Pekka Tuusa

Facebookin tietoturvasta

Tietotekniikan kandidaatintutkielma

30. huhtikuuta 2015

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Pekka Tuusa

Yhteystiedot: pekka.a.tuusa@student.jyu.fi

Ohjaaja: Anneli Heimbürger

Työn nimi: Facebookin tietoturvasta

Title in English: Information security in Facebook

Työ: Kandidaatintutkielma

Suuntautumisvaihtoehto: Tietotekniikka

Sivumäärä: 25+0

Tiivistelmä: Tämä työ sai alkunsa, kun kiinnostuin Internetin tietoturvasta Edward Snowdenin paljastusten myötä. Aluksi selvitän käsitteet sosiaalinen media ja tietoturva. Sitten yhdistän nämä käsitteet, tutkien sosiaalisen median tietoturvaa Facebookin tapauksessa. Esittelen tutkimuslähteiden valossa ilmenneitä keskeisempiä turvallisuusuhkia, jotka liittyvät Facebookiin ja vaikuttavat käyttäjien yksityisyyteen ja tietoturvaan. Tietoisuuden lisääminen mahdollisista uhista osoittautui parhaaksi keinoksi niiden torjunnassa.

Avainsanat: Facebook, tietoturva, yksityisyys

Abstract: This work began when I became interested in Internet data security because of Edward Snowden revelations. First, I explain the concepts of social media and security. Then I combine these concepts exploring the social media security in case Facebook. I present to Facebook's main security threats which affects users' privacy and information security. The awareness of potential threats seems to be the best way to fight against them.

Keywords: Facebook, security, privacy

Kuviot

Sisältö

1 Johdanto

Sosiaalinen media on noussut pinnalle viimeisen vuosikymmenen aikana. Yhteisöpalvelu Facebook on kerännyt enemmän käyttäjiä kuin mikään muu sosiaalinen yhteisöpalvelu. Vuonna 2009 Facebookilla oli yli 150 miljoonaa aktiivista käyttäjää ja käyttäjien määrä kasvoi tuolloin noin 3% viikossa. Facebook on lisäksi maailman suurin kuvien varasto ja se sisälsi jo vuonna 2009 yli miljardi sinne ladattua kuvaa. Facebook on maailman toiseksi käytetyin sivusto heti Googlen jälkeen. (Bilge ym. 2009) Facebookin suosio on jatkanut edelleen räjähdysmäistä kasvuaan ja viimeisimpien tilastojen mukaan Facebookilla on yli 1.4 miljardia aktiivista käyttäjää (http://www.statista.com).

Facebookin luonteeseen kuuluu, että käyttäjä luovuttaa itsestään suuren määrän henkilökohtaista tietoa palveluun. Käyttäjiltä kysytään heidän nimensä, syntymäaikansa, asuinpaikkansa, osoitteensa, sähköpostiosoitteensa, puhelinnumeronsa, harrastuksensa, kiinnostuksen kohteensa, koulutuksensa, ystävänsä ja niin edelleen. Mikään ei tietenkään pakota antamaan itsestään oikeita tietoja, mutta juuri oikeiden tietojen antaminen on koko palvelun kantava idea. (Tuunainen, Pitkänen ja Hovi 2009)

Edward Snowden nosti yksityisyyden ja tietoturvan maailman huomion keskipisteeksi tekemillään paljastuksilla vuonna 2013. Snowdenin tekemien paljastusten pohjalta on käynyt ilmeiseksi se, kuinka helposti kansalliset turvallisuuspalvelut voivat kerätä tietoja kansalaisista kaikkialta maailmasta. Sosiaalisten yhteisöpalvelujen ja suurten hakukoneyhtiöiden rooli valtavan tietomäärän kerääjinä korostuu, ja tästä tietomassasta, niin sanotusta Big Datasta, on tiedustelupalvelujenkin helppoa louhia haluamaansa tietoa. (Järvinen 2014).

Myös monissa päivittäisissä medioissa on keskusteltu tietosuojasta, yksityisyydestä, tietoturvasta ja kyberturvallisuudesta. Sosiaalisiin medioihin on liitetty usein heikko yksityisyyden suoja ja monet tietoturvaongelmat. Edellä mainittujen paljastusten ja oman lähipiirini innokkaan sosiaalisen median käytön myötä minulla heräsi halu tutkia sosiaalisen median tietoturvaa. Usein olen huomannut, että vaikka yksittäisistä turvallisuuteen liittyvistä asioista ollaan tietoisia, niin kokonaisuus jää silti usein hahmottamatta.

Liikkeelle lähdetään käsitteiden määrittelemisen kautta. Mitä on tietoturva suuremmassa vii-

tekehyksessä ja riittääkö pelkkä tietoturvan tarkastelu pohdittaessa palveluiden kokonaisturvallisuutta? Kuinka tietoturva suhteutuu lähiaikoina mediassakin esiintyneeseen kyberturvallisuuteen? Onko tässä tulossa liian iso suupala haukattavaksi? Mitä ovat sosiaaliset mediat ja kuinka Facebook, joka on kiinnostuksen kohteeni, sijoittuu tähän kokonaisuuteen? Näistä asetelmista lähdin liikkeelle ja aloitin tiedon keräämisen ja kriittisen analysoinnin tarkoituksenani tehdä aiheesta kattava kirjallisuuskatsaus. Tutkimusmetodini on yhdistelmä systemaattista ja kuvailevaa tutkimusta ja tutkimuskysymykset voidaan tiivistää seuraavasti: *mitkä ovat Facebookin tietoturvauhat ja kuinka tietoturvaa voidaan parantaa käyttäjälähtöisesti?*

Työn tarkoituksena on kiinnittää huomiota niihin asioihin, joiden tunteminen auttaa parantamaan tietoturvaa Facebook-ympäristössä ja suojaamaan käyttäjän yksityisyyttä paremmin. Katson onnistuneeni tehtävässä, jos tämä kirjoitelma auttaa lukijaa hahmottamaan sosiaaliseen mediaan liittyvia uhkia ja myös niitä mahdollisuuksia, jotka ovat pelottomammin hyödynnettävissä, kun myös riskit tunnetaan.

Tämä tutkielma on jaettu seuraaviin lukuihin: luvussa 2 määritellään turvallisuus, tietoturva ja yksityisyys. Luvussa 3 määritellään sosiaalinen media ja kuinka Facebook sijoituu erilaisten sosiaalisten medioiden joukkoon. Luvussa 4 esitellään Facebookin keskeisimpiä turvallisuusuhkia. Luvussa 5 esitetään yhteenveto ja tutkimuksen aikana tehtyjä havaintoja Facebookin turvallisuudesta ja siihen vaikuttavista tekijöistä.

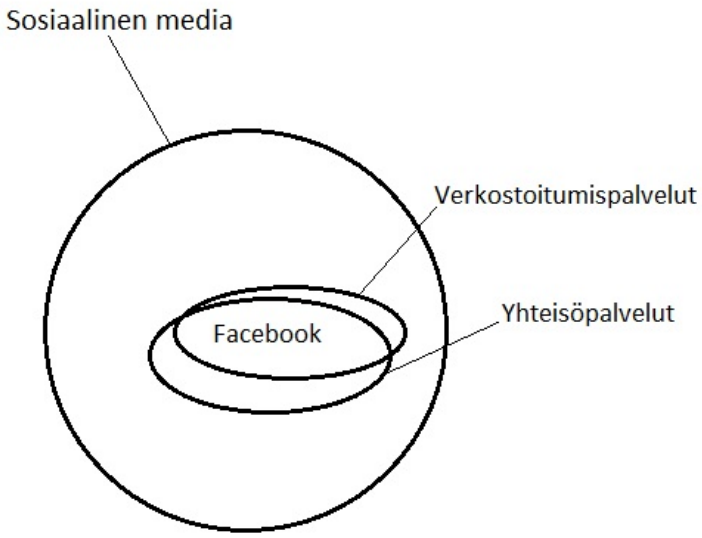
2 Sosiaalinen media ja Facebook

Mikä on sosiaalinen media ja kuinka se pitäisi määritellä? Kuinka Facebook suhteutuu sosiaaliseen mediaan, vai ovatko ne yksi ja sama asia? Usein kuulee puhuttavan sosiaalisesta mediasta (some) ikään kuin se olisi synonyymi Facebookille tai Twitterille. Tarkastellaan aluksi näitä käsitteitä ja pyritään määrittelemään ne.

Kaplan ja Haenlein (2010) ovat esittäneet määritelmän sosiaaliselle medialle. Heidän mukaansa sosiaalinen media on joukko Internet-pohjaisia sovelluksia, jotka ideologialtaan ja teknologialtaan perustuvat Web 2.0:aan, ja jotka täten sallivat loppukäyttäjien luoda ja välittää sisältöä. Määritelmän pohjalta on helppo tulla siihen johtopäätökseen, että kuvatunlaisia sovelluksia on useita ja niiden kirjo on monipuolinen. Kaplan ja Haenlein (2010) ovat myös ryhmitelleet sovellukset kuuteen kategoriaan: Yhteistyöprojektit (Collaborative projects), blogit, sisältöyhteisot (Content communities), verkostoitumispalvelut (Social networking sites), virtuaaliset pelimaailmat (Virtual game worlds) ja virtuaaliset sosiaaliset maailmat (Virtual social worlds). Jokaisesta ryhmästä voidaan nostaa esille esimerkkejä, jotka ovat varmasti meille kaikille tuttuja. Ensimmäisestä ryhmästä, yhteistyöprojektit, esimerkiksi voidaan nostaa Wikipedia, jossa käyttäjät voivat muokata samaa kohdetta, sisältösivua. Toisesta ryhmästä, blogit, voidaan mainita WordPress, Blogger ja Vuodatus. Kolmanteen ryhmään, sisältöyhteisöt, kuuluvat Youtube ja Flickr. Neljänteen ryhmään, verkostoitumispalvelut, kuuluvat Facebook, Google+ ja LinkedIn. Viidenteen ryhmään, virtuaaliset pelimaailmat, kuuluu esimerkiksi World of Warcraft. Kuudenteen ryhmään, virtuaaliset sosiaaliset maailmat, kuuluu Second Life.

Oleellista tästä määritelmästä on havaita se, että sosiaalinen media on monelta monelle -periaatteeseen perustuvaa sisällön tuotantoa ja jakelua. Keskiössä on käyttäjien itsensä tuottama sisältö, jonka tuoton ja jakelun mahdollistaa joukko ohjelmistoja, jotka on tehty toimimaan yhdessä www-selainten kanssa. Kuten Kaplan ja Haenlein (2010) esittävät, Web 2.0 ei tuo mukanaan mitään teknistä päivitystä World Wide Web -standardiin, mutta se liittää siihen sellaisia ohjelmistoja ja toimintoja, kuten Adobe Flash, RSS ja AJAX (Asynchronous Java Script), jotka mahdollistavat Web 2.0 ideologian mukaiset toiminnot. Web 2.0 voidaankin nähdä World Wide Webin ideologisena ja käsitteellisenä laajennuksena, ei niinkään suurena

teknologisena harppauksena. Sosiaalisen median palvelut näyttävätkin toteuttavan Web 2.0:n ideologiaa ja ovat näin ollen tuon ideologian ilmentymiä. Jotta sosiaalisen median palvelut toimisivat, tarvitaan nopeita internet-yhteyksiä. Toisaalta juuri sosiaalisen median kehitys ja nopea leviäminen on pakottanut palveluntarjoajat toteuttamaan yhä nopeampia ja edullisempia yhteyksiä.



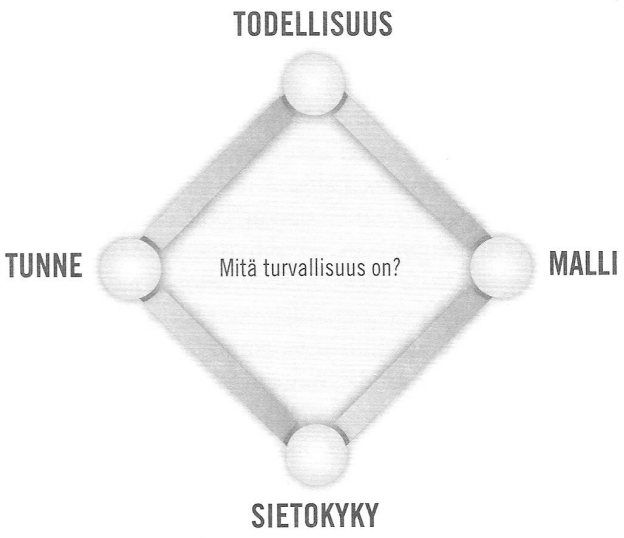
Kuvio 1. Facebook käsitteiden leikkausjoukossa.

Facebook on siis yksi sosiaalisen median palveluista ja kuuluu edellisen ryhmittelyn mukaan verkostoitumispalvelujen ryhmään. Facebookin kohdalla puhutaan kuitenkin usein yhteisöpalvelusta, verkkoyhteisöpalvelusta tai verkostoitumispalvelusta. Kaikki nämä termit ovat hiukan ongelmallisia ja niiden käyttö vaihtelee runsaasti eri lähteissä. Pienistä vivahde-eroista huolimatta usein tarkoitetaan samaa palvelujen joukkoa, vaikka tarkasti ottaen niiden merkitys vaihtelee. Englannin kielisessä lähdekirjallisuudessa asiasta puhutaan termeillä Social networks, Social networking sites, Social network communities, Social network service, Social networks sites (SNS), Online social networks (OSN). Jos vivahde-erot huomioidaan, niin saadaan erillisiä joukkoja, jotka leikkaavat kuitenkin vahvasti toisiaan. Tässä yhteydessä riittää, kun saamme tästä leikkausjoukkojen muodostamasta kokonaisuudesta yleiskuvan. Aloitetaan tarkastelemalla verkostoitumispalvelujen määritelmää tarkemmin (Social networking sites). Kaplan ja Haenlein (2010) ovat määritelleet verkostoitumispalve-

lut sovelluksiksi, jotka edellyttävät henkilökohtaisen profiilin luomista, jotta yhteys muihin saman palvelun käyttäjiin voidaan muodostaa. Pelkkä profiilin luominen ei yksin riitä, vaan muita käyttäjiä kutsutaan jakamaan tietoja oman profiilin kesken. Palveluissa voidaan esittää kaikentyyppistä informaatiota mukaan lukien kuvia, videoita, ääntä, blogeja ja lähettää erilaisia viestejä muille palvelun käyttäjille. Vastaavasti boyd ja Ellison (2007) ovat määritelleet yhteisöpalvelut web-pohjaisiksi palveluiksi, jotka mahdollistavat yksilön (1) luoda julkinen tai puolijulkinen profiili kyseiseen järjestelmään, (2) kommunikoida muiden käyttäjien kanssa, joihin he ovat luoneet yhteyden ja (3) nähdä ja selata näiden muiden yhteysverkostoja. Yhteisöpalvelujen kantava idea on profiilissa, josta meidät voidaan tunnistaa, sekä yhteyksissä, joita muodostamme muihin saman palvelun käyttäjiin. Facebook tuntuu sopivan näihin määritelmiin täydellisesti. Kaikki nämä havainnot sosiaalisen median yleisestä luonteesta ja yhteisöpalvelujen erityispiirteistä ovat oleellisia, kun alamme pohtia Facebookin tietoturvaa. Facebookista puhumme tästä eteenpäin yhteisöpalveluna. Laatimani kuva 1 havainnollistaa Facebookin paikkaa sosiaalisen median käsitteiden kentässä.

3 Mitä on turvallisuus ja tietoturva?

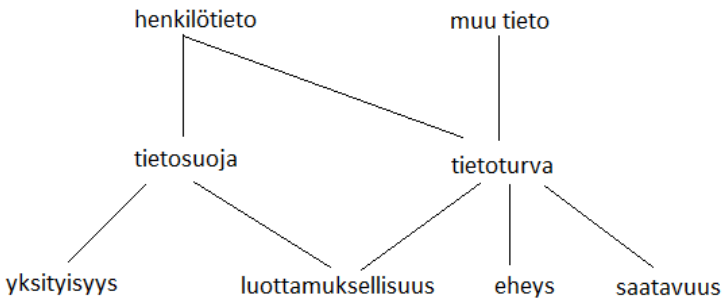
Mitä on turvallisuus ja kuinka se jäsentyy? Limnéll, Majewski ja Salminen (2014) ovat esittäneet turvallisuuden koostuvan neljästä osatekijästä: tunteesta, todellisuudesta, malleista ja sietokyvystä (kuva 2).



Kuvio 2. Turvallisuus. (Limnéll, Majewski ja Salminen 2014)

Mikään näistä tekijöistä yksin ei saa aikaan todellista turvallisuutta, vaan kaikkia elementtejä tarvitaan. Ei riitä, että tuntuu turvalliselta, vaan tunteen tulee vastata vallitsevaa todellisuutta. Malleilla puolestaan tarkoitetaan sitä, kuinka paljon olemme valmiit panostamaan turvallisuuteen, millaisena näemme ja jäsennämme ympäristömme ja miten ympäristö on opettanut meidät suhtautumaan erilaisiin tilanteisiin. Mielestäni tässä on kyse myös koulutuksesta ja tietämyksestä, kuinka erilaisiin tilanteisiin tulisi suhtautua. Oikeanlainen tietämys antaa meille oikeanlaisen mallin toimia vaaran uhatessa. Sietokyky on puolestaan sitä, että emme säikähdä pienestä eli mahdolliset häiriötekijät eivät estä meitä reagoimasta oikein uusissa ja yllättävissäkään tilanteissa. Kaikki nämä neljä turvallisuuden osatekijää voidaan siirtää helposti Facebookin maailmaan.

Tietoturvallisuus ja tietoturva mielletään synonyymeiksi keskenään. Wikipedian mukaan suomenkieleen on vakiintunut käytäntö, joka jaottelee tietoturvan (information security) ja yk-



Kuvio 3. Yksityisyys ja tietoturva.

sityisyyden (privacy). Tämä jako on helppoa havaita myös englanninkielisessä lähdekirjallisuudessa. Rousku (2014, s. 47 – 51) on esittänyt, että tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden takaamista. Luottamuksellisuudella tarkoitetaan sitä, että kulloinenkin tieto on saatavilla vain niille, joilla on sen käyttöön oikeus. Tällöin luottamuksellisuuteen liittyvät todennus, tunnistettavuus ja oikeudellinen kiistämättömyys. Jälkikäteen pitäisi siis pystyä varmuudella sanomaan, kuka on käyttänyt tai muuttanut tietoa, jonka saanti on ollut jollakin ennalta määrätyllä tavalla rajoitettua. Eheydellä tarkoitetaan sitä, että tietojärjestelmässä oleva tieto ei saa muuttua sattumanvaraisesti, eikä sitä saa muuttaa muut, kun ne joilla on siihen oikeus. Saatavuus puolestaan on sitä, että tieto on oikea-aikaisesti saatavilla niille joilla on siihen oikeus.

Yksityisyys on puolestaan oikeus päättää siitä mitkä tiedot ovat julkisia ja mitkä salaisia, siis yksityisiä. Yksityisyyden suojan määrittelee lopulta laki, mutta jokaisella tulisi olla tieto ja käsitys siitä, mitkä henkilökohtaiset tiedot kulkeutuvat eteenpäin ja kenelle, sekä lisäksi niin halutessaaan oikeus ja keinot tietojen leviämisen estämiseksi. Jos jollakin taholla on oikeus toisen yksityisiin tietoihin, niin silloin nämä tiedot ovat usein myös luottamuksellisia. Näin tuntuisi luontevalta, että luottamuksellisuus olisi yksityisyyttä ja tietoturvaa yhdistävä tekijä. Tuntuukin luontevalta puhua sekä tietoturvasta että yksityisyydestä samassa yhteydessä, sillä ne liittyvät kiinteästi toisiinsa. Järvinen (2010, s. 15) on puolestaan määritellyt: "Tietosuoja (eng. privacy) tarkoittaa henkilöön ja hänen toimintaansa liittyvien tietojen suojaamista luvatonta keräämistä ja käyttöä vastaan. Tietosuojan kohteena on ihminen." Oheisessa lainauksessa viitataan yksityisyyden suojaan ja se on käännetty tietosuojaksi. Wikipedias-

sa puolestaan on tietosuojalla viitattu henkilötietojen suojaamiseen. Edellisistä esimerkeistä selviää, että alueen terminologia ei ole täysin vakiintunutta. Tämä puolestaan heijastuu siihen, kuinka on nähty se, mitkä tiedot ovat henkilön identifioivia ja mitkä eivät ole. Jos tietojoukosta poistetaan henkilötiedot, riittääkö se tekemään lopuista tiedoista henkilön kannalta tunnistamattomia, vai voidaanko tiedot kenties liittää henkilön identiteettiin aivan jossakin muussa yhteydessä? Mikä määrittelee sen, milloin tieto on anonyymia? Usein rajanveto on tehty henkilötietojen ja muun tiedon väliin kuten kuva 3 osoittaa, mutta lopputulos riippuu siitä, kuinka laajasti henkilötiedot on määritelty. Henkilötiedoiksi pitäisi pystyä määrittelemään kaikki ne tiedot, joiden avulla yksilö on identifioitavissa.

Mitä on sitten kyberturvallisuus ja kuinka se liittyy tietoturvaan? Voiko Facebookin yhteydessä puhua kyberturvallisuusuhista? Limnéll, Majewski ja Salminen (2014) ovat nähneet kyberturvallisuuden ”bittien maailman” turvallisuutena. Heidän mukaansa *tietoturva* oli jo varattu tarkoittamaan olemassa olevan tiedon turvaamista ja tarvittiin siis uusi käsite, kyberturvallisuus, kattamaan myös tiedon liikkeen turvaaminen. Lisäksi kyberturvallisuus viittaa heidän mukaansa fyysisen ja digitaalisen rajapintaan. Rousku (2014, s. 56) määrittelee kyberturvallisuuden kybertoimintaympäristön kautta. Hänen mukaansa ”kyberturvallisuudella varmistetaan, että kybertoimintaympäristöön voi luottaa ja sen tarkoituksenmukaisesta toiminnasta voidaan huolehtia”. Kybertoimintaympäristön hän määrittelee sähköisessä muodossa olevaksi tietojenkäsittelyyn tarkoitetuksi ympäristöksi, joka koostuu tietojärjestelmistä. *Suomen kyberturvallisuusstrategia* (2013, s. 13) määrittelee kyberuhan: ”Kyberuhka tarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon.” Kyberturvallisuus nähdään siis laajempana kokonaisuutena kuin tietoturva ja siihen nähdään liittyvän myös fyysinen ympäristö, jossa tietoja käsitellään. Tässä valossa voisi esittää, että tietoturvauhka on myös kyberturvallisuusuhka, jos sillä on välittömiä vaikutuksia fyysiseen maailmaan. Pitäydynkin tässä tutkielmassa tietoturva-käsitteessä.

4 Facebookin tietoturva ja yksityisyys

Tässä luvussa nostan esille keskeisimpiä tietoturvan ja yksityisyyden uhkia, joita tutkimuksissa on havaittu liittyvän Facebookiin.

4.1 Identifioivan tiedon tunnistamattomuus ja profilointi

Facebookin perusidea lähtee liikkeelle henkilökohtaisen profiilin luomisesta ja sosiaalisen verkoston muodostamisesta ja ylläpitämisestä muiden käyttäjien kanssa. Profiilin perustiedot ovat jo hyvin identifioivia: nimi, syntymäaika, asuinpaikka, kieli, siviilisääty, uskonto, työpaikka, koulutus, puhelinnumero jne. Ajan kuluessa palveluun ladataan valokuvia ja videoita, jotka sisältävät lisää tietoa toiminnastamme ja henkilökohtaisesta elämästämme. Lisäksi valokuvat sisältävät metadataa, kuvailutietoa, joka tunnetaan valokuvien yhteydessä nimellä EXIF-data. Se sisältää muun muassa kuvan ottopaikan GPS-koordinaatit, jos paikkatieto on ollut kuvaushetkellä saatavilla, tekniset tiedot kuvauslaitteesta ja sen asetuksista. Jotkut laitteet kirjoittavat EXIF-dataan jopa käytetyn laitteen sarjanumeron (Järvinen 2010). Facebookiin rekisteröidyttäessä tarvitaan ainakin yksi sähköpostiosoite tai puhelinnumero. Heti rekisteröitymisvaiheessa Facebook haluaa tuoda yhteystietosi sähköpostistasi tai puhelimestasi. Lisätietoja-kohta kertoo tuonnista seuraavaa: "Tuo yhteystiedot tilistäsi ja tallenna ne Facebookin palvelimiin, joissa niillä voidaan auttaa muita etsimään kavereitaan ja luomaan yhteyksiä heihin tai luomaan ehdotuksia sinun tai muiden puolesta. Tiedot yhteystietolistaltasi ja viestikansioistasi voidaan tuoda. Työyhteystiedot voidaan tuoda, mutta lähetä kutsuja vain henkilökohtaisille tutuillesi. Lähetä kutsuja vain kavereille, jotka haluavat saada niitä." Tuonnista siis kyllä kerrotaan, jos asiaa huomaa tarkastella, mutta varsinainen tuonti on naamioitu Etsi kavereita -toiminnon alle. Kukapa ei haluasi löytää nopeasti kavereita. Haluatko jakaa paikkatietosi? Mitä seurauksia siitä voisi olla? Näitä kysymyksiä on hyvä esittää itselleen. Joillakin on tapana jakaa lenkkitietonsa Facebookissa, kuten Sport Trackerin keräämät tiedot, joista käy mahdollisesti ilmi kellonaika, paikka, syke, otetut askeleet jne. Voisiko näistä tiedoista päätellä esimerkiksi jotain henkilön terveydentilasta ja voisiko tieto kiinnostaa esimerkiksi vakuutusyhtiötä? Kuten nimikin kertoo, Facebook on ”naamakirja”. Passikuvan typpinen tarkka kasvokuva sisältää kaiken sen informaation, joka tarvitaan

biometrisen tunnistetiedon määrittämiseen. Lisäksi Facebook sisältää valokuvien taggäämistoiminnon. Toiminto pyytää sinua tunnistamaan kuvissa näkyvät kasvot ja merkitsemään eli taggäämään, henkilön. Varmasti löytyy aina kaveri, joka merkitsee sinutkin kuvaan, vaikka et sitä itse haluaisikaan. Kerran merkitty on aina merkitty. Digitaalisessa maailmassa ei ole peruutusvaihdetta. On hyvä ymmärtää, että tietojen poistaminen näkyviltä ei ole sama asia, kuin että ne olisivat peruuttamattomasti poistettu tietokannoista. Jälkeemme jää digitaaliset jalanjälkemme, joita on mahdotonta lakaista pois.

Kaikki edellä kuvattu yksityinen tieto avaa mahdollisuudet profiloinnille ja sitä kautta muun muassa kohdennetulle mainonnalle. Yksi profiloinnin seurauksena ilmenevä riski on niin sanottu kuplailmiö, jossa henkilön ympärillään havaitsema mainonta ja uutisointi on muokattu profiloinnin tuloksia vastaaviksi. Pitkälle vietynä tämä voi supistaa henkilön kuvaa ympäristöstään ja ikään kuin eristää henkilön, hänen ystävänsä ja aatteensa ” kuplan sisään”. Profiloinnin tarkkuus voi yllättää. On nimittäin esitetty, että Facebook voi ennustaa parisuhteen alkamisen ja päättymisen, ennen kuin henkilöt edes itse tietävät siitä (Järvinen 2014, s. 276). Facebook itse ei kuitenkaan ole ainoa tietojen hyödyntäjä. Muun muassa kansalliset turvallisuuspalvelut ovat kiinnostuneita yhteysverkostoista, profiileiden sisältämästä tarkasta tiedosta ja ihmisten keskinäisestä viestinnästä. On esitetty, että esimerkiksi NSA:lla on ollut suora pääsy Facebookin palvelimille ja sitä kautta kaikkeen siellä olevaan tietoon (Verble 2014). Lisäksi erilaiset yritykset ja yksityiset ihmisetkin voivat harrastaa Facebookissa tiedonlouhintaa samanlaisin yksinkertaisin keinoin kuin Edward Snowden todennäköisesti varasti tietonsa NSA:lta, hyödyntämällä Webin hakukoneiden kaltaista ryömijää (crawler) (Järvinen 2014). Esimerkiksi Catanese ym. (2011) ovat esittäneet, kuinka tiedonlouhinta ja analysointi onnistuu yksinkertaisin keinoin, muun muassa Wget-ohjelmaa hyödyntäen. Tutkimukseni aikana kokeilin itsekin Facebookin sosiaalisen verkoston graafista analysointia. Käytännössä loin graafisen näkymän kaverien ja kaverien kaverien keskinäisistä yhteyksistä. Tämä osoittaa sen, että vaikka Facebook on estänyt joitakin toimintoja GraphAPI:nsa kautta, niin tiedot voivat levitä muilla keinoilla. Lait ja asetukset vaihtelevat maakohtaisesti, mutta Facebook on globaali-ilmiö, joten tietojensa ei voi ajatella olevan suojassa, vaikka kansallinen laki niin vaatisikin.

4.2 Yksityisyysasetukset

Facebook sisältää monia asetuksia, jotka liittyvät turvallisuuteen ja yksityisyyteen. Facebookissa on myös erikseen nimetyt asetukset turvallisuudelle ja yksityisyydelle, mutta kategorisointi on hiukan harhaanjohtava, sillä yksityisyyden ja turvallisuuden alle kuuluvia asetuksia löytyy muualtakin. Esimerkiksi sovellus- ja mainosasetuksissa on selkeästi yksityisyyden alle kuuluvia asetuksia. Tarkastellaan aluksi asetuksia, jotka tunnetaan nimellä yksityisyys ja joiden avulla on tarkoitus määritellä se, kenellä on pääsy ja millä ehdoilla profiilien sisältämään informaatioon. Käyttäjä voi siis valita kuka näkee hänen statuksensa, linkkinsä ja kuvansa valitsemalla sopivan ryhmän listalta. Valittavana ovat ryhmät: julkinen, kaverit, vain minä ja mukautettu. Ensimmäisellä statuksen julkaisukerralla Facebook kysyy, kenen haluat näkevän julkaisusi. Valintavaihtoehdot ovat kaverit ja julkinen. Facebook lupaa muistaa asetukset jatkossa. Oma kokemus on kuitenkin osoittanut, että asetukset ja asetusten vaikutusalue saattavat muuttua alustan päivitysten myötä, joten asetukset tulisi tarkistaa säännöllisin väliajoin. Lisäksi Facebookiin on varsinaisen selainpohjaisen käyttöliittymän lisäksi tarjolla monia vaihtoehtoja. Joissakin ympäristöön integroiduissa sovelluksissa, kuten esimerkiksi Windows Phonen Facebook-sovelluksessa, asetusvaihtoehtoja on vaikea löytää tai niiden käyttö on kokonaan estetty. Tämä voi johtaa siihen, että mobiilikäyttäjällä on erilainen kuva valittavista asetuksista ja sitä kautta myös vallitsevasta turvallisuuden tilasta.

Albesher ja Alhussain (2013) ovat esittäneet kolme keskeistä syytä, miksi yksityisyysasetukset jäävät vaille asianmukaista huomiota. Ensiksi, käyttäjät eivät tiedosta niitä mahdollisia riskejä, jotka liittyvät asetusten huomiotta jättämiseen. Tähän on varsin inhimillinen syy. Kuten aikaisemmin totesin, Limnéll, Majewski ja Salminen (2014) ovat esittäneet turvallisuuden koostuvan neljästä osatekijästä: tunteesta, todellisuudesta, malleista ja sietokyvystä (kuva 2). Facebookissa tunne saattaa helposti irroittautua todellisuudesta. Kontaktit tuttuihin kavereihin lisäävät tunnetta turvallisuudesta, jolloin mahdollisten riskien ajattelu jää taka-alalle. Vain tietoisuus vallitsevasta todellisuudesta sekä tiedostetut oikeat toimintamallit voivat parantaa tilannetta ja lisätä todellista turvallisuutta. Toiseksi, he ovat nostaneet esille asetusten suuren määrän ja mahdollisen vaikeatajuisuuden siitä, miten ja mihin mikäkin asetus vaikuttaa. Kuten aikaisemmin todettiin, yksityisyyden alle kuuluvia asetuksia löytyy monesta paikasta. Kolmanneksi tekijäksi he nostivat edellisistä havainnoista johdetun ase-

tusten kompleksisuuden, asetuksia on paljon ja ne ovat hajallaan. Lisäksi osaa asetuksista voidaan muuttaa esimerkiksi mobiilisovelluksen kautta. Tällaiseen tapaukseen olen törmännyt, kun tabletilla pelatun pelin jälkeen onkin statukseeni ilmaantunut yllättäen tietoja pelistä ja siinä saavutetuista tuloksista. Huomaamattani olin antanut sovellukselle luvan julkaista tietoja Facebookissa ja samalla muokata yksityisyysasetuksiani. Lisäksi kaikki sovellus- ja mainosasetukset on Facebookissa asetettu oletuksena sallimaan kaikki. Lisäksi sovellusten kohdalla erityisesti pätee se, että mikä on mahdollista, sen myös joku toteuttaa. Niinpä asetuksilla ei voida estää yksityisyyden piiriin kuuluvien henkilökohtaisten tietojen vuotamista vihamielisten sovellusten kautta. Ainoa varma keino näyttää olevan kaikkien kolmannen osapuolen sovellusten käytön estäminen. Huomionarvoinen seikka on myös se, että kaverilista on oletusarvoisesti kaikkien nähtävillä.

Facebook on kokenut monia muutoksia historiansa aikana, siihen on tehty monia lisäyksiä, ehtoja, asetuksia ja tyyliä on muutettu. Alun perin opiskelijoille tarkoitetusta ympäristöstä on tullut kaikkien saatavilla oleva yhteisöpalvelu, jonka ovat löytäneet myös yritykset. Toimintakenttä on siis muuttunut ja tulee varmasti muuttumaan myös jatkossa, seuraavina verkostoitujina voidaan nähdä koneet – Things of the Internet.

4.3 Sovellukset

Muun muassa Albesher ja Alhussain (2013) sekä Fokes ja Li (2014) ovat nostaneet Facebookin merkittäväksi tietoturvauhaksi sovellukset. Facebook tukee erityyppisiä sovelluksia, kuten IOS, Android, Canvas ja web-sovellukset. Nämä sovellukset ovat niin sanottuja kolmannen osapuolen sovelluksia, joita sovelluksen luojat ylläpitävät omilla tahoillaan. Sovelluksia käytetään Facebookiin kirjautuneena ja käyttäjän tulee luovuttaa sovelluksen pyytämät tiedot itsestään sovelluksen käyttöön. Jokaisella sovelluksella on omat käyttöehtonsa ja sääntönsä, joiden sisältöön Facebook ei voi vaikuttaa. Sovellus voi siis olla hyvä tai paha. Facebookin yksityisyydensuojan kontrolli ei ulotu sovelluksiin, ainoastaan Facebookin Graph API edellyttää sovelluksen pyytävän käyttäjältä valtuudet erilaisten tietojen lukemiseen Facebookista; käyttäjälle jää päättely siitä, millaisia tietoja hän on luovuttamassa. Tosiasiassa sovellukset voivat käyttää saamiaan tietoja ihan kuten haluavat. Ne voivat jakaa tietoja keskenään tai muiden ulkopuolisten toimijoiden kanssa. Tiedot saattavat siten päätyä vaikka yritykselle,

joka myy tietoja eteenpäin. (Albesher ja Alhussain 2013) Näin henkilökohtaisista tiedoista on tullut kauppatavaraa.

Oletuksena Facebookin sovellusalusta on päällä ja sallii muun muassa ystävien jakaa tietoja sinusta sovelluksille. Tämä on selkeä tietoturvariski. Yksityisyyden suojaamiseksi kaikki tietojen jako pitäisi olla oletuksena estetty, ellei käyttäjä nimenomaan halua jakaa tietojaan, valinta tulisi olla käyttäjällä. Nyt kaikki on sallittu, ellei jotain näistä ole erikseen estetty. Varmin tapa estää tietojen vuotaminen eteenpäin on poistaa koko sovellusalusta käytöstä. Jos sovelluksia haluaa kuitenkin käyttää, niin niiden tekijät tulisi olla luotettuja, minkä varmistaminen on erittäin hankalaa. Lisäksi ystävien käyttämiltä sovelluksilta on hyvä estää omien tietojen oletusarvoinen käyttö. Sekään ei kaikissa tapauksissa estä omien tietojen leviämistä ystävien profiilien kautta.

4.4 Evästeseuranta

Evästeseuranta on useissa lähteissä mainittu menetelmä, mutta sen tarkkaa toimintamekanismia ei useinkaan selitetä. Evästeet ovat pieniä tietueita, jotka web-palvelin pyytää selainta tallentamaan koneelle. Evästeitä on kahta päätyyppiä: istuntokohtaisia ja pysyviä. Perusidea on se, että selain lähettää http-pyynnön mukana kulloisenkin palvelimen evästeet, jolloin palvelin voi tunnistaa yhteyden takana olevan koneen. Pysyvä eväste taas puolestaan kertoo uuden istunnon alkaessa esimerkiksi aikaisemmin valituista sivukohtaisista asetuksista. Eväste ei siis vielä mitenkään identifioi käyttäjää, mutta liittää tietyn selaimen ja koneen kyseisen palvelupyynnön lähettäjäksi. Http-pyynnön *User-Agent* -tietokenttä sisältää myös koneen käyttämän IP-osoitteen, perustiedot käyttöjärjestelmästä ja selaimesta. Alun perin tilattoman yhteyden yli on saatu näin kontrolli. Tällaisia evästeitä kutsutaan ensimmäisen osapuolen tai ensimmäisen asteen evästeiksi. Koska webin periaatteiden mukaan sivun sisältö voi olla linkitettyä eli mainokset, kuvat tai artikkelit voivat sijaita fyysisesti toisilla palvelimilla, niin nämäkin palvelimet voivat pyytää puolestaan selainta tallettamaan omat evästeensä. Näitä evästeitä kutsutaan kolmannen osapuolen evästeiksi. Nimi on kuvaava, sillä se kertoo ylimääräisestä tahosta kahdenkeskisessä toiminnassa. Nämä evästeet mahdollistavat tietyissä tapauksissa käyttäjän seurannan. (Tranberg, Heuer ja Laukkanen 2013) Yleisesti seuranta perustuu siihen, että kun esimerkiksi sama mainos on linkitetty monelle web-sivustolle

ja kun käyttäjä selaa näiltä sivuilta toiselle, niin joka kerta hänen selaimensa lähettää tämän kolmannen osapuolen evästeen kyseiselle palvelimelle. Tuloksena on ikään kuin kartta käyttäjän liikkumisesta verkossa. Niin kauan kuin käyttäjää ei voida identifioida tarkasti, ei seuranta luo merkittävää uhkaa yksityisyydelle. Tilanne muuttuu, jos identifiointi onnistuu jollakin menetelmällä riittävän luotettavasti.

Chaabane, Kaafar ja Boreli (2012) ovat esittäneet Facebookin käyttämän mekanismin, jolla käyttäjä voidaan identifioida tarkasti ja merkittävä osa hänen selaushistoriaansa voidaan liittää hänen profiiliinsa. Kun otetaan huomioon se, että Facebookin liiketoiminta nojaa kohdennetulle mainonnalle ja joissakin tapauksessa tietojen myymiselle, niin voidaan tulla siihen johtopäätökseen, että kyseinen toiminta muodostaa merkittävän tietoturvan ja yksityisyyden uhan. Lisäksi tämä tietojen keruu tapahtuu useimmiten käyttäjän sitä tiedostamatta. Lisäksi selaushistorian keruu on mahdollista, vaikka käyttäjä ei olisi edes kirjautuneena Facebookiin tai hän ei olisi edes rekisteröytynyt vielä palvelun käyttäjäksi (Chaabane, Kaafar ja Boreli 2012).

Chaabane, Kaafar ja Boreli (2012) ovat esittäneet, kuinka Facebook käyttää yhteensä 16 evästettä aktiivisen istunnon hallintaan, joista ainakin kahta, *datr* ja *d_user*, käytetään seurannan toteuttamiseen. Mekanismi on mielenkiintoinen, sillä riittää pelkästään se, että käyttäjä vierailee Facebookin web-sivuilla, jo tällöin asetetaan *datr*-eväste, joka on oletusarvoisesti voimassa kaksi vuotta. Varsinaisen seurantamekanismin muodostavat Facebookin aktiiviset elementit, kuten Tykkää-napit, joita on monilla web-sivuilla. Tällaiselle sivulle tuleminen jo pelkästään saa aikaan sen, että kyseisen sivun osoite ja edellä mainittu eväste lähetetään Facebookille http-kyselyn mukana. Eväste pitää siis huolen siitä, että selailukartta alkaa hahmottua, enää puuttuu vain käyttäjän tarkka identifiointi. Kun käyttäjä sitten mahdollisesti rekisteröityy Facebookin käyttäjäksi ja kirjautuu palveluun, astuu mukaan toinen eväste, *d_user*. Yhdessä *datr* ja *d_user* nyt liittävät selailuhistorian käyttäjän profiiliin. Mekanismi aktivoituu aina uudelleen samalla tavalla evästeiden poiston jälkeen.

Oheisella mekanismilla käyttäjästä pyritään keräämään tärkeää tietoa, jolla profiilia voidaan täydentää ja parantaa tätä kautta muun muassa kohdennetun mainonnan tehoa. Ensimmäinen askel tältä uhalta suojautumiseen on asian tiedostaminen. Kun asia on tiedostettu, toimenpiteet yksityisyyden ja tietoturvan parantamiseksi ovat suoraviivaisia: ei selailla web-sivuja

Facebookiin kirjautuneena, poistetaan selailuhistoria ja talletetut evästeet selaimesta poistuttaessa Facebookista ja poistetaan evästeet myös ennen kirjautumista Facebookiin. Käytännössä tämä hoituu sillä, että asetetaan selain poistamaan automaattisesti kaikki evästeet istunnon lopuksi ja kielletään selainta tallentamasta kolmannen osapuolen evästeitä. Kaiken kaikkiaan on merkille pantavaa se, että Facebook ei ole ainoa sosiaalisen median palvelu, joka käyttää kuvatunlaista seuratamekanismia. Muun muassa Twitter ja Google+ toimivat jopa vieläkin ovelammin. (Chaabane, Kaafar ja Boreli 2012; Tranberg, Heuer ja Laukkanen 2013)

4.5 Valeprofiilit, Sybil-hyökkäys ja identiteettivarkaus

Valeprofiiliit ovat nimensä mukaisesti profiileja, joiden tiedot eivät pidä paikkaansa ja joiden tarkoituksena on harhauttaa muita käyttäjiä omien tarkoitusperien saavuttamiseksi. Usein nämä tarkoitusperät ovat vahingollisia muille käyttäjille. Valeprofiilit liittyvätkin usein seksuaalirikoksiin, huijauksiin, erilaisten hyökkäysten valmisteluun ja toteutukseen. Facebookin profiiliin voi rekisteröityessä antaa keksityt tiedot, niiden alkuperää tai aitoutta ei tarkasteta millään tavalla. Sähköpostiosoite tai puhelinnumero vaaditaan, mutta nämäkin voivat olla täysin identifioimattomia, kuten väärillä tiedoilla luotu sähköpostiosoite tai anonyymi prepaid-liittymänumero. Valeprofiilin takaa on myös helppo levittää väärää tietoa ja tehdä muuta kiusaa. Valeprofiilit on viime aikoina liitetty myös trollaukseen, jonka tarkoituksena on sekaannuksen ja hämmennyksen aiheuttaminen omien tarkoitusperien vahvistamiseksi. Poliittisella tasolla tämä voi tarkoittaa epävarmuuden lisäämistä ennakoitavalla tavalla niin, että esimerkiksi tämä epävarmuus vaikuttaa trollaajan haluamalla tavalla äänestystulokseen. Monet käyttäjät ovat liian luottavaisia muiden hyvään tarkoitusperään myös verkossa. Monet ihmiset kilpailevat siitä, kenellä on suurin sosiaalinen verkosto ja hyväksyvät kavereikseen kaikki, jotka lähettävät kaveripyynnön. Luottamus on määritelty yksilön vapaaehtoisuudeksi asettua haavoittuvaan asemaan, koska uskoo vahvasti siihen, että toisen toimet ovat hyviä. Luottamusta lisää helposti se, että joku jo tunnettu kaveri on tämän uuden kaveriehdokkaan kaveri. (Fokes ja Li 2014; Limnéll, Majewski ja Salminen 2014; Tranberg, Heuer ja Laukkanen 2013)

Aina ei kuitenkaan valeprofiilin tarvitse kertoa pahoista aikeista. Valeprofiili voi liittyä myös

ns. virtuaalisiin verkkoyhteisöihin, jotka on luotu esimerkiksi Facebookin sisälle. Näissä tapauksissa väärien profiilitietojen ensisijainen tarkoitus on piilottaa käyttäjän oikeat tiedot Facebookin muilta käyttäjiltä, siis suojella yksityisyyttä virtuaalisen verkon ulkopuolella. Vain muilla virtuaaliverkon jäsenillä on tiedot muiden todellisesta henkilöllisyydestä. Yksinkertaisimmillaan Facebookin sisällä oleva virtuaaliverkko voisi perustua pelkästään käyttäjien keskinäiseen sopimukseen väärien henkilöprofiilien käytöstä. Satunnaiseen kommunikointiin menetelmä on varmasti riittävä, mutta toistuvassa yhteydenpidossa hankala. Niinpä virtuaaliverkkojen toteutukseen on kehitetty erilaisia malleja. Yksi mielenkiintoisista malleista perustuu väärien henkilötietojen korvaamiseen oikeilla Facebook-istunnon aikana. Kunkin käyttäjän oikeat tiedot on talletettu esimerkiksi xml-tiedostoon ja jaettu luotettavan kanavan kautta verkon muille käyttäjille. Facebookia käytetään Firefox-selaimella ja Firefox-liitännäinen huolehtii valeprofiilin väärien tietojen korvaamisesta oikeilla. Amsden, Chen ja Yuan (2014)

Toinen idea perustuu steganografiaan eli tiedon piilottamiseen. Tällaisessa lähestymistavassa profiilin oikeat tiedot voitaisiin piilottaa muun profiilissa esiintyvän datan joukkoon. Amsden, Chen ja Yuan (2014) ovat tutkineet steganografian käyttöä Facebookissa ja todenneet tiedon piilottamisen, salauksen ja purkamisen mahdolliseksi, kun piilottamiseen käytetään esimerkiksi JPHide-ohjelmaa ja tieto piilotetaan oikean kokoiseen kuvaan, joka ladataan Facebookin kansikuvaksi. Vaikka Facebook muokkaa talletettavaa kuvaa jonkin verran, niin kansikuvassa piilotetut tiedot säilyvät ja niiden purkaminen onnistuu. Niinpä kunkin virtuaaliverkon jäsenen tiedot voitaisiin piilottaa kansikuvaan ja purkaa ne ulos reaaliaikaisesti, vaikka sopivan liitännäisen avulla, joka automatisoisi toiminnot. Steganografisen sisällön löytäminen on osoittautunut haastavaksi tehtäväksi. Ja vaikka joistakin kuvista voitasiin päätellä niiden mahdollisesti sisältävän piilotettua informaatiota, niin tiedon riittävä salaus luo vielä omat haasteensa. Vuosituhannen alussa Provos ja Honeyman (2001) päätyivät etsimään eBayn ja USENETin kuvista steganografista sisältöä, kun liikkeellä oli huhuja siitä, että terroristit käyttävät kuvia hyökkäyssuunnitelmiensa välittämiseen. Provos ja Honeyman (2001) analysoivat yli 2 miljoonaa kuvaa, eivätkä onnistuneet löytämään yhtään viestiä. Joko viestejä ei ollut tai niitä ei saatu puretuksi.

Kun luodaan kokonainen valeprofiilien joukko omien tarkoitusperien edistämiseksi puhu-

taan Sybil-hyökkäyksestä. Sybil-hyökkäys on saanut nimensä samannimisestä kirjasta, joka kuvaa erään naisen dissosiatiivista identiteettihäiriötä. Sybil-hyökkäyksen tekijä luo monia rinnakkaisia valeprofiileja tarkoituksenaan niiden avulla harhauttaa muita käyttäjiä tai jotakin järjestelmää. Harhautukselle alttiita ovat esimerkiksi erilaiset äänestysjärjestelmät, joiden avulla kerrotaan mielipide jostakin tuotteesta tai palvelusta. Samoin yleistä mielipidettä jostakin asiasta voidaan pyrkiä muokkaamaan Sybil-hyökkäyksen keinoin. (Fokes ja Li 2014)

Identiteettivarkaus on toisen identiteetin haltuunotto. Usein tällöin puhutaan salasanan murtamisesta tai tunnusten saamisesta muilla keinoin, kuten huijaamalla. Salasanat ja käyttäjätunnukset voivat päätyä luvattomiin käsiin myös verkkoseurannan kautta. Näissä tapauksissa henkilö voi joutua esimerkiksi mies välissä -hyökkäyksen kohteeksi, jolloin hyökkääjä saa luettua käyttäjän verkkotunnukset ja salasanat istunnon alkaessa. Facebookin kirjautumisen yhteydessä mahdollisesti ilmaantuva sertifikaattivaroitus on syytä ottaa vakavasti. Myös valesivustot ovat yleinen keino käyttäjätunnusten ja salasanojen haltuunsaamiseksi. Näissä tapauksissa henkilö luulee kirjautuvansa Facebookiin, mutta syöttääkin tunnuksensa hyökkääjän väärentämälle ja uudelleen ohjaamalle verkkosivulle. Monia muitakin verkkoteknologiaan ja webin toimintaperiaatteisiin liittyviä tekniikoita löytyy ja ne ovat samoja kuin muidenkin palvelujen kohdalla tunnetuksi tulleet menetelmät. Fokes ja Li (2014) ovat myös esittäneet, että vanhentuneet sähköpostiosoitteet, joita käytetään edelleen Facebookin käyttäjätunnuksina ovat selkeä riski. Heidän mukaansa esimerkiksi Hotmailin ja Windows Liven käyttäjät ovat alttiita hyökkäykselle, joissa hyökkääjä ottaa käyttöönsä vanhentuneen sähköpostiosoitteen ja pyytää Facebookilta salasanan nollausta tähän osoitteeseen.

5 Yhteenveto

Alussa asetin tavoitteekseni kartoittaa Facebookin tietoturvauhkia ja etsiä keinoja, joilla uhkia voidaan torjua käyttäjälähtöisesti. Lähdin liikkeelle määrittelemällä ensin turvallisuus-, tietoturva- ja yksityisyyskäsitteen. Turvallisuus on sopivassa suhteessa tunnetta, todellisuutta, oikeaa asennetta ja vallitsevan tilanteen sietokykyä. Tähän näkemykseen on mielestäni helppo yhtyä. Tämä on myös se malli, jonka Limnéll, Majewski ja Salminen (2014) ovat esittäneet kuvaa turvallisuuden käsitettä selkeästi ja ymmärrettävästi. Huomattavasti enemmän pohdintaa aiheuttaa tietoturvan ja yksityisyyden käsitteet ja niiden keskinäinen suhde. Näyttää siltä, että yksityisyys mielletään liittyvän niihin identifioiviin tietoihin, jotka liittyvät suoraan meidän henkilöllisyyteemme ja siten paljastavat keitä todella olemme. Tutkimuksen valossa jako ei kuitenkaan ole kaavakuvamaisen selkeä, vaikka erilaiset palveluntarjoajat asian usein näin esittävätkin. Facebook ja monet muut tahot sanovat suojelevansa yksityisyyttämme pitämällä henkilökohtaiset tietomme salassa ja käyttävänsä kaupallisiin tarkoituksiinsa vain niitä tietoja, jotka eivät paljasta meidän henkilöllisyyttämme. Näitä tietoja he myös välittävät kolmansille osapuolille osana liiketoimintaansa. Puhutaan niin sanotusta anonyymista datasta. Tällaisten tietojen kulkeutuminen kolmansille osapuolille on mielestäni selkeä riski, koska osa näistä tiedoista voidaan kolmansien osapuolten toimesta liittää takaisin henkilöllisyyteemme tiedon uudelleenyhdistämisteorian mukaisesti. Tämä on asia, joka pitäisi ottaa paremmin huomioon määriteltäessä rajoja sille kaupallisille toiminnalle, joka liittyy ja pohjautuu meistä kerättäviin tietoihin. Yksityisyyden käsitteen tulisi perustua siihen, että jokaisella tulisi olla oikeus kaikkiin itseään koskeviin tietoihin ja siihen, mitä ja kuinka näitä tietoja käytetään ja kenelle niitä luovutetaan.

Sosiaalisen median käsitteen tarkastelu auttoi huomamaan sen, että monet tietoturvauhat ovat yhteisiä eri sosiaalisen median sovelluksille, sillä kaikki sosiaalisen median palvelut perustuvat Web 2.0:aan ja ovat sen ideologian ilmentymiä. Näin esimekiksi http-protokollan toimintaperiaatteet mahdollistavat evästeseurannan, verkkoseurannan ja salasanojen kaappaamisen. Kuitenkin Facebookilla on omat erityispiirteensä, jotka liittyvät profiileihin, kommunikointitapoihin ja yhteysverkostoihin. Facebookin ideologia jo sinänsä luo edellytykset profiloinnille. Tämä voi tapahtua helposti muun muassa verkostoja seuraamalla ja niitä ana-

lysoimalla. Keskeisimmiksi uhiksi olen nostanut profiloinnin, Facebookin osittain sekavat ja yllättäen muuttuvat yksityisyysasetukset sekä Facebookin sovellukset, jotka ovat kolmansien osapuolten ylläpitämiä ja siten Facebookin kontrollin ulkopuolella.

Tekemieni havaintojen mukaan erilaisten hyökkäystyökalujen ja niihin liittyvän ohjeistuksen löytäminen on yllättävän helppoa. Merkillepantavaa on muun muassa se, kuinka esimerkiksi salasanojen murtamiseen ja verkkoliikenteen seuraamiseen tarkoitettuja työkaluja on helposti saatavilla. Tämä oli minulle yllätys. Lisäksi yleisenä havaintona on se, että useimmissa tapauksissa hyökkäyksen tai haitanteon onnistuminen näyttää riippuvan hyökkääjän motivaatiosta. Hyökkääjällä on usein aikaa ja mahdollisuuksia miettiä keinojaan lähes loputtomasti, kun taas hyökkäyksen kohteen olisi pitänyt valmistautua kaikkiin mahdollisiin tapauksiin etukäteen. Tutkimuksen aikana minulle on hahmottunut kuva siitä, että keskeisin keino uhkien torjunnassa on tietoisuuden lisääminen olemassa olevista uhista, ja sitä olen pyrkinyt tekemään tässä työssäni kuvaamalla keskeisiä uhkia ja niiden mekanismeja riittävän selkeästi. Mielestäni asian voi tiivistää puolustusstrategian termein: "Uskottava puolustuskyky edellyttää riittävää ja uskottavaa hyökkäyskykyä." Edellinen väittämä nostaa esille asiaan liittyvän viestinnän haasteellisuuden. Ilman riittävää tietoa hyökkäysmekanismeista suojautuminen on mahdotonta, mutta samalla levitetään tietoa, joka palvelee myös hyökkääjiä. Tähän tuntuu kuitenkin pätevän sääntö, että "möröt asuvat pimeässä" ja hyökkääjät etsivät kohteikseen niitä, joilla ei ole riittävää tietoa ja kykyä suojautua.

Lähteet

Albesher, Abdulmohsen, ja Thamer Alhussain. 2013. “Privacy and Security Issues in Social Networks: An Evaluation of Facebook”. Teoksessa *Proceedings of the 2013 International Conference on Information Systems and Design of Communication,* 7–10. ISDOC ’13. Lisboa, Portugal: ACM. ISBN: 978-1-4503-2299-7. http://doi.acm.org.ezproxy.jyu.fi/10.1145/2503859.2503861.

Amsden, N. D., Lei Chen ja Xiaohui Yuan. 2014. “Transmitting hidden information using steganography via Facebook”. Teoksessa *Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on,* 1–7. ID: 1.

Bilge, Leyla, Thorsten Strufe, Davide Balzarotti ja Engin Kirda. 2009. “All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks”. Teoksessa *Proceedings of the 18th International Conference on World Wide Web,* 551–560. WWW ’09. Madrid, Spain: ACM. ISBN: 978-1-60558-487-4. http://doi.acm.org.ezproxy.jyu.fi/10.1145/1526709.1526784.

boyd, danah m., ja Nicole B. Ellison. 2007. “Social Network Sites: Definition, History, and Scholarship”. *Journal of Computer-Mediated Communication* 13 (1): 210–230.

Catanese, Salvatore A., Pasquale De Meo, Emilio Ferrara, Giacomo Fiumara ja Alessandro Provetti. 2011. “Crawling Facebook for Social Network Analysis Purposes”. Teoksessa *Proceedings of the International Conference on Web Intelligence, Mining and Semantics,* 52:1–52:8. WIMS ’11. Sogndal, Norway: ACM. ISBN: 978-1-4503-0148-0. http://doi.acm.org.ezproxy.jyu.fi/10.1145/1988688.1988749.

Chaabane, Abdelberi, Mohamed Ali Kaafar ja Roksana Boreli. 2012. “Big Friend is Watching You: Analyzing Online Social Networks Tracking Capabilities”. Teoksessa *Proceedings of the 2012 ACM Workshop on Workshop on Online Social Networks,* 7–12. WOSN ’12. Helsinki, Finland: ACM. ISBN: 978-1-4503-1480-0. http://doi.acm.org.ezproxy.jyu.fi/10.1145/2342549.2342552.

Fokes, Elizabeth, ja Lei Li. 2014. “A Survey of Security Vulnerabilities in Social Networking Media: The Case of Facebook”. Teoksessa *Proceedings of the 3rd Annual Conference on Research in Information Technology,* 57–62. RIIT ’14. Atlanta, Georgia, USA: ACM. ISBN: 978-1-4503-2711-4. http://doi.acm.org.ezproxy.jyu.fi/10.1145/2656434.2656444.

http://www.statista.com. *http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.*

Järvinen, Petteri. 2010. *Yksityisyys : turvaa digitaalinen kotirauhasi* [kielellä fin]. 351 s. Jyväskylä: Docendo. ISBN: 978-951-0-36157-3 (sid.)

———. 2014. *NSA : näin meitä seurataan.* 323 s. Jyväskylä: Docendo Oy. ISBN: 978-952-291-046-2.

Kaplan, Andreas M., ja Michael Haenlein. 2010. “Users of the world, unite! The challenges and opportunities of Social Media”. *Business horizons* 53 (1): 59–68.

Limnéll, Jarno, Klaus Majewski ja Mirva Salminen. 2014. *Kyberturvallisuus* [kielellä fin]. 246 s. Jyväskylä: Docendo. ISBN: 978-952-291-047-9.

Provos, Niels, ja Peter Honeyman. 2001. *Detecting steganographic content on the internet.*

Rousku, Kimmo. 2014. *Kyberturvaopas : tietoturvaa kotona ja työpaikalla* [kielellä fin]. 326 s. Helsinki: Talentum. ISBN: 978-952-14-2226-3.

Suomen kyberturvallisuusstrategia [kielellä fin]. 2013. 40 s. Valtioneuvoston periaatepäätös 24.1.2013. Helsinki: Turvallisuuskomitean sihteeristö. ISBN: 978-951-25-2433-4 (nid.)

Tranberg, Pernille, Steffan Heuer ja Mauri Laukkanen. 2013. *Älä kerro kaikkea! : itsepuolustusopas verkkoon.* [kielellä fin]. 263 s. Helsinki: Talentum. ISBN: 978-952-14-2007-8 (nid.)

Tuunainen, Virpi Kristiina, Olli Pitkänen ja Marjaana Hovi. 2009. “Users’ Awareness of Privacy on Online Social Networking sites-Case Facebook”. *Bled 2009 Proceedings:* 42.

Verble, Joseph. 2014. “The NSA and Edward Snowden: Surveillance in the 21st Century”. *SIGCAS Comput.Soc.* 44, numero 3 (lokakuu): 14–20. http://doi.acm.org.ezproxy.jyu.fi/10.1145/2684097.2684101.