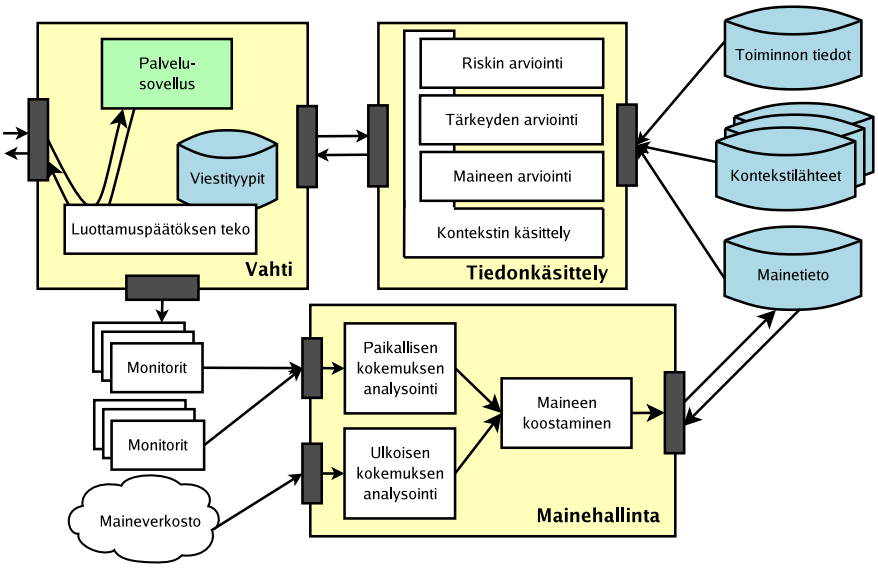
Tärkeys kuvaa toiminnon strategista merkitystä, ja edustaa kieltävän luottamuspäätöksen haittoja suhteessa myönteiseen. Nämä haitat eivät riipu vastapuolen mahdollisesta toiminnasta, joten ne eivät liity riskiarvioon. Tärkeyteen vaikuttavat esimerkiksi solmitun sopimuksen hyvitysmääräykset, jotka aktivoituvat mikäli toiminnasta päätetään vetäytyä ennenaikaisesti. Tärkeyttä lisäävät myös oman yrityksen palvelualttiin maineen ylläpitäminen ja hyvän partnerisuhteen rakentamistarpeet toimijan mahdollisesta käytöksestä huolimatta. Tällaisia valintaa rajaavia ristiriitoja esiintyy esimerkiksi pienten alihankkijoiden suhteissa suuriin yrityksiin.

Konteksti edustaa väliaikaisia, tilanteesta johtuvia muutoksia edellä kuvattuihin tekijöihin. Kontekstitieto saadaan kolmesta erityyppisestä lähteestä: yhteisön, yrityksen ja järjestelmän tilasta. Yhteisön tila vaikuttaa kaikkiin yhteisössä toimijoihin. Esimerkiksi yhteistyön alku- tai loppumisvaiheessa voidaan priorisoida tiettyjä toimintoja ja tulkita jotkut vähemmän tärkeiksi. Yrityksen tila kuvaa paikallisia, liiketoiminnallisia muutoksia. Esimerkiksi varastotilan puute voi lisätä myyntitoimintojen tärkeyttä, ja määräaikainen vakuutus pienentää tiettyjä riskejä, mahdollisesti yhteistyökumppanista riippuen. Järjestelmän tila kuvaa paikallisen järjestelmän vaikutusta: havaittu palvelunestohyökkäys vaikuttaa riskianalyysiin, kuten myös päätös tarkkailla uutta partneria tarkemmin.

Järjestelmän toiminnan kannalta verkoston jäsenten identiteetin pitkäkestoisuus on tärkeää, sillä maineen kertyminen ja huonon maineen rankaiseva vaikutus perustuvat toimijoiden tunnistamiseen. Helposti vaihdettavat identiteetit aiheuttavat lisähaasteita monissa maine- ja luottamusjärjestelmissä, koska huonoa mainetta voi tällöin paeta uuden identiteetin taakse, ja äänestysten reiluuden varmistaminen vaikeutuu. Koska liikeyritysten välillä solmitaan sopimuksia, niiden on joka tapauksessa voitava yhdistää partnerin tunniste verkossa todelliseen yritykseen, joten oletamme että käytössä on esimerkiksi X.509-standardin mukainen varmennejärjestelmä.

4 Luottamuksenhallintajärjestelmä

TuBE-projektin luottamuksenhallintajärjestelmällä on kaksi tehtävää luottamussuhteen elinkaaren mukaisesti: luottamuspäätösten tuottaminen käyttäen senhetkistä luottamustietoa, ja tietojen päivittäminen [12]. Järjestelmän jakautuminen alijärjestelmiin on esitetty kuvassa 2. Vahtialijärjestelmä valvoo viestiliikennettä palvelusovelluksen ja ulkomaailman välillä,



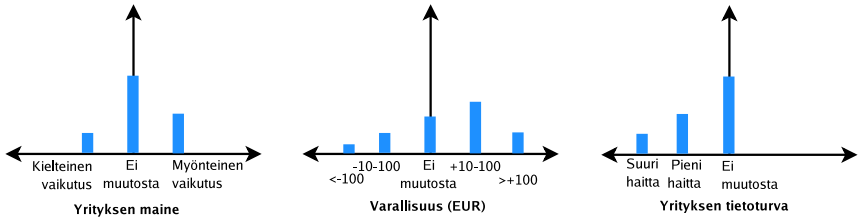
Kuva 2: Luottamuksenhallintajärjestelmän yleiskuva. Palvelukutsut ja vastaukset ohjataan vahtialijärjestelmän läpi.

ja tunnistaa luottamuspäätöskohdat viestityyppien perusteella. Tiedonkäsittelyn alijärjestelmä käyttää vahdilta saamiansa parametrejä ja paikallisia tietovarastoja laskeakseen oikeat arvot luottamuspäätöksen tekijöille, joiden pohjalta vahti tekee päätöksen paikallisen politiikan mukaan. Mainetiedon päivitys tapahtuu paikallisen valvonnan ja maineverkostosta saatavan täydentävän, ulkoisen kokemustiedon pohjalta mainehallinnan alijärjestelmässä.

4.1 Luottamuspäätösten tuki

Vahtialijärjestelmä koostuu palvelun viestiliikennettä valvovasta kääreestä ja luottamuspäätösmekanismista, joka tuottaa luottamusmallin mukaisista tekijöistä luottamuspäätöksen. Saapuvat ja lähtevät viestit liittyvät tyyppinsä puolesta tiettyyn toimintoon, jonka päätöspiste määritetään tietyn viestityypin kohdalle. Tällainen viesti voi olla saapuva palvelupyyntö parametreineen tai esimerkiksi palvelun vastaus, jossa se sitoutuu tuotteen toimittamiseen tilaajalle. Kun viestinvaihdosta kootut toiminnon keskeiset parametrit ja luottamuksen kohde ovat tiedossa, vahti pyytää luottamuspäätökseen tarvittavat tiedot niiden perusteella tiedonkäsittelyn alijärjestelmältä.

Tiedonkäsittelyn alijärjestelmä kokoaa laskukaavojen perusteella tilanteelle arvioidun riskin, tärkeyden ja luottamuksen kohteen maineen. Toiminnon riski- ja tärkeysanalyysille saadaan pohja kunkin toiminnon tiedot sisältävästä tietojärjestelmästä. Tärkeysarviota korjataan kontekstia edustavien muokkaussääntöjen perusteella, riskin korjaukseen käytetään lisäksi toimijan mainetietoa. Lopputuloksena on riskianalyysi ja sen sietoalue, joista edellinen perustuu riski- ja mainetietoihin ja jälkimmäinen toiminnon tärkeystietoihin.



Kuva 3: Kohdekohtainen riskianalyysi eri seurausten todennäköisyydestä.

Lopullinen luottamuspäätös palautuu vahtialijärjestelmälle. Mikäli päätös on selvä, se voidaan toteuttaa välittömästi: joko viesti välitetään tavalliseen tapaan eteenpäin tai se pysäytetään ja tarpeen mukaan viestitään palvelusovellukselle toipumistarpeesta toiminnon peruuntuessa.

Riskianalyysin ja toiminnon tärkeyden ilmaisumuotoa ei ole sidottu järjestelmässä, sillä politiikat ohjaavat tulkintaa. Ensimmäistä prototyyppiä varten luotu riski- ja tärkeystekijän malli esittää riskin joukkona todennäköisyyksiä eri vaikutuskategorioille, ja tärkeyden joukkona rajoituksia näille todennäköisyyksille.

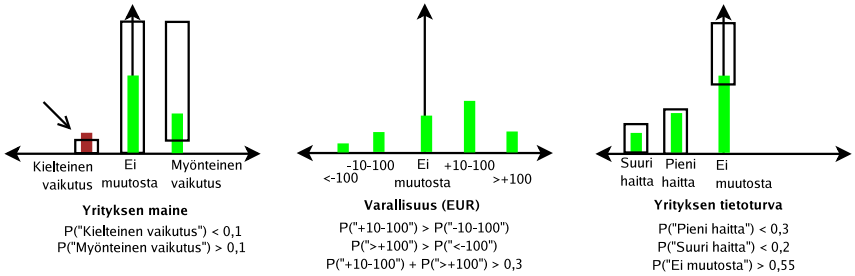
Esimerkiksi toiminnon sallimisella voidaan arvioida olevan yrityksen maineelle kielteinen vaikutus todennäköisyydellä 0,15, myönteinen vaikutus todennäköisyydellä 0,25 ja ei vaikutusta todennäköisyydellä 0,6. Kuvassa 3 on esimerkkiarvio toiminnon sallimisen vaikutuksista kolmelle suojattavalle kohteelle (maine, varallisuus ja tietoturva). Vaikutuskategoriat jakautuvat x-akselille, kun taas y-akseli kuvaa kunkin tuloksen todennäköisyyttä.

Kuvassa 4 on esimerkki arvion yhdistämisestä toiminnan tärkeydestä johdettuihin rajoituksiin. Toiminnon vaikutukselle yrityksen maineelle on määritetty yksinkertaiset rajat: kielteisen tuloksen todennäköisyyden tulee olla alle 0,1, kun taas myönteisen vaikutuksen todennäköisyyden on ylitettävä kyseinen arvo. Tässä kielteisen vaikutuksen todennäköisyys 0,15 ylittää annetun rajan, jolloin vahtialijärjestelmässä esimerkiksi politiikalla “kaikki rajoitteet täytyttävä” luottamuspäätös olisi kieltävä.

Uskomme eri kohteiden käsittelyn erikseen olevan järjestelmään tietoja ja rajoitteita syöttävälle ihmiskäyttäjälle luontevampaa kuin esimerkiksi kaikkien vaikutusten tulkitsemisen rahallisiksi menetyksiksi tai eduiksi, kuten SECUREn [3] riskimallissa. Klassinen esimerkki yhteen vakavuusasteikkoon perustuvan riskianalyysin ongelmallisuudesta on rahallisen hinnan asettaminen inhimilliselle kärsimykselle.

Ihmisen hahmotuskykyyn ja järjestelmän käytettävyyteen perustuen päätimme myös jakaa kunkin kohteen asteikot erillisiksi rypäiksi jatkuvan arvoasteikon sijaan. Vaikka tarkat arvot ovat joissakin tilanteissa arvokkaita, ei riskianalyysin kannalta merkityksellisiä siirtymiä ilmene jokaisella alivälillä. Rahallisten voittojen tai menetysten arviointi on lisäksi jokseenkin poikkeustapaus, sillä useimpiin kohteisiin kohdistuvia vaikutuksia ei voi kuvata niin tarkasti, että jatkuvan asteikon käyttö olisi järkevää.

SECUREn riskianalyysimalli pohjautuu tiedolle kaikkien mahdollisten lopputulosten erillisistä hinta/hyöty-



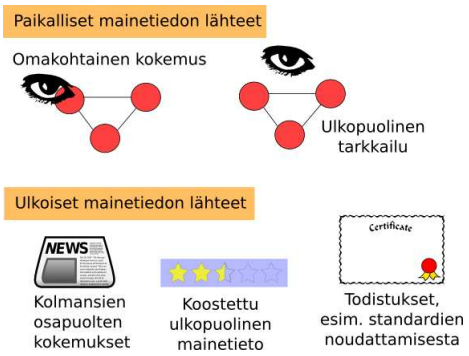
Kuva 4: Riskin ja tärkeydestä johdettujen rajotteiden vertaaminen. Rajoitteensa rikkova arvo on merkitty nuolella.

analyysistä, jotka yhdistetään lopulliseksi analyysiksi luottamuspäätöstä tehtäessä. TuBEn mallissa kokemusta käytetään eri vaikutusten todennäköisyyksien määrittämiseen, ja lopputulosten luokittelu perustuu yksin näille vaikutuksille. Esimerkiksi myöhästynyt tuote ja hieman kolhiintunut, ajoissa saapunut tuote ovat kaupankäynnin lopputuloksina samanveroisia, jos ja vain jos niiden vaikutusten yrityksen omaan maineeseen, varallisuuteen ja muihin kohteisiin arvioidaan olevan samat. Tässä mallissa mahdollisia lopputuloksia ei tarvitse tuntea ja luokitella etukäteen, kunhan niiden vaikutukset kyetään ilmaisemaan järjestelmän ollessa käynnissä. Yritysten välisessä yhteistyössä joustavuus on tarpeen, sillä toiminnan monimutkaistuessa mahdollisten lopputulosten määrä kasvaa nopeasti.

4.2 Mainetiedon ylläpito

Kun vahtialijärjestelmä tarkkailee viestiliikennettä, se välittää tietoa monitoreille. Kukin sovellustason monitori tarkkailee tiettyjä piirteitä viesteistä, syntaktisista ominaisuuksista semanttisiin. Kaikki monitorit eivät etsi uhkia; jonkin monitorin tehtävä voi olla toiminnon valmistumisen tunnistaminen, jotta toimintoon liittyvän kokemuksen analysointi voidaan saada käyntiin. Monitorit toimivat toisistaan riippumatta, ja niiden väliset painotuserot sekä poissulkeminen ratkaistaan mainehallinnan alijärjestelmässä paikallisen kokemuksen analysointikomponentissa. Paikallista kokemusta voidaan saada myös välittömän teknisen ympäristön ulkopuolelta. Ulkoinen tiedonlähde voi olla esimerkiksi fyysisen tavarantoimituksen vastaanottaja tai vastaanottajan raportti yrityksen toimitustietojärjestelmässä. Sovelluksen viestinvaihdon valvonta ei tällöin yksin riitä, sillä tilauksen kulusta ei voida arvioida, saapuiko luvattu tuote ajallaan ja kunnossa.

Paikallinen kokemus on luotettavaa ja varmimmin asiaankuuluvaa, mutta kallista kerätä. Huijarit ja ammattitaidottomat yhteistyön tarjoajat tulisi voida erotella jo ennen ensimmäisen projektin kokeilemista. Tätä varten käytetään ulkoista kokemusta, jota saadaan maineverkoston kautta. Nykyiset luottamuksenhallintajärjestelmät olettavat useimmiten yhden, jokseenkin maailmanlaajuisen mainejärjestelmän olevan käytössä; usein mainejärjestelmä rakennetaan kiinteäksi osaksi luottamuksenhallintajärjestelmää. Toisaalta mainejärjestelmien tutkimus on vasta siirtymässä matalan riskin ympä-



Kuva 5: Mainetiedon lähteet.

ristöistä, kuten tiedostonjakojärjestelmistä [6], yritysten väliseen toimintaan [8]. Lisäksi olemassaolevia yrityksiä koskevia tietojärjestelmiä on lukuisia ja ne vastaavat eri tarpeisiin: esimerkiksi Dun & Bradstreet, World Trade Organization ja Bolero [14].

Uskomme että paras tulos saadaan tällä hetkellä käyttämällä useampaa kuin yhtä tietojärjestelmää myös mainetiedon keruuseen. Järjestelmistä tulevat tiedot kulkevat maineverkoston kautta ulkoisen kokemustiedon analysointikomponentille, joka painottaa tiedot suhteessa toisiinsa ja voi analysoida tarpeen mukaan tietojen uskottavuutta, mikäli mainejärjestelmä ei itse tarjoa kyseistä palvelua.

Mainetiedon eri lähteet on koottu kuvaan 5. Näistä keskeisimpiä sovellusalueellamme ovat omakohtainen kokemus, kolmansien osapuolten kokemukset sekä todistukset. Koostettu ulkopuolinen mainetieto on tiivistetty kokemuksista, joten sen oikeellisuutta on vaikeampi arvioida. Toisaalta käytännön syistä yksittäisten kokemusten sijaan mainejärjestelmissä välitetään usein koostearvoja muun muassa tarvittavan viestiliikenteen rajoittamiseksi. Ulkopuolinen tarkkailu kokemuksen keräämiseksi on luottamusksenhallintajärjestelmästä käsin hankalaa, mutta monitorien kautta voidaan syöttää myös tällaista tietoa, mikäli sitä on järjestelmän ulkopuolelta saatu.

Omakohtaiset ja ulkoiset kokemus- ja koostetut mainetiedot karsitaan ja painotetaan kukin omassa analyysikomponentissaan, ja syötetään paikallisen mainekäsityksen koostavalle komponentille. Tämä komponentti vertaa saatua uutta tietoa nykyisiin ja päivittää mainetietokantaa paikallisen politiikan mukaisesti. Politiikka määrittää erityisesti vanhan tiedon painotuksen suhteessa siihen lisättävään uuteen tietoon.

Ulkoisen mainetiedon käytössä on haasteita, joista suurin lienee tiedon oikeellisuuden ja asianmukaisuuden arviointi. Maineverkoston toimijat ovat autonomisia ja ajavat omaa etuaan siinä missä niiden arvioinnin kohteetkin. Lisäksi niiden oikeellistenkin kokemusten kohde voi olla sopimaton: esimerkiksi sama palveluntarjoaja voi tarjota kahta hyvin erilaista palvelua, joista edullisemmalla se kerää positiivista mainetta mutta toimii hyvin epäilyttävästi enemmän resursseja vaativan palvelun tarjoamisessa. Esimerkiksi verkkohuutokauppa eBayn [5] kontekstissa kokemuksen asianmukaisuus

riippuu myydyn esineen hinnasta: järjestelmä pitää nappikauppaa ja käytetyn auton myymistä samanarvoisina kokemustilastoja kootessaan, mutta auton ostoa harkitsevan käyttäjän kannattaisi ehdottomasti keskittyä tarkastelemaan kokemuksia arvokaupoista.

Toinen mainetiedon keräämistä hankaloittava haaste on osallistumisen arvostus. Käyttöönotetut, yksityishenkilöille suunnatut mainejärjestelmät ovat yllättäneet tutkijat toimimalla käytännössä varsin hyvin, vaikka teoreettisessa analyysissä mekanismin onkin arveltu olevan ongelmallinen [10]. Esimerkiksi hyvää palvelua antavan yrityksen maineen kasvattaminen voi olla opportunistisen toimijan intressien vastaista, mikäli sen seurauksena palvelun kysyntä kasvaa siinä määrin että sen saatavuus vaikeutuu; tietoa toimivasta yhteistyösuhteesta ei välttämättä haluta jakaa, vaan mieluummin säilytetään lähes yksinoikeus hyvää palvelua tarjoavaan kumppaniin.

Tässä maineen oletetaan vaikuttavan palveluntarjoajan valintaan yhteensopivien ehdokkaiden joukosta, mikä toteutuu esimerkiksi tiedostonjakojärjestelmissä tai lapsenvahtien etsinnässä. Lisäksi yritysten kilpailusuhteet aiheuttavat mielenkiintoisia haasteita maineen keruulle. Saman toimenkuvan palveluntarjoajat saavat epäilemättä toistensa kannalta erityisen asianmukaisia kokemuksia, mutta niiden intressi auttaa toisiaan jakamalla tätä tietoa jäänee hyvin rajoittuneeksi.

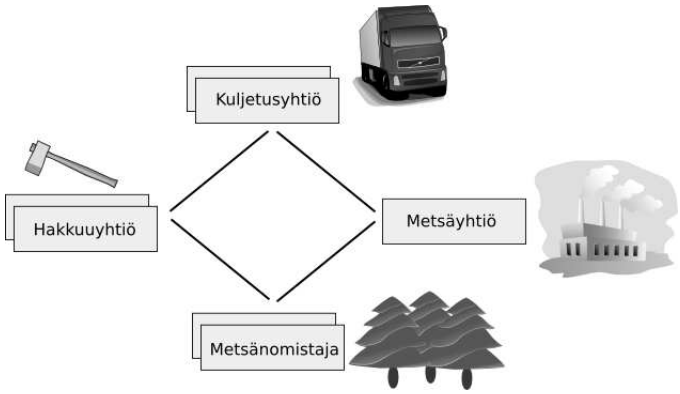
5 Tapauskuvaus

Järjestelmän toimintaa voidaan havainnollistaa puuteollisuuteen sijoittuvan tapauskuvauksen kautta. Puutavaran toimitus metsästä tehtaalle vaatii neljän toimijatyypin välistä yhteistyötä. Hakkuuyhtiö kaataa sovitun alueen metsänomistajan metsää, kuljetusyhtiö kuljettaa puutavaran metsäyhtiön omistamalle tehtaalle. Metsäyhtiö maksaa hyvityksen tavarasta metsänomistajalle, joka maksaa hakkuuja kuljetusyhtiölle näiden palveluista. Kuva 6 esittelee yhteistyöasetelman.

Tehtaat omistava metsäyhtiö on usein kooltaan huomattavasti muita toimijoita suurempi, ja käyttää riittävän puutavaran määrän kokoamiseksi useita kunkin muun toimijatyypin edustajaa. Jos metsäyhtiö myös koordinoi toimintaa keskitetysti, se voi sanella käytettävän toimintaympäristön, kuten tiedon välittämiseen käytettävät tietojärjestelmät. Toimijat voivat myös pysyä itsenäisinä ja varmistaa eri järjestelmien yhteentoimivuuden kokoamalla tarvittavat viestinvaihdot webpalveluiksi. Tällöin myös useiden eri yhteistyökumppanien käyttö helpottuu, jolloin toimijat eivät jää riippuvaiseksi yksittäisestä kumppanista ja tämän toiminnan jatkumisesta. Esimerkiksi metsänomistaja voi järjestää tarjouskilpailun, jossa se hakee kulloinkin edullisimman mahdollisen kumppaniyhdistelmän tietyn metsäalueen hyödyntämiseksi, ja hakkuuyhtiö voi tarjota palveluksiaan yhtä aikaa useissa yhteistyöverkostoissa.

Toimijoiden roolit, suhteet ja kunkin palvelun toiminnalliset vaatimukset kuvataan liiketoimintaverkostomallina [13]. Kukin toimija muodostaa mallissa kuvattuun rooliin sopivan palvelutarjouksen, ja julkaisee sen tallennettavaksi palvelutarjousvarastoon. Yksi toimija voi myös täyttää useita rooleja samanaikaisesti. Hakkuuyhtiö, jolla on käytössään oma kuljetusauto, voi tehdä hakkuulle palvelutarjouksen edullisempaan hintaan asettaen ehdoksi, että kuljetusyhtiön roolin täyttää sen oma kuljetuspalvelu, ja päinvastoin.

Uutta yhteistyöverkostoa etsivä metsänomistaja ilmoittaa julkiselle populaattoripalvelulle haluavansa yhteentoimivan



Kuva 6: Puuteollisuuden toimijoiden yhteistyö.

toteutuksen liiketoimintaverkostomallille, jossa se itse täyttää metsänomistajan roolin omalla palvelutarjouksellaan. Populaattoripalvelu hakee palvelutarjousvarastosta muihin rooleihin sopivat ehdokkaat, ja palauttaa metsänomistajalle yhden tai useamman verkostoehdotuksen. Verkostoehdotusten on täytettävä metsänomistajan antamat sekä muista palvelutarjouksista tulevat lisärajoitukset, esimerkiksi kuljetuksesta tarjotun hyvityksen ja kuljetusyhtiön hinnoittelun tulee täsmätä.

Kun metsänomistaja saa verkostoehdotuksen, se tekee luottamuspäätöksen siitä, haluaako se yhteistyötä tarjottujen kumppanien kanssa. Ehdotuksen tarjousjoukkoon saattaa kuulua hakkuuyhtiö, josta metsänomistajalla on huonoja kokemuksia aikataulussa pysymisen suhteen. Luottamuksenhallintajärjestelmä analysoi kokemusten perusteella riskin ja tärkeyden hakkuuyhtiön ottamiselle mukaan. Jos riski on liian suuri metsänomistajan päätöspolitiikan kannalta, ehdotus hylätään. Metsänomistaja saattaa myös määrittää lisärajoitteita hylkäämättä ehdotusta, jolloin se esimerkiksi voi rajoittaa omassa palvelutarjouksessaan ilmaistua hyvityksen määrää. Kun aloitteen tehnyt metsänomistaja on valmis hyväksymään muokkaamansa ehdotuksen, se lähettää ehdotuksen muille verkoston osapuolille neuvoteltavaksi.

Verkoston muut mahdolliset jäsenet tekevät niin ikään luottamuspäätöksiä mukaan lähtemisestä, ja muokkaavat tarjouksiaan neuvottelujen edetessä. Kun osapuolet ovat päässeet sopimukseen palvelun ehdoista, verkosto käynnistetään. Mikäli yhteisymmärrystä ei synny, metsänomistaja voi pyytää populaattorilta uuden ehdotuksen.

Verkoston aloitteentekijä voi valita ehdotuksista mielestään parhaan neuvoteltavaksi. Paremmuus voi määrittyä luottamusanalyysin lisäksi myös esimerkiksi hinnoittelun perusteella. Nykyiselle populaattoripalvelulle voidaan välittää hyötyfunktio, jonka avulla se voi järjestää palvelutarjouksia paremmuusjärjestykseen. Hyötyfunktiota hyödyntämällä esimerkiksi hinnan mukaan järjestäminen yksinkertaistuu. Sen sijaan luottamuksen perusteella järjestäminen ei suju yhtä luontevasti populoinnin aikana, sillä populaattoripalvelu ei ole riittävän luotettu käsittelemään yksityisiä luottamusarvioita [7]. Jos palvelu kuitenkin järjestää

ehdotukset valmiiksi edullisuusjärjestykseen julkisten tietojen perusteella, aloitteentekijä voi valita ensimmäisten joukosta sen, johon se luottaa riittävästi.

Metsänomistaja on solminut pitkäaikaisen sopimuksen lähialueen kuljetusyhtiön kanssa siitä, että se saa alennetun hinnoittelun tilatessaan siltä tietyn määrän kuljetuksia vuodessa. Se voi ilmoittaa saman tien liiketoimintaverkostoa täytettäessä, että kuljetusyhtiön rooli tulee täyttää tällä palveluntarjouksella. Toisaalta, mikäli alennus ei ole suuren suuri, se voi vain määrittää hyötyfunktiossa kyseisen yhtiön käytön hieman edullisemmaksi. Tällöin jokin parempi tarjous voi ylittää paikallisyhtiön tarjouksen hyötyarvon, jolloin se tulee valituksi ensisijaisesti.

Lopulliseen valintaan luottamuspäätöksen perusteella tähtäävä metsänomistaja on tilannut useita ehdotuksia populaattoripalvelulta, joista edullisimmissa kuljetuksen tarjoaa tuntematon yritys, ja paikallinen yhtiö on vaihtoehtona hieman pienemmän kokonaishyödyn ehdotuksissa. Maltillinen metsänomistaja on asettanut oletuksena tuntemattomille toimijoille asetettavan maineen varsin alhaiseksi, ja se saa maineverkostosta hyvin vähän tietoa uudesta tulokkaasta. Tämän seurauksena luottamusjärjestelmä arvottaa lopulta lähialueen hyvämaineisen kuljetusyhtiön sisältämän ehdotuksen parhaaksi, sillä halvempaan mutta tuntemattomaan kuljetuspalveluun sisältyvät riskit muun muassa koko puulastin menetyksestä ovat suhteessa liian suuret.

Kun liiketoimintaverkosto on käynnissä, kukin toimija valvoo välittömien yhteistyökumppaneidensa toimintaa ja kerää sen perusteella kokemusta paikallisen mainenäkemyksen tueksi. Kaikki verkoston jäsenet eivät kuitenkaan kykene arvioimaan toistensa toimintaa: esimerkiksi hakkuuyhtiö on tekemisissä vain metsänomistajan ja kuljetusyhtiön kanssa toimeksiannon, kuljetuksen ja palkkionmaksun yhteydessä. Se ei tästä syystä saa suoraa kokemusta metsäyhtiön toiminnasta yhteistyöverkoston kautta. Hakkuuyhtiö voi kuitenkin muodostaa mainenäkemyksen metsäyhtiöstä kolmansilta osapuolilta saatujen tietojen perusteella. Paikallinen mainenäkemys tai sen osa, kuten yksittäinen kokemus, raportoidaan maineverkostoon.

Liiketoimintaverkoston toimintaan liittyy kunkin toimijan kohdalla sitoumushetkiä, jolloin voi olla syytä tehdä uusi luottamuspäätös yhteistoiminnan jatkamisesta. Esimerkiksi kuljetusyhtiö voi saman verkoston toiminnan aikana sopia hakkuuyhtiön kanssa useaan kertaan kuljetusautojen lähettämisestä hakkuualueelle hakemaan valmistunut puuerä toimitettavaksi tehtaalle. Mikäli hakkuuyhtiö kutsuu autoja paikalle toistuvasti liian aikaisin ja aiheuttaa täten ylimääräisiä kuluja kuljetusyhtiölle, tämä voi päättää olla hyväksymättä kutsuja jatkossa. Mikäli puuta ei haeta hakkuupaikalta, verkoston toiminta pysähtyy. Täten kuljetusyhtiöllä on kaksi vaihtoehtoa: se voi päättää erota verkostosta itse, tai se voi vaatia hakkuuyhtiön erottamista verkoston toiminnan toistuvan vaikeuttamisen perusteella.

Eroamiseen riittää yksipuolinen päätös, joka saattaa kuitenkin aktivoida verkostosopimukseen kirjattuja hyvitysehtoja. Kuljetusyhtiö voi esimerkiksi joutua luopumaan siihenastisten toimitusten maksuista. Verkoston jäsenen erottamisesta neuvotellaan verkostossa. Mikäli erottamisesta päästään sopimukseen, se astuu voimaan ja sopimuksesta saattaa aktivoitua erottamiseen liittyviä hyvitysehtoja. Hakkuuyhtiö voi olla saanut aikaan edullisen sopimuksen, jossa se saa osan luvatusta palkkiosta myös, jos se erotetaan verkostosta.

Molemmissa tapauksissa verkoston

toiminta keskeytyy, kunnes puuttuvalle paikalle löydetään uusi toimija. Tämä toteutetaan populaattorikutsulla, jossa verkoston roolit on esitäytetty nykyisillä palveluntarjoajilla, lukuunottamatta juuri poistunutta. Mikäli tilalle ei löydy toista palvelutarjoajaa, verkosto hajoaa. Uuden sopivan tarjouksen löytyessä käydään uusi neuvottelukierros, ja sen päättyessä yhteisymmärrykseen verkosto voi jatkaa toimintaansa uudessa muodossaan.

Liiketoimintaverkoston elinkaari jakautuu useisiin vaiheisiin. Merkittävät, elinkaaren vaiheet ovat verkoston pystytys, neuvottelu, verkostoon liittyvien toimintaprosessien suorittaminen ja verkoston alasajo toiminnan jälkeen [13]. Kun verkoston käsittelyn kohteena olleen metsäpalstan puutavara on kaadettu ja toimitettu metsäyhtiölle, sopimuksen mukaisten prosessien suoritus on valmistunut ja verkosto siirtyy alasajovaiheeseen. Metsäyhtiö maksaa puutavarasta kauppahinnan metsänomistajalle, joka välittää sovitut maksut hakkuu- ja kuljetusyhtiöille. Yhteistyöverkosto puretaan ja siihen sidotut resurssit voidaan vapauttaa seuraavaa verkostoa varten.

6 Yhteenveto

TuBE-projekti tutkii luottamusta ja sen hallintaa web-palveluympäristössä. Luottamusmallissa päätökseen vaikuttavat tekijät ovat luottaja itse, luottamuksen kohteena oleva toimija, suoritettava toiminto, luottamuksen kohteen maine, toimintoon liittyvä riski ja sen tärkeys sekä konteksti, jossa päätös tehdään. Päätös on dynaaminen, joten se riippuu epäsuorasti myös ajan hetkestä.

TuBE-projektin luottamusmallissa on kiinnitetty huomiota muuttuviin tilanteisiin reagointiin, mainepäivitysten lisäksi myös järjestelmään saapuvan paikallisen kontekstitiedon kautta. 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 liitettynä ne lisäävät pääsynhallinnan joustavuutta.

Luottamuksenhallintajärjestelmän keskeiset osat valmistavat luottamuspäätöksen kootusta tiedosta sekä ylläpitävät mainetietoa sekä omakohtaisen että ulkoisen kokemustiedon pohjalta.

Kiitokset

Artikkeli perustuu työlle TuBE-projektissa (*Trust based on evidence*) Helsingin yliopiston tietojenkäsittelytieteen laitoksella. Projektia ovat rahoittaneet TEKES, Nixu ja StoneSoft.

Viitteet

[1] Abdul-Rahman, A., ja Hailes, S. A distributed trust model. *Proceedings of the New Security Paradigms workshop, Langdale, Cumbria, United Kingdom* (1998), ACM Press, s. 48–60.

[2] Blaze, M., Feigenbaum, J., ja Lacy, J. Decentralized trust management. *Proceedings of the IEEE Symposium on Security and Privacy* (May 1996), IEEE, s. 164–173.

[3] Cahill, V., et al. Using trust for secure collaboration in uncertain environments. *Pervasive Computing 2*, 3 (Aug. 2003), 52–61.

[4] 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 (Jan. 2001), vol. 1995, s. 18–38.

[5] Sähköinen kauppapaikka eBay, 2005. URL `http://www.ebay.com/`.

[6] Kamvar, S., Schlosser, M., ja Garcia-Molina, H. The EigenTrust algorithm for reputation management in P2P networks. *Proceedings of the Twelwth International World-Wide Web Conference (WWW03)* (2003), s. 446–458.

[7] Kutvonen, L., Metso, J., ja Ruohomaa, S. From trading to eCommunity population: Responding to social and contractual challenges. *Proceedings of the Tenth IEEE International EDOC Conference (EDOC 2006)* (lokakuu 2006). Hyväksytty julkaistavaksi.

[8] Lutz Schubert, M. W., et al. Trustcom reference architecture, deliverable d09. Tekninen raportti, TrustCoM WP27, elokuu 2005.

[9] Rasmusson, L., ja Jansson, S. Simulated social control for secure Internet commerce. *Proceedings of the 1996 workshop on New Security Paradigms* (1996), ACM Press, s. 18–25.

[10] Resnick, P., Zeckhauser, R., Friedman, E., ja Kuwabara, K. Reputation systems. *Communications of the ACM 43*, 12 (joulukuu 2000), 45–48.

[11] Ruohomaa, S., ja Kutvonen, L. Trust management survey. *Proceedings of the iTrust 3rd International Conference on Trust Management, 23–26, May, 2005, Rocquencourt, France* (2005), LNCS 3477, Springer-Verlag.

[12] Ruohomaa, S., Viljanen, L., ja Kutvonen, L. Guarding enterprise collaborations with trust decisions—the TuBE approach. *Proceedings of the First International Workshop on Interoperability Solutions to Trust, Security, Policies and QoS for Enhanced Enterprise Systems (IS-TSPQ 2006)* (maaliskuu 2006). Painossa.

[13] Ruokolainen, T., Metso, J., ja Kutvonen, L. Web-Pilarcos: väliohjelmistopalveluita sähköisille liiketoimintaverkostoille. *Tietojenkäsittelytiede 24* (joulukuu 2005), 52–66.

[14] Tan, Y.-H. A trust matrix model for electronic commerce. *Proceedings of Trust Management: First International Conference, iTrust 2003, Heraklion, Crete, Greece, May 28–30, 2003* (toukokuu 2003), vol. LNCS 2692, s. 33–45.

[15] 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* (toukokuu 2004), LNCS 2995, Springer-Verlag, s. 16–26.