Luottamus

Jorma Stenman
Helsingin Yliopisto
Tietojenkäsittelytieteen laitos
Avoimien järjestelmien tutkimusseminaari

18. huhtikuuta 2000

Tiivistelmä

Luottamuksen tarve tietoverkoissa toimivien komponenttien välillä on lisääntynyt viime vuosina. Erityisesti tämä koskee Internetiä, jossa WWW-sivustojen kautta on alettu tarjota sähköisiä kaupankäyntipalveluita. Luottamuspalveluiden tarjonta ei kuitenkaan ole kehittynyt tarpeita vastaavassa suhteessa, mikä on estänyt monien luottamusta tarvitsevien toimintojen käytön laajenemisen. Tässä esitelmässä käsitellään luottamusta yleisenä käsitteenä sekä sen käytössä ja hallinnassa hyödynnettäviä menetelmiä ja työkaluja.

Sisältö

1 Johdanto

Internetissä voi nykyään toimittaa monia arkipäiväisiä asioita kuten esimerkiksi käydä kauppaa sähköisesti tai käyttää julkishallinnon palveluita. Usein näiden toimintojen suorittamista rajoittaa pula luottamuksesta—ei ainoastaan ihmisten vaan myös tietokoneiden ja ohjelmien välillä. Tämä on ristiriidassa sen kanssa, että Internetin pitäisi periaatteessa parantaa palveluiden käytettävyyttä ja saatavuutta. Luottamuspulan ja muiden Internetin infrastruktuurin puutteiden vuoksi Internetin palveluresurssit ovat selkeästi vajaakäytössä.

Internetin puutteet luottamuksen suhteen johtuvat siitä, että sitä ei alunperin ole tarkoitettu luottamusta vaativien toimenpiteiden tekemiseen. Monet tällaisista toiminnoista, kuten sähköinen kauppa, ovat syntyneet vasta vuosia sen jälkeen, kun Internet oli jo otettu käyttöön, jolloin sen käyttämät tekniikat olivat ehtineet jo vakiintua.

Alunperin Internet kehitettiin korkeakoulujen ja sotilaallisten organisaatioiden tarpeisiin. Sitä suunniteltaessa ajateltiin, että verkon käyttäjämäärät pysyisivät pieninä. Ennenkaikkea verkon käyttäjien uskottiin käyttäytyvän sääntöjen mukaan. Se ehkä onnistuu pienissä yhteisöissä, joissa kaikki kunnioittavat toistensa oikeuksia ja joiden hallinta on suhteellisen keskitetty. Internetin käytön laajetessa erityisesti WWW:n ansiosta tällaisia oletuksia ei enää voitu tehdä.

Osapuolten välisen luottamuksen saavuttaminen on edellytys tällaisten tietoverkkojen palveluiden toiminnalle. Molemminpuolisen luottamuksen saavuttaminen tietoverkon välityksellä on huomattavasti hankalampaa kuin esimerkiksi reaalimaailmassa ihmisten kesken. Tämä johtuu ensisijaisesti siitä, että luottamusta tarvitsevat osapuolet eivät aina ole ihmisiä vaan esimerkiksi hajautetun ohjelmiston komponentteja. Ne eivät siis voi turvautua aisteihinsa ja intuitioonsa.

Tällä hetkellä suosituin luottamusta vaativa toimenpide, joka voi tapahtua Internetissä, on sähköinen kaupankäyntitransaktio. Tästä syystä tämän esitelmän esimerkit liittyvät enimmäkseen sähköiseen kaupankäyntiin. Koska se ei kuitenkaan ole tämän esitelmän aihe, esimerkit eivät ole yksityiskohtaisia. Tekstissä viitataan usein yksikön kolmatta persoonaa käyttäen sekä ihmiskäyttäjiin että ohjelmisto- tai laitteistokomponentteihin, jotka toimivat jonkin järjestelmän käyttäjinä.

2 Luottamuksen määrittely

Luottamus on uskomuksista muodostuvaa tietoa, joka perustuu kokemukseen. Jos luotetaan ilman kokemusta tai muuta parempaa tietoa, kyseessä on sokea usko. Yleisemmin luottamuksella tarkoitetaan jonkin entiteetin uskoa jonkin väitteen tai havainnon totuuteen. Osapuolten A ja B välinen luottamus voi tarkoittaa esimerkiksi, että kumpikin pystyy luotettavasti todentamaan toisen identiteetin ja uskoo toisen toimivan sopimuksen mukaisesti. Luottamuksen kehittämisen vuoksi on myös oleellista, että osapuolten toimintaa valvotaan.

Luottamus on kaikenkattavaa ellei se liity johonkin tiettyyn asiaan. Luottamuksen absoluuttista määrää tai tasoa voidaan arvioida numeerisesti: Se voi olla ehdotonta eli joko luotetaan (1) tai ei (0), tai osoittaista, jolloin se vaihtelee nollasta sataan prosenttiin. Yleensä sellaisissa käytännön toiminnoissa, joissa luottamuksella on jokin rooli, sitä todella tarvitaan jonkin verran. Esimerkiksi yksinkertainenkaan kaupankäynti tietoverkossa ei onnistuisi, jos kukaan ei luottaisi kehenkään.

Matemaattisesti luottamus on relaatio, jolla on seuraavat ominaisuudet:

- Se on refleksiivinen eli A luottaa aina A:han.

- Se voi olla transitiivinen eli jos A luottaa B:hen ja B C:hen, A luottaa myös C:hen. Koska luottamus ei välttämättä ole kokonaisvaltaista, A voi olla luottamatta B:n käsitykseen C:stä, mutta silti luottaa joihinkin C:n ominaisuuksiin.
- Se on myös yleensä, mutta ei aina, symmetrinen eli jos A luottaa B:hen, myös B luottaa A:han.

Käytännössä luottamus on usein epäsuoraa. Esimerkiksi sähköinen kauppajärjestelmä voi vaatia toimiakseen epäsuoraa luottamusta, koska suoran luottamussuhteen muodostaminen kaikkien järjestelmän käyttäjien välille voi olla mahdotonta. Yleensä muiden paitsi yksinkertaisimpien järjestelmien kaikki käyttäjät eivät tunne kaikkia muita, mikä estää suorat kahdenväliset luottamussuhteet joidenkin välillä. Vaikka jokainen käyttäjä tuntisikin kaikki muut, suorien luottamussuhteiden muodostaminen voi olla epäkäytännöllistä. Epäsymmetrisestä luottamuksesta saattaa olla joskus hyötyä. Se voi esimerkiksi mahdollistaa transaktion, joka aiemmin oli mahdoton luottamuksen täydellisen puutteen vuoksi [KeG96].

Luottamusta ei ole sama asia kuin tiedon salaus vaikka salausta käytetäänkin usein luottamusta vaativissa toiminteissa. Salauksen käyttö sisältää toisaalta luottamuksen siihen, että kukaan muu kuin oikean purkuavaimen haltija ei voi lukea salattua tietoa. Erityisesti pelkkä salauksen käyttö osapuolten välisessä tietoliikenteessä ei luo niiden välille mitään erityisempää luottamussuhdetta. Se ei välttämättä edes tarkoita, että osapuolet olisivat onnistuneet luotettavasti tunnistamaan toisiaan. Tästä syystä salausta käytettäessä tulisi myös aina pyrkiä tunnistamaan toinen osapuoli luotettavasti. Esimerkiksi PGP-salausjärjestelmän [Sta99] väärinkäyttö on hyvin helppoa, jos salattujen viestien lukija ei tarkasta lähettäjän henkilöllisyyttä PGP-allekirjoitusketjun avulla.

3 Luottamustyökaluja

Luottamuksen saavuttamiseen ja hallintaan erityisesti tietoverkoissa on kehitetty menetelmiä ja työkaluja, joilla on usein suorat vastineet reaalimaailmassa. Tämä vastaavuus johtuu siitä, että reaalimaailman menetelmät on usein siirretty käsitteistöineen sellaisenaan tietoverkkoihin. Monet menetelmistä edellyttävät, että käytettävissä on joukko *luotettuja välimiehiä* (engl. *trusted intermediary*). Ne tuottavat tilanteeseen sen luottamuksen alkutason, joka mahdollistaa tilanteen etenemisen.

3.1 Pantit ja ennakkomaksut

Esimerkiksi pantin tai ennakkomaksun käsitettä voidaan käyttää tietoverkoissa samoin kuin reaalimaailmassa riippumatta niiden esitystavasta. Panttia voidaan käyttää esimerkiksi sähköisessä kaupankäynnissä siten, että transaktion osapuolet antavat luotetulle välimiehelle pantiksi tietyn rahasumman. Pantin suuruus vastaa sen hyödykkeen tai palvelun arvoa, jonka pantin antajan on tarkoitus tuottaa. Jos pantin antaja epäonnistuu omassa osassaan transaktiota, luotettu osapuoli luovuttaa pantin haitan kärsineelle osapuolelle [KeG96].

Ennakkomaksut puolestaan soveltuvat luottamuksen ostamiseen, koska ne ovat tavallaan yksisuuntaisia eli peruuttamattomia tapahtumia, joiden alkuunpanija ei voi kieltää niitä jälkeenpäin. Jos transaktion myyjäosapuoli ei luota ostajaan, ostaja voi antaa hyödykeen arvoa vastaavan ennakkomaksun luotetulle välimiehelle. Tämän jälkeen myyjä tietää, että se tulee varmasti saamaan ennakkomaksun välimieheltä itselleen heti kun se antaa hyödykkeen sille. Luotetut välimiehet muistuttavat tässä mielessä yleisemmissä hajautetuissa transaktioissa käytettyjä *kontrollereita* [GrR93].

Edellä mainittiin, että luottamusta tarvitaan yleensä jonkin verran yksinkertaisimmissakin toiminnoissa. Luotetut välimiehet ovat yleisin tapa ratkaista tämä alustava luottamuspula. Siksi sille, kuka tai mikä voi toimia luotettuna välimiehenä, täytyy asettaa tiukat kriteerit. Välimiesten sopivuusvaatimuksia käsitellään lisää myöhemmin.

3.2 Maksuvälineet

Kaupankäynnissä tarvitaan maksuvälineitä riippumatta siitä, tapahtuuko se tietoverkoissa vai reaalimaailmassa. Vain harvoille reaalimaailman maksuvälineille on kuitenkaan kehitetty vastineita tietoverkkoihin, mikä johtuu siitä, että niiden tarve on ollut olemassa vasta vähän aikaa.

Koska maksuvälineen tarkoitus on arvon luominen tai siirtäminen, se ei ole varsinainen luottamustyökalu. Koska luottamustyökaluilla kuitenkin edistetään maksuvälineiden käyttöä, ne liittyvät kiinteästi toisiinsa.

Myös tietoverkkojen harvalukuisen maksuvälinejoukon jäsenillä on esikuvansa reaalimaailmassa. Keskenään molempien ympäristöjen maksuvälineet eroavat siinä, mikä määrä luottamusta vaaditaan osapuolten välille, jotta ne voisivat käyttää maksuvälinettä. Jotkin maksuvälineet soveltuvat tilanteisiin, joissa luottamusta on hyvin vähän, mikä on tyypillisin tilanne nykyisen Internetin transaktioissa. Toiset välineet vaativat suuren luottamuksen osapuolten välille, mutta tarjoavat vastineeksi esimerkiksi nopeammat transaktiot. Eri maksuvälineiden käyttäminen on myös tyypillisesti eri hintaista.

Reaalimaailmassa tyypillisin edullinen matalan luottamuksen maksuväline, joka myös tarjoaa käyttäjälleen identiteettisuojan, on käteinen raha. Rahaa käytettäessä osapuolten tulee voida luottaa ainoastaan kyseisen valuutan vakauteen. Tällöin valuutan takana oleva valtio toimii tavallaan epäsuorasti välimiehenä. Käteisen etuna on myös se, että se suojaa käyttäjänsä identiteetin. Käteinen ei kuitenkaan sovellu sellaisenaan sähköisiin transaktioihin, minkä vuoksi sille on kehitetty useita digitaalisia vastineita. Esimerkiksi VI-

SA:n ja Mastercardin SET-järjestelmä on yksi sellainen, mutta sitä, kuten muitakaan vastaavia, ei ole otettu laajasti käyttöön.

3.3 Kryptografisia työkaluja

Tietoverkoissa todentamiseen eli *autentikointiin* käytetään yleensä *digitaalista allekirjoitusta*, joka on allekirjoittajan *salaisella avaimella* ja kryptografisella algoritmilla tuotettu tarkistussumma. Se lasketaan tiedosta, joka on molempien osapuolten saatavilla. Allekirjoitetun tiedon muuttumattomuus voidaan tarkastaa tarkastamalla allekirjoitus. Allekirjoitus voidaan tarkastaa salausavaimella käytettäessä symmetristä salausalgoritmia. Jos allekirjoitus tuotetaan *julkisen avaimen algoritmilla* kuten RSA [RSA78] tai DSA [Sta99], tarkastaja tarvitsee allekirjoittajan julkisen avaimen. Jos allekirjoituksen tarkastus onnistuu, tarkastaja voi olla lähes varma, että vain salaisen avaimen haltija on voinut tuottaa sen. Tämän jälkeen tarkastajan täytyy vielä jollain keinolla varmistaa, että allekirjoittaja todella on se henkilö, jonka hän uskoo liittyvän avainpariin. Yleensä julkisen avaimen autentikoi jokin kolmas osapuoli, johon tarkastaja jo luottaa. Eräissä Yhdysvaltojen osavaltioissa julkisen avaimen algoritmilla tuotetulla digitaalisella allekirjoituksella on sama lainvoima kuin manuaalisella allekirjoituksella [Rea96], mikä mahdollistaa tietoverkoissa tehtävät sitoumukset ja siten parantaa oleellisesti niiden luottamusominaisuuksia.

Julkisten avainten jakelu ja luottamuksen puute osapuolten välillä ovat suurin ongelma osapuolten todentamisessa. Sen ratkaisemiseksi käytetään tyypillisesti *digitaalisia varmenteita*, joita voi ostaa luotetuilta varmennekauppiailta. Varmenteita voi käyttää myös ilmaiseksi PGP:n tyyppisissä yhteisöpohjaisissa järjestelmissä. Varmenne yhdistää entiteetin nimen tai muun tunnisteen, julkisen avaimen ja sen voimassaoloajan varmenteen todentajan allekirjoitukseen.

Varmenteiden käyttö helpottaa erityisesti sähköistä kaupankäyntiä, koska niiden avulla voidaan todentaa tapahtumia ja antaa vakuuksia. Esimerkiksi normaalien finanssimarkkinoiden käyttämä haltijavelkakirja voitaisiin toteuttaa digitaalisesti joukkona varmenteita [Rea96]. Varmenteen käyttö todentamiseen vastaa reaalimaailman lisenssin käsitettä. Lisenssi osoittaa, että sen haltija on oikealla asialla eli että siihen voi luottaa. Esimerkiksi sähköisen etälääkäripalvelun tarjoaja voisi esittää lääkäriliiton myöntämän varmenteen todisteeksi siitä, että pystyy tarjoamaan kunnollista palvelua.

Varmenteen käyttö on jossain määrin monimutkaista, koska se vaatii tuekseen *varmennehierarkian*, joka muodostuu varmenteiden myöntäjistä (engl. *certificate authority, CA*. Sen avulla varmenteiden käyttäjät voivat tarkastaa varmenteiden oikeellisuuden ja voimassaolon. Varmenteiden käyttö hajautetussa prosessointiympäristössä saattaa olla epäkäytännöllistä, jos järjestelmässä on paljon keskenään kommunikoivia komponentteja tai jos järjestelmän toiminnalla on reaaliaikavaatimuksia. Varmenteen tarkastaminen saattaa vaatia varmennehierarkian navigointia eli useamman kuin yhden varmenteiden myöntäjäpalvelimen käyttöä. Jos varmentei käyttö ei ole mahdollista, voidaan turvautua keskitetympiin autentikointipalvelimiin, jotka mahdollistavat turvalliset transaktiot. Esimerkiksi Kerberos-järjestelmä [SNS88] perustuu keskitettyihin autentikointipalvelimiin ja siinä käytetään ainoastaan symmetrisiä salausalgoritmeja. Näistä syistä sen käyttö ei ole yhtä raskasta kuin varmenteiden eli se sopii paremmin käytettäväksi laajoissa hajautetuissa järjestelmissä.

4 Luottamuksen käyttöympäristöt

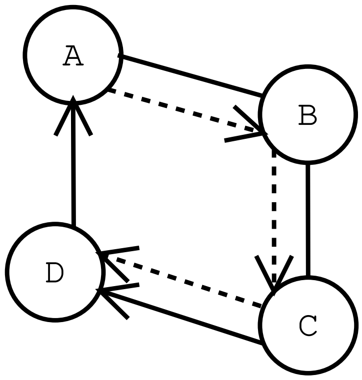
Luottamusta vaativia toimenpiteitä voidaan joutua tekemään hajautetuissa järjestelmissä, jotka koostuvat heterogeenisistä komponenteista. Niillä ei yleensä ole yhtenäistä näkemystä koko järjestelmästä, ja niitä myös hallitaan eri paikoista käsin. Esimerkiksi sähköisessä kaupassa ostajakomponentti ei välttämättä tunne yhtään myyjäkomponenttia vaan asioi niiden kanssa *meklarin* välityksellä. Tällöin ei voida olettaa, että kaikki komponentit luottaisivat toisiinsa eli noudattaisivat jotain yhteisesti sovittua protokollaa. On siis mahdollista, että komponentti tyytyy muiden kannalta epätäydelliseen lopputulokseen tai yrittää jopa huijata. Jos komponentit olisivat tässä mielessä homogeenisia, voitaisiin käyttää sellaisenaan esimerkiksi *kaksivaiheista sitoutumista* (engl. *two phase commit*) [GrR93] tai muita hajautettujen transaktioiden yhteydessä käytettyjä menetelmiä. Niitä voidaan käyttää, jos komponenteilla on järjestelmästä ja transaktion päämäärästä yhtenäinen näkemys ja tahattomienkaan väärinkäytösten vaaraa komponenttien taholta ei ole. Ne estävät lähinnä tietojen joutumisen epäyhdenmukaiseen tilaan, koska niissä transaktio tapahtuu yleensä kokonaisuutena tai ei ollenkaan.

Mitä useampia luotettuja komponentteja järjestelmä sisältää, sitä pienempi on sellaisten komponenttien suhteellinen osuus, jotka yrittävät huijata tai eivät välitä säännöistä. Luotetun komponentin uskotaan siis käyttäytyvän sovittujen sääntöjen mukaan. Toisaalta, mitä vähemmän luotettuja komponentteja tarvitaan, sitä enemmän muut komponentit voivat kommunikoida suoraan keskenään ja sitä tehokkaampi transaktio on kokonaisuutena. Jotkin kahdenväliset transaktiot saattavat jopa olla mahdottomia, jos niiden suorittamisessa käytetään pelkästään välimiehiä eikä minkään kahden osapuolen välillä ole suoraa luottamusta [KeG96].

5 Luottamusverkot

Komponenttien välisiä luottamussuhteita voidaan kuvata *luottamusverkkoina* (engl. *web of trust* [Rea96], *trust web* [AAS99]). Se on abstrakti käsite, jonka käytännön ilmentymä on mikä tahansa hajautettu järjestelmä, jonka komponentit tarjoavat toisilleen luottamuspalveluita *suositusten* muodossa tai luottavat toisiinsa suoraan. Komponentti voi suositella muille niiden komponenttien palveluita, joihin se itse luottaa jossain asiassa. Se voi esimerkiksi luottaa toisen komponentin tarjoamiin autentikointipalveluihin, ja suositella niitä muillekin. Koska luottaa voidaan monissa eri asioissa, täytyy luottamustyypit pystyä luokittelemaan. Eräitä suhteellisen yleiskäyttöisiä luottamusluokkia ovat kyky pitää salaisuuksia, kyky generoida kryptografisesti hyviä satunnaislukuja ja kyky noudattaa protokollia [YKB93].

Kuva 1 esittää yksinkertaisen luottamusverkon, jossa on neljä komponenttia. Viivat esittävät komponenttien välisiä suoria luottamussuhteita. Nuolet tarkoittavat epäsymmetristä luottamusta ja katkoviivalla piirretyt nuolet sitä, että A:n ja D:n välillä on epäsuora luottamussuhde, joka on muodostettu B:n ja C:n kautta. A:n ja D:n väliset toimenpiteet, jotka liittyvät niiden väliseen luottamussuhteeseen, kulkevat siis B:n ja C:n kautta.



Kuva 1: luottamusverkko

Verkon solmut, kuten komponentit B ja C kuvassa 1, toimivat joskus luotettuina välimiehinä, joita voidaan käyttää esimerkiksi kaupankäyntisovelluksissa pienentämään transaktioon liittyvää riskiä. *Luottamuspolku* verkossa on ketju solmujen välisiä linkkejä, joiden oletetaan olevan luottamuksen arvoisia, ja joille voidaan antaa tiettyjä arvoja. Polun linkkejä voidaan arvioida esimerkiksi niihin liittyvien luottamuksen muodostamiskustannusten mukaan [AAS99].

Luottamusverkossa ne verkon komponentit, joihin tietty komponentti luottaa suoraan tai epäsuorasti, saadaan selville transitiivista sulkeumaoperaatiota muistuttavan algoritmin [YKB93] avulla. Algoritmi ottaa syötteenään listan verkon komponenteista ja niiden asettamista vaatimuksista ja tarjoamista palveluista, jotka liittyvät luottamukseen. Algoritmia voidaan käyttää myös uusia protokollia kehitettäessä niiden luottamustarpeiden arviointiin ja olemassaolevien protokollien analysointiin.

6 Luottamusalgoritmit

Edellisen luvun algoritmi on vain yksi käytännön esimerkki yleisemmistä *luottamusalgoritmeista*, joita käytetään luottamuksen muodostamisessa kahden tai useamman osapuolen välille. Käytännössä nämä algoritmit sisältävät yleensä muutakin kuin pelkän verkon navigoinnin, koska niiden käyttäjä haluaa tyypillisesti muutakin kuin vain selvittää, mihin komponentteihin se luottaa.

Algoritmien toiminta pyrkii monessa asiassa jäljittelemään ihmisten käyttäytymistä luottamusta muodostettaessa. Luottamuksen muodostamispäätökseen ihmisillä vaikuttavat ainakin seuraavat kolme asiaa riippumatta siitä, onko vastakappaleena toinen ihminen tai jokin järjestelmä, kone tai ohjelma [KiC98]:

- Henkilökohtaiset ominaisuudet, jotka perustuvat esimerkiksi siihen, millaisessa ympäristössä henkilö on varttunut tai toiminut. Jos on tottunut luottamaan muihin, myönteisen luottamuspäätöksen tekeminen on helpompaa.

- Ympäristövaikutukset eli esimerkiksi henkilön havainnot ihmisten tai instituutioiden käyttäytymisestä luottamusta vaativissa tilanteissa. Näistä havainnoista muodostuu kokemusta. Esimerkiksi sähköisen kaupankäyntijärjestelmän toimivuus, käyttötuntuma ja ulkonäkö vaikuttavat käyttäjien sitä kohtaan tuntemaan luottamukseen.

- Päätöksen kohteena olevaan asiaan liittyvän riskin ja hyödyn kokonaissuhde. Jos odotettavissa on suuri hyöty, saattaa pienen riskin ottaminen kannattaa eli ei tarvita niin suurta luottamusta kuin hyvin riskialttiissa asioissa.

- Päätöksen kohteena olevan asian luonne eli se, mitä ollaan tekemässä. Esimerkiksi sähköisessä kaupankäynnissä rahan tai luottokorttinumeron välittäminen tietoverkossa vaatii suurta luottamusta järjestelmään.

Muodostettaessa luottamuspäätöstä joidenkin muiden kuin ihmiskomponenttien välille näitä asioita ehkä joudutaan simuloimaan. Algoritmien toteutuksissa voidaan hyödyntää esimerkiksi tekoälytutkimuksen tuloksia.

Algoritmit saattavat hyödyntää historiatietoa, joka muodostuu käyttäjän aiemmista kokemuksista luottamuksen käyttötilanteissa, ja vaikuttaa käyttäjän myöhempään käyttäytymiseen. Luottamusalgoritmi voi käyttää historiatietoa yksinkertaisimmillaan jakamalla positiivisten kokemusten määrän kokemusten kokonaismäärällä. Näin saadaan eräänlainen odotusarvo tai todennäköisyys sille, että toinen osapuoli käyttäytyy luottamuksen arvoisesti ensi kerralla. Vääryyden kokenut osapuoli on varovaisempi seuraavalla kerralla, mikäli sellaista enää tulee. Jos luottamus on epäsuoraa, todennäköisyys saadaan laskettua komponenttiparien välisten todennäköisyyksien tulona, koska kyseessä on joukko riippumattomia tapahtumia.

Merkitään esimerkiksi (x, y):llä komponentin x laskemaa luottamusarvoa komponentille y. Jos kuvan 1 tapauksessa on $(A, B) = 75\%$, $(B, C) = 50\%$ ja $(C, D) = 80\%$ saadaan $(A, D) = 30\%$ eli A:n tulee olla varovainen suhteessaan D:hen tällä polulla.

Monimutkaisemmissa luottamusalgoritmeissa historiatiedon sisältämiä kokemuksia voidaan painottaa jotenkin muuten tai voidaan esimerkiksi huomioida niiden tilastolliset ominaisuudet luottamuksen arvoa muodostettaessa. Myös päätösanalyysillä (engl. *decision analysis*) [Neu90] on käyttöä luottamuspäätösten muodostamisessa ja riskiarvioinneissa. Päätösanalyysissä toimenpiteestä päättäminen perustuu toimenpiteellä saavutettavan hyödyn ja tappion arviointiin. Esimerkiksi ostaja voi luottaa myyjään lähettämällä käteismaksun ilman takeita tuotteen saamisesta, jos käteisalennus on huomattava ja myyjä on aiemmin ollut luottamuksen arvoinen. Jos myyjä toimii taas kuten ostaja odottaa, ostaja saa suuren hyödyn. Päätöksen tekijän saatavilla olevan tiedon laatu ja määrä vaikuttavat oleellisesti päätösanalyysin lopputulokseen eli luottamuksen muodostamispäätökseen. Esimerkiksi luotolla tapahtuvassa kaupankäynnissä myyjä saattaa kieltäytyä aiemmin lupaavalta vaikuttaneesta kaupasta saatuaan ostajan luottotiedot.

Kokemuksia voidaan painottaa niiden vahvuuden, läheisyyden ja tarkkuuden mukaan. Vahva kokemus on sellainen, jonka todenmukaisuutta on vaikea epäillä. Esimerkiksi ihmisten on usein helpompi uskoa näkemäänsä kuin lukemaansa. Kokemuksen vahvuus voi myös heijastua sitä ajallisesti lähellä oleviin kokemuksiin vahvistaen niitä. Kokemuksen tarkkuus on suhteessa kokijan luottamuksen tasoon. Jos kokija esimerkiksi uskoo, että tapahtuma toistuu kymmenen kertaa, mutta todellisuudessa toistoja on vain seitsemän, kokemus on epätarkka.

Uusia kokemuksia voidaan arvioida vertaamalla niitä historiatiedosta laskettuihin tilastollisiin suureisiin. Esimerkiksi sellaiset kokemukset, jotka ovat liian hyviä ollakseen tosia, voidaan tunnistaa ja ehkä poistaa vertaamalla niitä aiempien keskiarvoon ja varianssiin.

Riippumatta siitä, miten saatavilla olevan luottamuksen taso on määritetty, se vaikuttaa toimenpiteissä käytettävien menetelmien monimutkaisuuteen, mikä yleensä vaikuttaa niiden tehokkuuteen. Suuri luottamustaso mahdollistaa yleensä yksinkertaisempien ja tehokkaampien menetelmien käytön. Jos komponentit esimerkiksi luottavat toisiinsa suoraan, ne eivät tarvitse välimiehiä lainkaan.

7 Riski ja maine

Luottamusta vaativissa ympäristöissä toimivan tulee pystyä asettamaan rajat sille, kuinka suuren riskin hän ottaa ja kuinka paljon hän luottaa muihin osapuoliin. Riskin käsite liittyy luottamukseen kiinteästi, koska ilman mitään riskejä ei ole tarvetta luottamukselle. Riski on suure, jota usein mitataan rahana, joka menetetään silloin kun riski toteutuu. Myös henkilökohtaisten tietojen menetys tai paljastuminen voi olla riski. Riskiin liittyy tietty toteutumistodennäköisyys, joka on teoriassa luottamusta kuvaavan todennäköisyyden komplementti—mitä enemmän luotetaan sitä vähemmän asiaan liittyy riskiä, jos luottamus on perusteltua.

Se, kuinka paljon komponentti aikoo luottaa toiseen, riippuu monista asioista. Ensinnäkin luotetun komponentin tulee pystyä toimimaan luottamuksen edellyttämällä tavalla. Esimerkiksi pörssin asiantuntijapalveluita tarjoavan komponentin tulee pystyä todistamaan kykynsä tarjota luotettavaa palvelua. Kuten edellä esitettiin, tämä voidaan tehdä komponentille myönnetyn varmenteen avulla. Todistaminen voi tapahtua epäsuorasti esimerkiksi siten, että todistuksen tarvitsija pyytää varmenteen todennuspalveluita tarjoavalta välimieheltä. Komponentin luottamusta toiseen komponenttiin voi myös lisätä se, että se saa luottamussuosituksia useilta muilta tuntemiltaan ja luottamiltaan komponenteilta. Tällöin sen täytyy määrittää jokin kynnysarvo saatujen suositusten määrälle, jonka ylittyessä luottamus syntyy.

Komponentin oma toiminta vaikuttaa sen maineeseen eli muiden komponenttien käsitykseen siitä. Maine on sitä parempi mitä useammin komponentti toimii luottamuksen arvoisesti, ja mitä parempi komponentin maine on sitä helpommin se voi saavuttaa muiden luottamuksen. Jos osapuolet luottavat toisiinsa, ne saattavat pärjätä ilman kolmansien osapuolien tarjoamia välimies- tai todennuspalveluita, jolloin toiminta tulee halvemmaksi. Hyvä maine on arvokas myös siksi, että sen menettäminen kannattaa siitä saatavan hyödyn ollessa tappiota suurempi. Luottamuksen hallinta toimii tässäkin mielessä markkinatalouden ehdoilla. Myös muita normaalista talouselämästä tuttuja maineen parannus- tai muodostuskeinoja kuten tyytyväisyystakuita tai liikemerkin tunnettuutta voidaan hyödyntää tietoverkoissa.

8 Luottamus ja protokollat

Luottamusta vaativissa toimenpiteissä, joista monet liittyvät sähköiseen kaupankäyntiin, voidaan käyttää ainakin seuraavan tyyppisiä protokollia [Rea96]. Ne vaikuttavat luottamuksen tarpeeseen siirtämällä sitä osapuolelta toiselle, muuttamalla sen suuntaa tai poistamalla sen kokonaan.

Välimiesprotokollassa (engl. *arbitrated protocol*) toimenpiteet tehdään kolmannen osapuolen välityksellä. Jos kaikki muut toimenpiteen osapuolet luottavat johonkin osapuoleen, se voi ottaa välimiehen roolin eikä erillistä välimieskomponenttia tarvita. Välimiehet tarjoavat usein luottamuspalvelun lisäksi myös meklari- tai arviointipalveluita[1]. Välimies voi olla esimerkiksi sähköinen kauppakeskus, joka huolehtii myös tavaroiden ja palveluiden toimittamisesta silloin kun se ei ole tietoverkossa siirrettävässä muodossa.

Välimiesprotokollan ongelma on sellaisen välittävän osapuolen löytäminen, johon kaikki toimijat luottavat. Variaationa tästä on *tarkkailijaprotokolla* (engl. *adjudicated protocol*), jossa välimies ainoastaan valvoo osapuolten toimintaa ja kirjaa ylös mahdolliset väärinkäytökset tai virheet. Toimijat eivät

[1] arviointipalvelun tarjoaja voi esimerkiksi varmistaa, että tilaaja saa tilaustaan vastaavan tuotteen

siis luota välimieheen muissa asioissa. Kolmas protokollatyyppi on *itsesäätelevät* (engl. *self-enforcing*) protokollat, joissa väärinkäytökset ovat heti osapuolten nähtävissä, eikä ylimääräisiä välimiehiä tarvita. Nämä protokollatyypit toteutetaan pääosin kryptografisin menetelmin.

Välimiesten hyvä puoli on, että ne mahdollistavat luottamuksen saavuttamisen silloin, kun transaktion osapuolet eivät tunne toisiaan ja eivät siksi luota toisiinsa. Tämä on tyypillinen tilanne esimerkiksi Internetin sähköisessä kaupassa. Välimiespalvelun tarjoajan saattaa tosin olla hankala todistaa luotettavuutensa. Toisaalta, koska transaktion osapuolet varmasti valvovat välimiesten toimintaa luottamusalgoritmiensa välityksellä, epäluotettava välimies menettää nopeasti maineensa.

Jos kaikki transaktion osapuolet voivat luottaa samaan välimieheen, transaktio on helppo suorittaa luotettavasti. Välimies pystyy tällöin takaamaan hyväksyttävän lopputuloksen kaikille osapuolille yhtä aikaa. Hyväksyttävä lopputulos esimerkiksi kaupankäynnissä on, että ostaja saa tuotteen tai rahat takaisin ja myyjä saa rahat tai tuotteen takaisin.

Kuka tai mikä sitten on sopiva välimies? Valtioiden, pankkien tai vakuutuslaitosten sopivuudesta välimiespalveluiden tarjoajiksi on keskusteltu. Se olisi luonteva rooli niille, koska ne hoitavat vastaavan tyyppisiä tehtäviä reaalimaailmassa. On totuttu muun muassa siihen, että valtio painaa rahaa, säätelee jossain määrin talouselämää sekä säätää lakeja ja valvoo niiden noudattamista. Nämä ovat toiminteita, jotka mahdollistaisivat luottamuspalveluiden tarjoamisen välimiehen roolissa, jos ne voitaisiin toteuttaa tietoverkoissa. Kansainvälistä pankkiverkostoa voisi mahdollisesti hyödyntää luottamuspalveluiden tarjonnassa ainakin siihen asti, kunnes syntyy pelkästään luottamuspalveluita tarjoavia instituutioita.

Toisaalta tietoverkot eivät muistuta joka suhteessa reaalimaailmaa eikä niiden välttämättä tarvitsekaan. Esimerkiksi valtiot ovat tottuneet toimimaan pääasiassa rajojensa sisäpuolella, kun taas tietoverkoissa valtioiden rajat ovat hämäriä tai ainakin valtioiden on hankala valvoa etujaan rajojen avulla.

Jotkin asiat voisivat mahdollisesti toimia tietoverkoissa paremmin, jos niitä ei tarvitse tehdä samoin kuin vastaavia asioita reaalimaailmassa. Jos esimerkiksi oikeus levittää sähköistä rahaa ei olisi rajoitettu koskemaan pelkästään valtioita, yksityiset yritykset voisivat tarjota luottamuspalveluitaan oman sähköisen rahan muodossa. Kaikille tietoverkkojen mahdollistamille toiminnoille ei välttämättä edes löydy vastineita, joita matkia.

9 Yhteenveto

Luottamuspula vaivaa tällä hetkellä Internetin sähköistä kaupankäyntiä, joka on suosituin luottamusta vaativa palvelu. Käytännössä se usein estää transaktiot kokonaan, koska ostajan ja myyjän välillä ei ole luottamusta eikä liioin keinoja sen saavuttamiseksi. Tästä syystä kaupankäyntitransaktioissa jonkin osapuolen täytyy yleensä ottaa riski luottamalla jokseenkin sokeasti toiseen.

Tilannetta auttaa luottamusalgoritmien käyttö: Keräämällä kokemuksia kaikki osapuolet voivat saada paremman pohjan luottamuspäätösten tekemiselle jatkossa. Käytännössä tämä koskee lähinnä myyjäosapuolia, koska negatiiviset kokemukset eli huijatuksi tuleminen tulisi kalliiksi ostajille.

Myös välimiespalveluita lisäämällä voidaan parantaa Internetin luottamuspalveluiden tasoa. Löytämällä sopivat organisaatiot, jotka voisivat tarjota luotettavia välimiespalveluita, voidaan oleellisesti parantaa sähköisen kaupankäynnin toimivuutta. Myös muut luottamusta tarvitsevat palvelut, jos ja kun niitä ilmaantuu, hyötyvät välimiespalveluiden olemassaolosta.

Viitteet

[AAS99] Arshad, K., M., Atif, Y., Siyal, M., Y., "*A CORBA based Framework for Trusted E-Commerce Transactions*", IEEE Proceedings, 1999.

[GrR93] Gray, J., Reuter, A., "*Transaction Processing: Concepts and Techniques*", Morgan Kaufmann, 1993.

[KeG96] Ketchpel, S., P., Garcia-Molina, H., "*Making Trust Explicit in Distributed Commerce Transactions*", Proceedings of the 16th ICDCS, IEEE, 1996.

[KiC98] Kini, A., Choobineh, J., "*Trust in Electronic Commerce: Definition and Theoretical Considerations*", IEEE Proceedings of the 31st Annual Hawaii International Conference on System Sciences, IEEE, 1998.

[Neu90] De Neufville, R., "*Applied Systems Analysis: Engineering Planning and Technology Management*", McGraw-Hill, 1990.

[Rea96] Reagle Jr., J., M., "*Trust in electronic Markets*", http://www.firstmonday.dk/issues/issue2/markets/, 1996.

[RSA78] Rivest, R., L., Shamir, A., Adleman L., "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*", Communications of the ACM, February, 1978.

[SNS88] Steiner, J., Neuman, C., Schiller, J., I., "*Kerberos: An Authentication Service for Open Network Systems*", Usenix Workshop Proceedings, UNIX Security Workshop, Portland, Oregon, 1988.

[Sta99] Stallings, W., "*Cryptography and Network Security, Principles and Practice*", Second edition, Prentice Hall, 1999.

[YKB93] Yahalom, R., Klein. B., Beth, T., "*Trust Relationships in Secure Systems - A Distributed Authentication Perspective*", Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy, IEEE, 1993.