Tamminen Jimi

MOBIILIMAKSAMISEN TURVALLISUUSUHAT JA NIIDEN TORJUNTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Tamminen, Jimi
Mobiilimaksamisen turvallisuusuhat ja niiden torjunta
Jyväskylä: Jyväskylän yliopisto, 2018, 33 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Luoma, Eetu

Tässä kandidaatin tutkielmassa esitellään kirjallisuuskatsauksen keinoin mobiilimaksamista, siihen liittyviä turvallisuusuhkia ja niiden torjuntatapoja. Tutkielmassa esitellään mobiilimaksamisen tärkeimmät ominaisuudet ja toimintatavat. Lisäksi tutkielmassa esitellään mobiilimaksamisen mahdollistavia teknologioita. Mobiilimaksamisen suosion arvioidaan kasvavan huomattavasti tulevien vuosien aikana ja yksi tärkeimmistä tekijöistä mobiilimaksamisen käyttöönoton kannalta on turvallisuus. Turvallisuus on mobiilimaksamisessa tärkeässä asemassa, sillä mobiilimaksujärjestelmät käsittelevät arkaluontoista tietoja. Esimerkiksi henkilö- ja rahaliikennetiedot voivat olla uhattuina mobiilimaksujärjestelmään kohdistuvan tietomurron aikana. Tutkimuksessa esitellään mistä turvallisuus muodostuu mobiilimaksamisessa ja millaisia uhkia siihen liittyy. Lopuksi selvitetään, mitkä ovat olennaisimpia torjuntatapoja mobiilimaksamisen uhkia vastaan.

Asiasanat: mobiilimaksaminen, mobiilipalvelut, turvallisuus, turvallisuusuhat, tietoturva

ABSTRACT

Tamminen, Jimi
Security threats and their prevention in mobile payment
Jyväskylä: University of Jyväskylä, 2018, 33 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Luoma, Eetu

The Bachelor's Thesis is a literature review, which discusses mobile payment, security threats relating to it, and prevention methods against these threats. The thesis presents the most important features and functions of mobile payment. On top of these, the thesis highlights the technologies that make mobile payment possible. The popularity of mobile payment is projected rise significantly in the following years and security is one of the most important aspects regarding customer acceptance. Security is key attribute for mobile payment systems due to the sensitive information that they process. For example, personal and financial information may be compromised in case of a data breach on a mobile payment system. The thesis explains what the building blocks for security of mobile payment are and what types of threats related to it. Finally, the thesis will describe the essential methods to prevent these threats.

Keywords: mobile payment, mobile services, security, threat, data security

KUVIOT

SISÄLLYS

1 JOHDANTO

Matkapuhelin on mullistava keksintö, joka ravistelee vakiintuneita toimialoja ja liiketoimintamalleja. Musiikkisoittimet, navigaattorit ja kamerat ovat jo laajalti kadonneet käytöstä erillisinä laitteina ja sulautuneet osaksi matkapuhelinta. Matkapuhelimen voittokulku näyttää jatkuvan edelleen ja seuraavana valloituksena kohteena on maksamisen. (Kazan & Damsgaard, 2014) Langattoman teknologian vallankumous on mahdollistanut mobiililaitteiden kehittymisen keskeiseksi osaksi uutta, digitaalista taloutta. Mobiililiiketoiminta, jolla tarkoitetaan sähköistä kaupankäyntiä mobiililaitteita ja langattomia verkkoja hyödyntäen, on luonnollista jatkumoa elektroniselle liiketoiminnalle ja edustaa uutta tapaa käydä kauppaa. Mobiililaitteiden hyödyntämistä maksutapahtumassa kutsutaan mobiilimaksamiseksi. (Isaac & Sherali, 2014).

Perinteisiin maksutapoihin verrattuna mobiilimaksamisen etuna on sen ubiikkius, joka tarkoittaa sitä, että käyttäjät voivat suorittaa maksuja missä ja milloin tahansa. (Zhou, 2013) Mobiilimaksaminen onkin kasvattanut suosiotaan valtavalla nopeudella varsinkin Aasiassa ja Afrikassa. Etenkin Kiinassa suosittu pikaviestisovellus WeChat avasi mobiilimaksupalvelunsa elokuussa 2013, mikä oli merkittävä osatekijä maan mobiilimaksujen kokonaisarvon kasvaessa peräti 391 prosenttia seuraavan vuoden aikana. (Wu, Liu & Huang, 2016)

Ensimmäiset mobiilimaksupalvelut lanseerattiin jo 90-luvulla, joten kyseessä ei ole täysin uusi konsepti. Se ei kuitenkaan ole onnistunut sementoimaan paikkaansa arkipäiväisessä käytössä, lukemattomista yrityksistä huolimatta. Nyt on kuitenkin havaittavissa taas uutta nostetta, ennen kaikkea älylaitteiden kehittymisen ja laajemman leviämisen sekä tarvittavan teknologian parantumisen myötä.

Mobiilimaksamisen tutkimus on keskittynyt aiempina vuosina jopa turhankin voimakkaasti käyttöönottoon vaikuttaviin tekijöihin. Näissä tutkimuksissa turvallisuus on noussut lähes poikkeuksetta tärkeimpien käyttöönottoon vaikuttavien tekijöiden joukkoon helppokäyttöisyyden ja koetun hyödyn ohella. Mobiilimaksamisen turvallisuutta on tutkittu jonkin verran, mutta näkökulma on ollut lähes poikkeuksetta teknisen turvallisuusratkaisun esittely. (Dahlberg, Guo & Ondrus, 2015) Tämä tutkielma pyrkii paikkaamaan aukkoa mobiilimak-

samisen turvallisuuden tutkimuksessa tarjoamalla kokonaiskuvan mobiilimaksamiseen ja sen turvallisuuteen liittyviin asioihin perehtymällä alan tutkimuksiin.

Tässä tutkielmassa aihetta lähestytään seuraavan tutkimuskysymyksen kautta:

- Mitä ovat mobiilimaksamisen turvallisuusuhat ja kuinka niitä voidaan torjua?

Tutkimuksen tavoitteena on selvittää mitkä ovat keskeisimpiä turvallisuusuhkia mobiilimaksamisen kannalta ja mitkä ovat tärkeimpiä tapoja näihin uhkiin vastaamisessa. Tämän lisäksi tavoitteena on esitellä, mitä mobiilimaksaminen oikeastaan on, millaisia eri ominaisuuksia tai tekijöitä siihen liittyy ja kuinka se toimii käytännössä.

Tutkimus on toteutettu kirjallisuuskatsauksena, joten se tarjoaa selkeän katsauksen alan tieteellisiin artikkeleihin ja kirjallisuuteen. Lähteiden etsinnässä tärkeimpinä tietokantoina ovat toimineet Scopus ja Google Scholar yhdessä - Jyväskylän yliopiston JYKDOK -tietokannan kanssa. Keskeisimpiä hakutermejä ovat olleet ”mobile payment” ja ”m-payment” yhdistettynä termeihin ”security”, ”threat” ja ”risk”. Hakulauseissa on myös käytetty erilaisia kombinaatioita edellä mainituista termeistä. Tärkeimmät kriteerit lähteiden valinnassa ovat olleet tekstin sisällön ohella lähteiden luotettavuus. Luotettavuutta on arvioitu viittausten määrän, julkaisukanavan ja kirjoittajien muiden töiden perusteella. Lisäksi lähteiden sisältöä on arvioitu niiden julkaisuvuoden perusteella ajantasaisen tiedon varmistamiseksi.

Tutkimusta on työstetty siten, että aiheen valinnan jälkeen on etsitty keskeisimmät lähteet ja tutustuttu niiden sisältöön. Tämän jälkeen on hahmoteltu tutkielman rakenne sisältölukujen otsikoiden ja alaotsikoiden avulla ja etsitty lisää lähteitä kustakin aiheesta. Sisältölukujen valmistuttua on kirjoitettu johdanto- ja yhteenvetoluvut. Lopuksi tutkielma on tarkastettu mahdollisimman hyvän yhtenäisyyden ja selkeyden varmistamiseksi.

Rakenteensa puolesta tutkimus etenee seuraavasti: luvussa kaksi vastataan kysymykseen mitä mobiilimaksaminen on. Tämä tapahtuu käymällä läpi mobiilimaksamisen määritelmä, tunnuspiirteet ja erilaiset luokittelutavat. Lisäksi toisessa luvussa esitellään mobiilimaksuprosessi ja siihen liittyvät toimijat sekä esitellään mobiilimaksamisen mahdollistavia verkkoliikenneteknologioita. Kolmannessa luvussa kerrotaan, mitä turvallisuus on mobiilimaksamisen kontekstissa ja käydään läpi olennaisimpia turvallisuusuhkia. Aihealueen rajaamiseksi viestintäteknologioiden turvallisuusongelmia ei tarkastella tässä tutkielmassa, vaikka ne liittyvätkin myös mobiilimaksamisen turvallisuuteen. Tämän jälkeen neljäs luku käsittelee tärkeimpiä ratkaisuja edellä esiteltyjen uhkien torjuntaan. Lopussa tiivistetään tutkimuksen tulokset kirjoittajan omien ajatusten kera ja pohditaan alan tutkimuksen tulevaisuuden suuntaa.

2 MOBIILIMAKSAMINEN

Tässä luvussa käsitellään mobiilimaksamista, mitä sillä tarkoitetaan ja miten se on kehittynyt vuosien aikana. Luvussa esitellään myös mobiilimaksutransaktion vaiheet ja keskeiset roolit. Lisäksi luvussa käsitellään mobiilimaksupalveluiden vaatimuksia ja niissä käytettyjä teknologioita.

2.1 Mobiilimaksupalvelut

Tuhansia vuosia sitten ennen ajanlaskumme alkua ihmiskunta kehitti ensimmäisen rahan vaihdon välineeksi tavoitteenaan tehostaa kaupankäyntiä. Raha toimii paitsi vaihdon välineenä myös arvon säilyttäjänä ja mittayksikkönä. Vuosituhansien saatossa raha on käynyt läpi monia ja merkittävä mullistuksia. Ensimmäisinä rahoina käytettiin esimerkiksi valaanhampaita ja simpukankuoria, jotka korvattiin myöhemmin jalometalleilla ja lopulta paperisilla seteleillä. Nyt lähestytään kuitenkin aikaa, jolloin raha käy läpi kenties suurimman muutoksen tähän mennessä: se muuttuu täysin elektroniseksi. (Lerner, 2013)

Samaan aikaan rahan muuttumisen kanssa mobiiliverkkoteknologiat ovat kehittyneet ja levinneet huimaavaa vauhtia syrjäisillekin alueille. Kansainvälisen televiestintäliiton arvion mukaan jopa 84 prosenttia maailman ihmisistä asuu 3G- tai 4G-verkon peittoalueella, tosin siitä huolimatta vain 47 prosenttia ihmiskunnasta käyttää internettiä. (Sanou, 2016) Langattomien teknologioiden kehitys on mahdollistanut tilanteen, jossa käyttäjät voivat suorittaa maksuja myös liikkeessä ollessaan (Isaac & Sherali, 2014).

Nykyään puhutaan usein mobiililiiketoiminnasta, joka on täydentävä osa laajempaa elektronista kaupankäyntiä. Mobiilikaupankäynti voidaan määritellä olevan elektronisen liiketoiminnan muoto, joka keskittyy erityisesti mobiililaitteiden käyttöön. Mobiililiiketoiminnan keskeisiin muotoihin kuuluu mobiilimaksaminen ja mobiilipankkitoiminta. Näiden kahden selkeä erottelu toisistaan on haastavaa, sillä ne sisältävä osittain päällekkäisiä toimintoja ja voivat olla osa samaa kokonaisuutta. (Jovanovic & Muñoz-Organero, 2011)

Mobiilimaksamiselle ei ole luotu yhtä, täysin vakiintunutta määritelmää vaan on olemassa useita hieman toisistaan poikkeavia määritelmiä. Yleisesti ottaen mobiilimaksut ovat mobiililaitteella (esimerkiksi matka- tai älypuhelimella) tehtäviä maksuja hyödykkeestä, palvelusta tai laskusta hyväksikäyttäen langattomia tai muita kommunikaatioteknologioita (Dahlberg, Mallat, Ondrus & Zmijewska, 2008). Mobiilimaksu voidaan myös määritellä maksuksi, jossa mobiililaitetta käytetään kaupallisen transaktion käynnistämiseen, valtuuttamiseen tai vahvistamiseen. (Au & Kauffman, 2008). Ondrusin ja Pigneurin (2007) mukaan suurimassa osassa määritelmissä keskeistä on juurikin mobiililaitteen käyttö maksutapahtumassa, mikä erottaa mobiilimaksun muun tyyppisistä maksutapahtumista. He myös huomioivat, että osassa määritelmistä mobiilimaksuun ei lasketa itse maksun toteutumista, kun taas joissakin määritelmissä se sisällytetään osaksi prosessia. Ondrus ja Pigneur itse määrittelevät mobiilimaksun laaja-alaisesti, sillä heidän määritelmässään mobiilimaksuiksi lasketaan kaikki maksut hyödykkeistä, palveluista tai laskuista, joiden valtuuttamiseen, aloittamiseen tai vahvistamiseen käytetään mobiililaitetta. On myös syytä huomioida, että mobiilimaksu ei rajoitu ainoastaan matka- tai älypuhelimella suoritettaviin maksuihin, vaan ne ovat mahdollisia käytännössä millä tahansa langattomia verkkoteknologioita käyttävällä mobiililaitteella (Karnouskos & Fokus, 2004). Tässä tutkielmassa seurataan Ondrusin ja Pigneurin määritelmää mobiilimaksusta.

Yleisen käytännön mukaan mobiilimaksut voidaan jakaa kahteen eri tyyppiin niiden toimintatavan perusteella: etämaksuihin ja lähimaksuihin. Etämaksussa käyttäjä ottaa yhteyden mobiilimaksupalvelun back end-järjestelmään mobiililaitetta käyttäen ja mobiiliverkkojen avulla, kun taas lähimaksussa käyttäjä suorittaa maksun käyttäen mobiililaitetta ja lyhyen kantaman kommunikaatioteknologioita (Agarwal, Khapra, Menezes & Uchat, 2007; Isaac & Sherali, 2014). Etämaksujärjestelmien käyttäminen vaatii asiakkaalta rekisteröitymistä palveluun, mikä sisältää usein sovelluksen asentamisen mobiililaitteeseen. Tämän jälkeen asiakas voi käyttää sovellusta mobiililaitteella maksun suorittamiseen. Asiakkaalla voi olla tilillään valmiiksi ladattuna rahaa, ”pre-paid”-tyyppisesti, tai palvelu voi ottaa maksun suoraan siihen yhdistelty pankkitililtä (Taylor, 2016).

Mobiilimaksuja jaotellaan myös usein maksetun summan suuruuden mukaan. Tyypillisesti maksut jaetaan kahteen luokkaan, mikro- ja makromaksuihin, jossa mikromaksuja ovat kaikki alle 10 dollarin suuruiset maksut. Sitä suuremmat maksut puolestaan kuuluvat makromaksuihin. (Zmijewska, Lawrence & Steele, 2004) Tarkka raja-arvo mikro- ja makromaksun välillä vaihtelee hieman lähteen mukaan ja esimerkiksi Isaac ja Sherali (2014) esittävät vielä kolmannen luokan, pikomaksun, alle 0.10 dollarin maksuille.

On myös syytä huomata, että mobiilimaksu voi olla niin sanottu P2P-maksu (peer-to-peer) tai C2B-maksu (consumer-to-business). P2P-maksu on yksityinen maksu kahden palvelun käyttäjän välillä ja ne ovat tyypillisesti etämaksuja. Kaupallinen maksualusta saattaa olla mukana transaktiossa, mutta transaktio itsessään on suoraan kahden henkilön välinen. P2P-maksut ovat suosittuja varsinkin kehitysmaissa ja niillä arvioidaan olevan valtava kasvupotentiaali. Esimerkiksi Kiinassa toimivan WeChatin kautta lähetettiin yli 40 miljoona

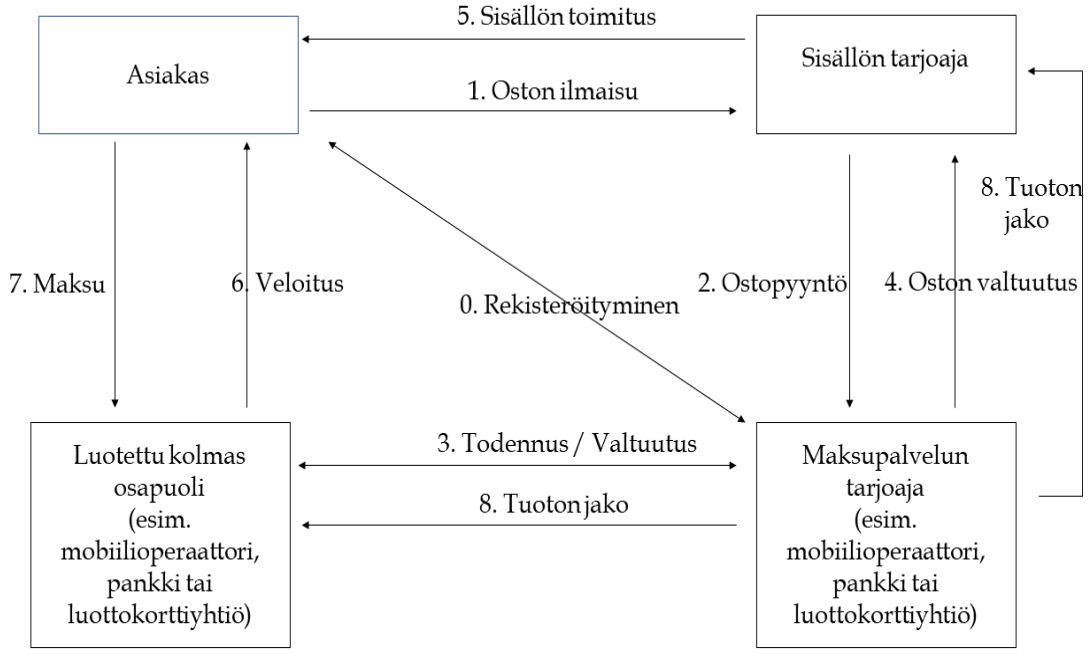
rahalähetystä, niin sanottuja punaisia kirjekuoria, pelkästään vuoden 2015 kiinalaisen uudenvuoden aikana. C2B-maksu puolestaan on ostotapahtuma, jossa asiakas maksaa jollekin yritykselle tuotteesta tai palvelusta. (Wang, Hahn & Sutrave, 2016)

Gaon, Cain, Patelin ja Shimin (2005) mukaan Telecom Media Network (2002) on määritellyt mobiilimaksuprosessiin neljä eri avainroolia. Nämä neljä roolia ovat sisällön tarjoaja, todentamisen tarjoaja, maksun valtuutuksen ja selvityksen tarjoaja sekä asiakas. Maksuprosessi koostuu kolmesta vaiheesta, jotka ovat rekisteröitymisvaihe, transaktiovaihe ja maksun selvitys- ja toimitusvaihe. Kuvio 1 esittää näihin vaiheisiin sisältyvät askeleet, jossa sisällön tarjoajana (eng. *Content Provider*) on tyypillisesti jonkin tuotteen myyjä, todentamisen tarjoajana toimii maksupalvelun tarjoaja (eng. *Payment Service Provider*) ja maksun valtuutuksesta ja selvityksestä vastaa luotettu kolmas osapuoli (eng. *Trusted Third Party*). Asiakas voi olla kuka tahansa palvelun käyttäjä.

Rekisteröitymisvaiheessa asiakkaan tulee tyypillisesti avata tili maksupalvelun tarjoajan kautta. Tämän vaiheen aikana maksupalvelun tarjoaja tarvitsee vahvistuksen luotetulta kolmannelta osapuolelta, joka on päävastuussa suhteesta asiakkaaseen. Luotettu kolmas osapuoli voi olla palvelusta riippuen esimerkiksi pankki tai mobiilioperaattori.

Transaktiovaiheessa asiakas ilmaisee halukkuuteensa ostaa sisältöä sisällön tarjoajalle, joka puolestaan välittää tiedon maksupalvelun tarjoajalle. Maksupalvelun tarjoaja pyytää tämän jälkeen maksun todennusta ja valtuutusta luotetulta kolmannelta osapuolelta. Saatuaan hyväksyvän vastauksen todennus- ja valtuutuspyyntöönsä, maksupalvelun tarjoaja ilmoittaa asiasta sisällön tarjoajalle, joka toimittaa halutun sisällön asiakkaalle.

Jos luotettu kolmas osapuoli on pankki, maksun selvitys- ja toimitusvaiheessa asiakasta voidaan veloittaa suoraan pankkitililtä reaaliaikaisesti. Muussa tapauksessa maksupalveluntarjoaja ensin lähettää laskun asiakkaalle luotetun kolmannen osapuolen kautta, joka palauttaa asiakkaalta saadun summan takaisin maksupalvelun tarjoajalle. Tämän jälkeen maksupalvelun tarjoaja jakaa tuoton sopimusten mukaan eri osapuolten kesken.



KUVIO 1 Mobiilimaksutransaktion vaiheet (mukaillen Gao, Cai, Patel & Shim, 2005)

Mobiilimaksaminen ei itsessään ole aivan uusi ilmiö, sillä ensimmäiset palvelut tulivat markkinoille jo 90-luvulla. Yhtenä ensimmäisistä mobiilimaksuratkaisuista pidetään suomalaisen puhelinoperaattori Soneran vuonna 1997 lanseeraamaa palvelua, jonka avulla myyntiautomaateista pystyi ostamaan tuotteita matkapuhelimella. (Dahlberg, Mallat & Öörni, 2003)

Analyytikot ja tutkijat ovat julistaneet jo 2000-luvun alkupuolelta lähtien mobiilimaksamisen olevan seuraava läpimurto mobiililiiketoiminnan alalla. Siitä huolimatta mobiilimaksupalveluilla on ollut suuria vaikeuksia vakiinnuttaa jalansija varsinkin kehittyneiden maiden markkinoilla. Menestyneet palvelut keskittyvät usein johonkin yksittäiseen käyttötapaukseen, esimerkiksi julkisen liikenteen lippujen välittämiseen. Kehitysmaissa mobiilimaksut ovat sen sijaan saavuttaneet suosiota, ennen kaikkia muiden maksuvälineiden huonon saatavuuden myötä. Mobiilimaksamisen lopullisen läpilyönnin suurimpana esteenä ovat olleet teknologiaan liittyvät haasteet, kuten sopivien laitteiden puuttuminen kuluttajilta, sekä palveluiden heikko käytettävyys verrattuna jo käytössä oleviin maksutapoihin (Gannamaneni, Ondrus & Lyytinen, 2015). Nokian mobiilimaksamisen johtaja Lauri Pesonen kuvasikin mobiilimaksamisen haasteita osuvasti, ja osittain edelleen paikkaansa pitävästi, jo vuonna 2005:

> Mobiilimaksut ovat olleet suuri lupaus, joka ei ole toistaiseksi materialisoitunut. Sen ympärillä on ollut paljon hypetystä. Mobiilimaksun edistäjien on löydettävä tapoja vakuuttaa kuluttajat kurottamaan puhelimiaan kohti maksukorttien sijaan – ja vakuuttaa jälleenmyyjät, että uusien maksutapojen hyväksyminen on laiteinvestointien arvoista. Keskeisin kysymys on: Mikä on liiketoimintamalli kauppiaille; mikä on kannustin kuluttajalle käyttää matkapuhelinta maksaessaan? (Jette, 2005)

Karnouskousin ja Fokusin (2004) mukaan mobiilimaksupalvelun tulisi täyttää tiettyjä yleisiä vaatimuksia saavuttaakseen laajemman käyttöönoton markkinoilla. Näihin vaatimuksiin kuuluvat:

1. Yksinkertaisuus ja käytettävyys: Palvelun yksinkertaisuus ja käytettävyys määrittävät hyvin pitkälti saavuttaako palvelu käyttäjiä. Tämä sisältää esimerkiksi matalan oppimiskynnyksen, käyttäjäystävällisen käyttöliittymän ja palvelun muokattavuuden käyttäjän omiin, päivittäisiin tarpeisiin sopivaksi.
2. Yleismaailmallisuus: Palvelun tulee tarjota mahdollisuus moneen eri tyyppiseen maksuun vastatakseen käyttäjien tarpeisiin. Transaktioiden tulee olla mahdollisia paitsi asiakkaalta yritykselle myös kahden käyttäjän välillä. Lisäksi on oltava mahdollisuus sekä pieniin mikromaksuihin että suurempiin makromaksuihin.
3. Yhteensopivuus: Mobiilimaksupalvelun kehityksessä tulisi ottaa huomioon yhteensopivuus finanssialan standardeihin ja avoimen teknologian hyödyntäminen maailmanlaajuisella tasolla. Palvelun tulisikin toimia esimerkiksi mahdollisimman monella mobiililaitteella ja hyödyntää standardien mukaisia ratkaisuja.
4. Turvallisuus, luottamus ja yksityisyys: Ensinnäkin käyttäjän tulee voida luottaa siihen, että palveluntarjoaja ei väärinkäytä hänen pankki- tai henkilötietojaan. Toiseksi käyttäjän yksityisyyden on pysyttävä suojattuna ja suoritetut transaktiot eivät saa vuotaa palvelun ulkopuolelle. Mobiilimaksamisen tulee olla yhtä anonyymia kuin käteisen rahan käyttö. Kolmanneksi palvelu tulee suunnitella kestämään ulkopuolisia hyökkäyksiä kuten hakkerointeja. Tässä voidaan hyödyntää erilaisia turvallisuusominaisuuksia, kuten julkiseen avaimeen perustuvaa salausta, biometrisiä tunnisteita ja salasanatekniikoita.
5. Rajat ylittävä maksaminen: Maksutapahtuman suorittaminen tulee olla yhtä helppoa sekä paikallisella että kansainvälisellä tasolla. Palvelun tulee toimia käyttäjän sijainnista ja valuutasta riippumatta.
6. Kustannukset: Mobiilimaksupalvelun käyttö ei saa olla kalliimpaa kuin muiden tarjolla olevien maksutapojen käyttäminen. Lisäksi palveluiden tulisi luoda uusia tulovirtoja tai toimia paremmin olemassa olevien prosessien kanssa oikeuttaakseen olemassa olonsa.
7. Nopeus: Palvelun kautta tehtävien transaktioiden tulee tapahtua nopeasti ilman kompromisseja turvallisuuden suhteen.
8. Paikallisen markkinan ymmärtäminen: Käyttäjät ovat tottuneet käyttämään tiettyjä maksuvälineitä ja tarvitsevat erityisen syyn vaihtaakseen maksutavakseen mobiilimaksamisen. Tästä syystä palvelun on tarjottava käyttäjälle jotain lisähyötyä verrattuna jo käytössä oleviin maksutapoihin. Nämä hyödyt vaihtelevat eri markkinoiden välillä ja kunkin markkinan uniikkien tilanteiden ymmärtäminen on keskeistä palvelun menestymiselle.

9. Integraatio perinteisiin toimintatapoihin: Olemassa olevan infrastruktuurin ja laskutusjärjestelmien käyttö tulisi olla mahdollista, etenkin pankkijärjestelmien kaltaisten vaikeasti muutettavissa olevien toimintatapojen kohdalla. Palvelun tulee mahdollistaa integraatio pankki- ja luottopalveluita tarjoaviin organisaatioihin ja niiden infrastruktuuriin.

2.2 Mobiilimaksupalvelumallit

Mobiilimaksupalveluita voidaan luokitella myös palvelun taustalla olevan organisaation tai organisaatioiden perusteella. Lerner (2013) jakaa palvelut neljään eri malliin tämän perusteella, joista jokaisella on omat hyvät ja huonot puolensa. Nämä mallit ovat pankkivetoinen malli, mobiiliverkko-operaattorivetoinen malliin, yhteistyömalli sekä itsenäinen malli.

Pankkivetoisen mallin etuina voidaan pitää pankkien kokemusta maksujen käsittelystä ja välittämisestä. Lisäksi pankit pystyvät tarjoamaan jo olemassa olevia lisäpalveluita raha-asioissa – esimerkiksi pankkikorttien myöntäminen ja kansainvälisten maksujen välitys - ja niitä pidetään yleisesti ottaen luotettavina toimijoina. Tämän mallin etuna on myös pankkien jo valmiiksi laaja käyttäjäkunta ja olemassa olevat suhteet loppuasiakkaisiin, jotka helpottavat palvelun lanseeraamista. Toisaalta mahdollinen ongelma voi syntyä pankkien kokemattomuudesta mobiilisovellusten kehittämisessä. Lisäksi pankit saattavat olla haluttomia sijoittamaan uuden palvelun luomiseen pelätessään sen uhkaavan jo tarjolla olevien palveluiden synnyttämiä tulovirtoja.

Mobiiliverkko-operaattorivetoisen mallin parhaimpiin puoliin kuuluu operaattoreiden kokemus matkaviestinverkkojen toiminnasta, valmis suhde mobiililaitteiden käyttäjiin sekä tietämys asiakkaiden mobiililaitteiden käytöstä. Mobiilimaksujen summa voidaankin usein lisätä suoraan asiakkaan puhelinlaskuun (Karnouskos & Fokus, 2004). Operaattorit voivat myös todennäköisesti hyötyä läheisistä yhteistyösuhteistaan mobiililaiteiden valmistajien kanssa, toisin kuin esimerkiksi pankit. Mallin heikkouksiin taas kuuluu olemassa olevan maksupalveluekosysteemin puute ja ylipäätään kokemattomuus maksunvälittäjänä toimimisesta.

Yhteistyömalli perustuu pankkien ja mobiiliverkko-operaattorien yhteistyöhön, jossa kumpikin osapuoli tarjoaa parhaat puolet omasta osaamisestaan. Yhteistyömalli eliminoi suurilta osin kahden edeltävänä mallin heikkoudet ja riskin jakaminen on houkuttelevaa useille yrityksille. Toisaalta osapuolten väliset neuvottelut voivat osoittautua monimutkaisiksi ja yhteistyön tekeminen tarkoittaa kokonaispotin jakamista toisen organisaation kanssa, mikä ei välttämättä houkuttele suuria pankkeja tai mobiiliverkko-operaattoreita. Gannamanenin, Ondrusin ja Lyytisen (2015) mukaan mobiilioperaattorien ja finanssilaitosten

välinen yhteistyö onkin yksi suurimmista haasteista mobiilimaksupalvelun menestyksen kannalta.

Itsenäisessä mallissa jokin erillinen ja yksityinen toimija, joka ei ole pankki tai mobiiliverkko-operaattori, aloittaa mobiilimaksupalvelun tarjoamisen. Tämän mallin merkittävimpiä etuja on selkeästi rahansiirtoon keskittynyt liiketoimintamalli, uudet lisäarvoa tuottavat palvelut sekä mahdollisuus ristiin myyntiin. Yksi selkeimpiä heikkouksia on valmiina olemassa olevan käyttäjäkunnan puuttuminen, mikä luo haasteita luottamuksen synnyttämisessä. Lisäksi koko liiketoiminta on luotava käytännössä katsoen tyhjästä, mikä puolestaan on kallista ja riskialtista.

2.3 Mobiilimaksamiseen käytetyt viestintäteknologiat

Mobiilimaksupalvelut voivat hyödyntää useita eri teknologioita maksun välittämiseen ja monet palveluista hyödyntävätkin useampaa kuin yhtä teknologiaa (Lerner, 2013). Eri teknologioilla on omat erityisominaisuutensa, joita esitellään seuraavaksi mobiilimaksamisessa yleisesti käytettyjen teknologioiden osalta.

2.3.1 3G- ja 4G-teknologiat

Langattomat mobiiliverkot ovat käyneet läpi neljän tai viiden sukupolven (eng. *generation, G*) verran kehitystä niin sanotuista 0G-teknologioista tällä hetkellä käytössä oleviin 4G-teknologioihin. 0G-termillä viitataan matkapuhelimia edeltäviin puhelinteknologioihin, kuten radiopuhelimiin. Näihin kuuluvat esimerkiksi Suomessa 70-luvulla käyttöön tullut Autoradiopuhelin (ARP).

Epävirallisesti 2.5G-teknologiaksi kutsuttu General Packet Radio Service-teknologia (GPRS) mahdollisti datan siirtämisen suurimmillaan 115 kilobittiä sekunnissa (kb/s). GPRS-teknologiaa on käytetty mobiilimaksamisessakin Wireless Access Protocol-palvelun (WAP) kautta ja se mahdollistaa esimerkiksi internetin selaamisen.

3G-teknologiat toivat tarjolle laajemman valikoiman kehittyneempiä palveluita, saavuttaen samalla suuremman tiedonsiirtonopeuden ja paremman spektrisen tehokkuuden. Mahdollinen tiedonsiirtonopeus 3G-teknologioissa on 14.4. megabittiä sekunnissa (Mb/s) vastaanottajana ja 5.8 Mb/s lähettäjänä. Muun muassa Enhanced Data rates for GSM Evolution (EDGE) ja Universal Mobile Telecommunications System (UMTS) kuuluvat kolmannen sukupolven teknologioihin. (Bhalla & Bhalla, 2010)

Kansainvälinen televiestintäliitto ITU julkaisi vuonna 2008 julkaisi vuonna 2008 määritelmän 4G:lle, jonka mukaan 4G-palvelun on saavutettava 100 Mb/s tiedonsiirtonopeus liikuttaessa nopeasti esimerkiksi autolla. Hitaassa liikkeessä nopeuden on saavutettava 1 gigabitti sekunnissa (Gb/s). (ITU-R, 2008) 4G:stä

puhuttaessa viitataan useimmiten Long Term Evolution (LTE)-teknologiaan ja sen kehittyneempään seuraajaan LTE-Advancediin (LTE-A). LTE on saavuttanut maailmanlaajuisen hyväksynnän, mikä on poikkeuksellista verrattuna aiempiin sukupolviin, joissa oli käytössä useampia, keskenään kilpailevia teknologioita. Tarkkaan ottaen LTE ei täyttänyt kaikkia ITU:n alkuperäisiä teknisiä vaatimuksia 4G-teknologoille, mutta puolestaan LTE-A täyttää ne. (Dahlman, Parkvall & Skold, 2016; Parkvall ym., 2008)

2.3.2 NFC

Near Field Communication (NFC) on Radio Frequency Identification (RFID) -tekniikkaa käyttävä teknologia kahden laitteen väliseen kommunikaatioon. Se perustuu sähkömagneettiseen induktioon ja toimii radiotaajuudella 13,56 MHz. NFC-teknologian tarkoituksena on tehdä digitaalisista transaktioista ja materiaalin siirroista helpompia ja käytännöllisempiä. Teknologian kehitystyön takana ovat NXP Semiconductors, aikaisemmalta nimeltään Philips Semiconductors, ja Sony Corporation. Kyseistä teknologiaa käyttävien laitteiden on oltava lähellä toisiaan, mutta niiden ei tarvitse koskettaa, sillä pisin kantama on noin 10 senttimetriä. Suurin mahdollinen tiedonsiirtonopeus on 848 Kbit/s.

Vuonna 2010 Google julkaisi Android-käyttöjärjestelmästä version 2.3, joka ominaisuksiin kuului ensimmäistä kertaa tuki NFC-teknologian käytölle. NFC edellyttää, että toinen laitteista toimii transaktion käynnistävänä osapuolena (eng. *initiator*), joka on tuottaa RF-signaalin ja hallinnoi datan siirtoa. Toinen laite puolestaan toimii passiivisena vastaanottajana (eng. *target*), joka vastaa toisen osapuolen pyyntöön. Mobiilimaksutapahtumassa maksulaite on tyypillisesti käynnistävä osapuoli ja älypuhelin on passiivinen vastaanottaja. (Curran, Millar & Mc Garvey, 2012)

NFC-teknologian etuja verrattuna käteiseen rahaan tai sirulliseen pankkikorttiin maksun välittämisessä ovat nopeus ja luotettavuus. Pankkikortin siru voi vahingoittua tai kulua käytön myötä, mikä ei ole ongelma NFC-teknologian kaltaisessa kontaktittomassa teknologiassa. Maksutapahtuma on kuitenkin muutoin hyvin saman tapainen kuin korttimaksussa ja NFC-teknologiaa voidaankin teknisestä näkökulmasta tarkasteltuna pitää eräänlaisena älykortin ja matkapuhelimen fuusiona (Ondrus & Pigneur, 2009).

2.3.3 SMS ja USSD

Short Message Service (SMS) on Global System for Mobile Communications (GSM) -verkkoa varten kehitetty viestintätekniikka, joka syntyi yhteiseurooppalaisen yhteistyön pohjalta. (Harris, Hillebrand, Holley & Trosby, 2010) GSM-verkko kuuluu 2G-teknologioihin. Sen kehitystyö aloitettiin jo 80-luvun puolivälissä ja 90-luvun aikana teknologia tuli laajasti käyttöön. Yhden viestin suurin

hyötykuorma on 140 tavua, jonka seurauksena viestin suurin mahdollinen mitta on 160 aakkosnumeerista merkkiä. Tätä pidempien viestien lähettäminen on myös mahdollista, jolloin viestin välitysjärjestelmä pilkkoo viestin pienempiin osiin ja liittää niihin tunnisteen joka käyttää osan maksihyötykuormasta. Yleisin käyttö SMS-teknologialle on kahden käyttäjän välinen keskustelu, mutta teknologiaa voidaan hyödyntää myös useissa muissa sovelluksissa. (Harris ym., 2010)

Unstructured Supplementary Service Data (USSD) on myös tekniikka tiedon välittämiseen GSM-verkon välityksellä. Keskeisimpiä eroja USSD- ja SMS-tekniikoiden välillä on se, että USSD avaa reaaliaikaisen yhteyden, USSD-session, tietojen vaihdon ajaksi, toisin kuin asynkroninen SMS. Voidaankin sanoa, että SMS on niin kutsuttu etappivälitystekniikka, kun taas USSD on orientoitunut enemmän transaktioihin. (Carr, 2007; Kadhiwal & Zulfiquar, 2007)

GSM-verkossa toimivaa laitetta käyttäessä asiakkaan tunnistamiseen maksutapahtuman yhteydessä voidaan käyttää Subscriber Identity Module (SIM)-korttia

2.3.4 Bluetooth

Bluetooth on lyhyen kantaman kommunikaatiostandardi, joka perustuu radiotekniikkaan. Standardin takana on ruotsalainen Ericsson, jonka alkuperäisenä tavoitteena oli kehittää korvaaja kaapeleille. Se on halpa, pieni energiankulutukseltaan ja yksinkertainen. Bluetooth toimii taajuudella 2.4GHz ja se suurin kantama voi olla jopa 100 metriä, joskin se vaatii vahvistimien käyttöä. Tyypillisissä olosuhteissa kantama on noin 10 metriä. Teknologia tukee niin datan kuin äänen siirtoa ja sen täysi spesifikaatio on täysin avoin ja ilmainen. Bluetoothin tiedonsiirtonopeus on 1 Mbit/s. (McDermott-Wells, 2004)

3 TURVALLISUUSUHAT

Tässä luvussa kerrotaan, mitä turvallisuudella tarkoitetaan mobiilimaksamisen kontekstissa. Tämän ohella luvussa käsitellään mobiilimaksamisen keskeisimpiä turvallisuusuhkia. Kaikkia turvallisuusuhkia ei kuitenkaan käsitellä tarkemmin tässä tutkimuksessa aiheen rajaamiseksi. Keskeisin tarkemman tarkastelun ulkopuolelle jätetty uhkakokonaisuus on eri verkkoteknologioiden turvallisuus mobiilimaksujen siirrossa.

Mobiilimaksamiseen kohdistuviin uhkiin kuuluvat myös esimerkiksi mobiililaitteen kadottaminen tai varkauden kohteeksi joutuminen sekä laitteen toimintahäiriöstä johtuvat riskit. (Me, 2003) Mobiililaitteiden suojaaminen on muutoinkin avainasemassa mobiilimaksamisen turvallisuudesta puhuttaessa.

3.1 Mobiilimaksamisen turvallisuus

Turvallisuus on mobiililiiketoiminnassa tärkeä tekijä. Mobiilimaksujärjestelmät välittävät arkaluontoista dataa, joten sekä teknisen että käyttäjän kokeman turvallisuuden on oltava korkealla tasolla. (Isaac & Sherali, 2014) Arkaluontoinen data voi tarkoittaa tässä yhteydessä esimerkiksi asiakkaan maksukortin tietoja, kuten nimeä, luottokortin numeroa ja maksua varten olevaa palvelukoodia. Järjestelmään kohdistuvan tietomurron sattuessa käyttäjät ovatkin altistuneita identiteettivarkauksille ja petoksille. (Wang ym., 2016)

Uhka määritellään tilanteeksi, josta voi koitua vahinkoa. Uhka voi olla luonnollinen, tahaton tai tahallinen. Haavoittuvuus puolestaan on ominaisuus tai heikkous, joka nostaa alttiutta uhalle. Osapuolta, joka on vastuussa tahallisen uhan synnyttämisestä, kutsutaan hyökkääjäksi. (Clarke, 2008)

Monet mobiilimaksamiseen liittyvät turvallisuusuhat ovat seurausta siitä, että maksamiseen käytettävää mobiililaitetta käytetään useaan eri tarkoitukseen ja ne sisältävät useita eri sovelluksia. Mobiililaitteen turvallisuus- ja ohjelmistopäivitysten asentamiset ovat tyypillisesti käyttäjän omalla vastuulla, mikä voi entisestään heikentää laitteen turvallisuutta. (Wang, Streff & Raman, 2012)

Mobiilimaksamisen turvallisuudesta voidaan erottaa kaksi eri ulottuvuutta, objektiivinen ja subjektiivinen turvallisuus. (Linck, Pousttchi & Wiedemann, 2006). Linckin, Pousttchin ja Wiedemannin (2006) mukaan Merz (2002) on esittänyt, että objektiivinen turvallisuus on teknologinen ominaisuus, jonka omaava teknologinen ratkaisu täyttää kaikki viisi siihen liittyvää tavoitetta. Nämä tavoitteet ovat:

- Luottamuksellisuus. Järjestelmän sisältämä luottamuksellinen tieto täytyy olla luvattomien henkilöiden, prosessien ja laitteiden tavoittamattomissa. Luottamuksellisuuden varmistamisessa avainasemassa ovat salaustekniikat.
- Todentaminen. Todentamisella varmistetaan, että kaikki osapuolet, joilla on pääsy transaktioon ovat luotettuja ja eivät ole toiseksi tekeytyneitä. Tämän tavoitteen mahdollistavat esimerkiksi salasanat ja muut tunnistustavat.
- Eheys. Maksuun liittyvät tiedot ja järjestelmät eivät ole ulkopuolisen osapuolen muuttamia tai korruptoimia. Eheyden takaamisessa voidaan hyödyntää esimerkiksi digitaalista allekirjoitusta.
- Valtuuttaminen. Kaikkien transaktioon liittyvien osapuolten on voitava vahvistaa, että kaikki transaktioon osallistuvat ovat oikeutettuja suorittamaan kyseisen transaktion, esimerkiksi digitaalisen sertifikaatin avulla.
- Kiistämättömyys. Järjestelmän on varmistettava, että käyttäjä ei voi kieltää suorittaneensa transaktiota ja siten jättää maksua suorittamatta. Käyttäjän on esitettävä todisteet väitteensä tueksi, jos tällainen tilanne esiintyy.

Kadhiwal ja Zulfiquar (2007) lisäävät tähän listaan vielä kuudennen tavoitteen, saatavuuden. Heidän mukaan järjestelmän tulee olla saatavilla valtuutetuille käyttäjille kaikkina ajankohtina.

Subjektiivisella turvallisuudella puolestaan tarkoitetaan käyttäjän kokemaa turvallisuuden tasoa. Mobiilimaksamisen täytyy vaikuttaa turvalliselta käyttäjälle, sillä tavallinen käyttäjä ei todennäköisesti osaa arvioida turvallisuutta objektiivisen turvallisuuden näkökulmasta.

On myös huomion arvoista, että objektiivinen ja subjektiivinen turvallisuus eivät ole toisistaan irrallisia tai itsenäisiä ulottuvuuksia. Subjektiivinen turvallisuus ei vaikuta objektiiviseen turvallisuuteen laisinkaan, mutta toiseen suuntaan vaikutus toimii. Empiirisen tutkimuksen mukaan objektiivinen turvallisuus vaikuttaa subjektiivisen turvallisuuden tasoon. (Linck ym., 2006)

3.2 SSL/TLS haavoittuvuudet

Secure Sockets Layer (SSL) ja Transport Layer Security (TLS) ovat salausprotokollia, joiden tarkoituksena on suojata tietoliikennettä. SSL-protokollan alkuperäinen kehittäjä oli Netscape Communications 90-luvun alkupuolella, joka myöhemmin luovutti kehitysvastuun Internet Engineering Task Force (IETF)-organisaatiolle. IETF on avoin organisaatio, joka on vastuussa internet-protokollien standardoinnista. Erilaisista nimistä huolimatta TLS-protokolla on suoraa jatkumoa SSL-protokollalle, sillä TLS versio 1.0 vastaa hyvin pitkälti SSL 3.0 versiota. Nykyään TLS onkin käytännössä korvannut SSL:n kaikessa käytössä, mutta edelleen niistä puhutaan usein yhteisesti SSL/TLS-protokollina. Tällä hetkellä uusin versio on TLS 1.2, mutta versio 1.3 on myös työn alla. (Oppliger, 2016)

Transmission Control Protocol/Internet Protocol (TCP/IP) on joukko tietoverkkoprotokollia, jotka mahdollistavat tietokoneiden välisen kommunikaation. Internetin toiminta rakentuu TCP/IP-protokollaperheen päälle, minkä johdosta kyseessä onkin laajimmin käytetty verkkoliikenneprotokolla. TCP/IP kehitettiin ennen tiedonsiirtoprotokollien standardina toimivaa Open Systems Interconnection (OSI)- mallia, joten niiden välillä on eroja kerrosten määrissä. Vaikka TCP/IP ei perustukaan OSI-malliin, voidaan sitä kuitenkin hyödyntää verratessa TCP/IP:tä muihin protokollaperheisiin. (Blank, 2004) TCP/IP- ja OSI-mallien rakenteet ovat kuvattuna kuviossa 2.

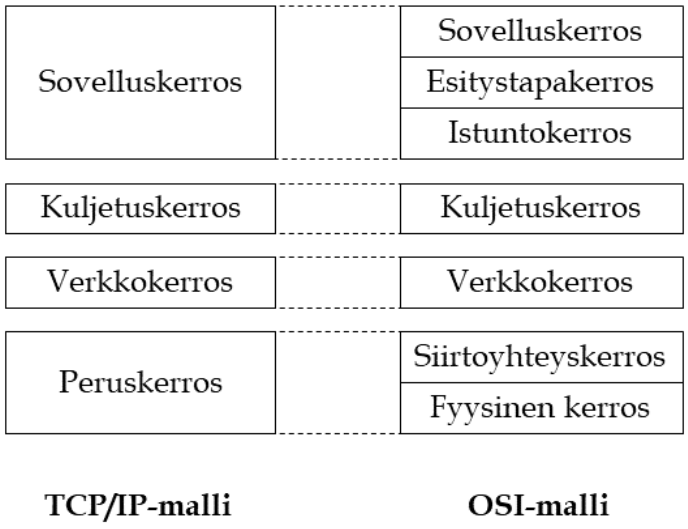
TCP/IP-mallin eri tasoilla käytetään eri protokollia ja menetelmiä. SSL/TLS-protokollia käytetään yhdessä muiden turvallisuusmekanismien ja -protokollien kanssa niin sanotun päästä päähän salauksen saavuttamiseksi. Tarkkaan ottaen SSL/TLS-protokollat toimivat TCP/IP-mallin sovellus- ja kuljetuskerroksen välissä, joskin yksinkertaistamisen vuoksi ne voidaan laskea kuljetuskerroksessa toimiviksi. Tyypillisessä käyttötilanteessa SSL/TLS-protokolla toimii yhdessä esimerkiksi Hypertext Transfer Protocol (http) -protokollan kanssa, joka puolestaan toimii sovelluskerroksella. Tätä yhdistelmää kutsutaan https-protokollaksi.

Kyseiset protokollat ovat läsnä kaikkialla tämän päivän internetissä. Niiden menestyksen takana on kaksi merkittävää tekijää. Ensinnäkin, niitä voidaan käyttää suojaamaan mitä tahansa sovelluskerroksen protokollaa. Käytännössä mikä tahansa TCP-yhteyttä käyttävä sovellus voidaan mahdollisesti suojata SSL/TLS-protokollilla. Tämän lisäksi SSL/TLS-protokollat toimivat lähestulkoon käyttäjälle näkymättömästi, joten käyttäjän ei tarvitse olla edes tietoinen niiden olevan käytössä. Tämä helpottaa protokollien käyttöönottoa huomattavasti. (Oppliger, 2016)

Monet mobiilimaksujärjestelmistä luottavatkin SSL/TLS-protokolliin datan suojaamiseksi verkossa. Näistä protokollista ja niiden käytöstä on kuitenkin löydetty kriittisiä haavoittuvuuksia, joita hyökkääjät ovat voineet hyödyntää turvallisuuden murtamisessa. (Wang ym., 2016)

Vuonna 2014 OpenSSL:stä, joka on avoimen lähdekoodin SSL/TLS toteutus, paljastui Heartbleed Bug-nimellä kutsuttu vakava haavoittuvuus. Haavoittuvuutta hyväksikäyttämällä hakkeri saattoi päästä käsiksi henkilökohtaiseen kuten luottokorttien numeroihin, käyttäjänimiin ja salasanoihin. Kenties huolestuttavinta oli se, että se mahdollisti myös salausavainten kaappaamisen ja palvelimena esiintymisen tai sen hallinnan. Kyseisen haavoittuvuus vaikutti moniin suosituimmistakin verkkopalveluista, kuten Facebook, Google ja Twitter. (Gujrathi, 2014) Heartbleed-nimitys juontuu TLS/DTLS-protokolliin liittyvästä heartbeat-laajennuksesta, jonka heikkoutta hyödyntämällä palvelimen tai asiakasohjelman muistin sisältö saatiin vuotamaan. Heartbleed-haavoittuvuutta hyväksikäyttävä hyökkääjä pystyy toimimaan täysin jälkiä jättämättä, haavoittuvuus on sittemmin paikattu OpenSSL:n uudemmissa versioissa. Palvelun käyttäjien on kuitenkin vaihdettava salasanansa haavoittuvuuden paikkaamisen jälkeen. (Synopsys, 2014)

Edellä mainittujen seikkojen ohella SSL/TLS:n on myös haavoittuvainen esimerkiksi Man in the Middle-hyökkäyksiä vastaan, joista kerrotaan kattavammin seuraavaksi.



KUVIO 2 TCP/IP- ja OSI-mallien kerrokset (mukaillen Oppliger, 2016)

3.3 Man in the Middle-hyökkäykset

RFC2828:ssa Man in the Middle (MitM tai MITM)-hyökkäys määritellään aktiiviseksi salakuunteluhyökkäyksen muodoksi, jossa hyökkääjä sieppaa ja valikoivasti muuntaa data naamioituakseen yhdeksi tai useammaksi yhteyttä pitäväksi osapuoleksi. (Shirey, 2003) Hyökkäystyypistä puhutaan joskus myös suomenkielisillä termeillä mies välissä- tai epärehellinen välittäjä-hyökkäys.

(Viestintävirasto, 2011) Tyypillisessä MitM-hyökkäyksessä hyökkääjä asettuu käyttäjän ja palvelimen väliin siten, että hän voi kommunikoida erikseen molempien osapuolten kanssa. Tällä tavoin sekä käyttäjä että palvelin luulevat kommunikoivansa suoraan toistensa kanssa, tietämättä hyökkääjän läsnäolosta. (Oppliger, Hauser & Basin, 2006)

MitM-hyökkäyksiin tarvittavat työkalut ovat helposti ja usein ilmaiseksi saatavilla verkossa, mikä nostaa niiden uhkaavuutta. Hyökkäyksen toteutukseen käytettävät työkalut riippuvat siitä, minkälaisessa verkossa hyökkäys toteutetaan. Esimerkiksi yhteyden tyyppi ja se, ovatko datapaketit salattuja vai eivät vaikuttavat käytetyn työkalun valintaan ja hyökkäyksen toimintaperiaatteeseen. Näistä seikoista riippuen hyökkääjä voi työkalujen avulla tekeytyä esimerkiksi reitittimeksi tai viestinnän kohteena olevana palvelimeksi. (Xia & Brustoloni, 2005)

Vaikka SSL/TLS-protokollat periaatteessa antavatkin riittävän suojan MitM-hyökkäyksiltä, ovat ne vakava uhka monille SSL/TLS-pohjaisille websovelluksille. Tämä johtuu ennen kaikkea kahdesta pääsyystä: ensinnäkin SSL/TLS palvelimen varmennus on monesti toteutettu huonosti tai ei ollenkaan naiivin loppukäyttäjän toimesta. Tämä johtaa tilanteeseen, jossa käyttäjä päätyy keskustelemaan epärehellisen välittäjän kanssa ja siten luovuttaa tunnistetietonsa tälle. Toiseksi SSL/TLS istunnon muodostus on usein irrallaan käyttäjän varmentamisesta, jonka johdosta hyökkääjä voi saamillaan tunnistetiedoilla huijata palvelinta. (Oppliger ym., 2006)

3.4 Haittaohjelmat

Haittaohjelmat ovat yksi suurimmista uhista mobiilimaksujärjestelmille ja niiden määrä kasvaa jatkuvasti. (Wang ym., 2016) Hyökkääjät ovat kehittäneet uusia tapoja mobiililaitteiden saastuttamiseen ja uusien mobiilihaittaohjelmien määrä kasvoikin vuonna 2017 peräti 54 prosenttia verrattuna vuoteen 2016. (Symantec, 2018)

Wangin, Streffin ja Ramanin (2012) mukaan älylaitteita uhkaavat haittaohjelmat voidaan jakaa kolmeen pääkategoriaan: vakoiluohjelmiin, viruksiin ja troijalaisiin. Viruksien leviävät laitteesta toiseen monistamalla itseään. Usein ne ovat piilotettuna johonkin tiedostoon, joka ladataan ja suoritetaan mobiililaitteessa. Virukset voi levitä myös Bluetoothin kautta.

Troijalaiset ovat usein naamioitu peleiksi, turvallisuuspäivitykseksi tai muuksi haluttavaksi sovellukseksi, jonka käyttäjä lataa laitteelleen. Nimitys juontuu antiikin Kreikan tarusta, jossa muinaiseen Troijaan hyökättiin suuren puuhevosen sisään piilotettujen sotilaiden avulla.

Suurin osa älypuhelimiin kohdistuvista haittaohjelmista kuuluvat vakoiluohjelmien ryhmään, joiden tavoitteena on kerätä käyttäjän tietoja tämän huomaamatta. Arvioiden mukaan yli 60 prosenttia Android-käyttöjärjestelmän puhelimista löytyvistä haittaohjelmista on juuri vakoiluohjelmia. (Wang ym., 2012)

Näiden haittaohjelmatyyppien lisäksi mobiililaitteita uhkaa niin sanotut grayware-sovellukset, jotka eivät ole suoranaisesti haittaohjelmia tai välttämättä edes pahantahtoisia, mutta voivat silti olla vahingollisia käyttäjälle. Grayware-sovellukset voivat esimerkiksi vuotaa käyttäjän sijaintitietoja ja muuta henkilökohtaista dataa. Myös tämän tyyppisten, käyttäjien yksityisyyttä uhkaavien sovellusten määrä on kasvussa, sillä mobiililaitteissa toimivien grayware-sovellusten lukumäärä nousi 20 prosenttia vuodesta 2016 vuoteen 2017. (Andow, Nadkarni, Bassett, Enck & Xie, 2016; Symantec, 2018)

Mobiililaitteiden lisäksi kassajärjestelmiin on tehty tietomurtoja haittaohjelmien avulla. Esimerkiksi vuonna 2014 suurten yhdysvaltalaisten vähittäismyyjäketjujen Targetin ja Home Depotin kassajärjestelmiin murtauduttiin Backoff-nimisellä haittaohjelmalla, jonka seurauksena rikolliset pääsivät käsiksi jopa miljoonien asiakkaiden henkilö- ja maksukorttitiedot. (Wang ym., 2016)

4 TURVALLISUUSUHKIEN TORJUNTA

Tässä luvussa käsitellään tärkeimpiä torjuntatapoja mobiilimaksamisen turvallisuusuhille. Myös edellisessä luvussa käsitelty SSL/TLS kuuluu keskeisiin tekijöihin mobiilimaksamisen turvallisuudessa heikkouksistaan huolimatta. Keskeisimpiin torjuntatapoihin kuuluvat salaustekniikat, käyttäjän todentaminen sekä haittaohjelmien tunnistaminen ja torjunta.

4.1 Salaus

Salaustekniikoilla on merkittävä rooli mobiilimaksujen suojaamisessa avoimissa verkoissa, joissa on hyvin vähän tai ei lainkaan fyysistä turvaa. (Isaac & Sherali, 2014) Salaustekniikat voidaan jakaa kahteen tyyppiin, symmetrisiin ja epäsymmetrisiin. (Järvinen, 2005)

Symmetrinen salaus tarkoittaa sitä, että viestin lähettäjät ja vastaanottajat käyttävät samaa, ennalta sovittua avainta salauksen purkamiseen. Symmetriset salaustekniikat perustuvat bittien sekoittamiseen ja soveltuvat hyvin mobiiliympäristöön niiden matalien laskentatehovaatimusten vuoksi. Toisaalta avainten hallinta on haasteellista symmetrisistä salausta käytettäessä. (Järvinen, 2005; Isaac & Sherali, 2014)

Epäsymmetrinen tai asymmetrinen salaus puolestaan perustuu kahteen erilliseen avaimeen, julkiseen (eng. *public key*) ja yksityiseen (eng. *private key*). Viestin lähettäjä salaa viestin julkisella avaimella ja viestin vastaanottaja puolestaan purkaa sen yksityisellä avaimellaan. Julkista avainta voidaan jakaa täysin huoletta, sillä sitä käytetään vain salaamiseen. Sen avulla ei voida purkaa viestin salausta, joten edes lähettäjä itse ei pysty avaamaan salaamansa viestiä. Yksityinen avain sen sijaan on pidettävä huolellisesti suojattuna ja sen paljastuessa järjestelmä on haavoittuvainen. Epäsymmetrinen salaus perustuu bittien sekoittamisen sijaan matemaattiseen laskentaan. Avainten hallinta on siis huomattavasti helpompaa julkiseen avaimen järjestelmissä, mutta ne tarvitsevat merkittävästi pidemmät avaimet. Tämän seurauksena epäsymmetrinen salaus vaatii

paljon enemmän laskentatehoa ja on yleisesti ottaen hitaampaa. (Järvinen, 2005; Isaac & Sherali, 2014)

Epäsymmetriset salausjärjestelmät käyttävät yleensä RSA salausalgoritmia, joka on nimetty sen kehittäjien - Rivest, Shamir ja Adleman - sukunimien alkukirjainten mukaan. (Järvinen, 2005) RSA ei kuitenkaan ole ainut mahdollisuus julkisen avaimeen perustuvien salausten tekemiseen ja yksi potentiaalinen, uudempi ehdokas on elliptisten käyrien salausmenetelmä (eng. *elliptic curve cryptography, ECC*). Toistaiseksi elliptisten käyrien salausmenetelmiä ei ole juuri hyödynnetty, mutta se takaa samanlaisen turvallisuuden kuin RSA huomattavasti lyhyemmillä avaimilla. Lyhyempien avainten etuja ovat nopeammat laskutoimitukset, matalampi virran ja muistin kulutus sekä kaistanleveyden säästyminen. Näistä syistä ECC olisi mainio ratkaisu mobiililaitteisiin, jotka ovat resursseilla rajoittuneita. Toisaalta käytännön toteutusta pidetään haasteellisempana verrattuna RSA:han, joka on vanhempi ja laajemmin tuettu menetelmä. (Isaac & Sherali, 2014)

4.2 Käyttäjän todentaminen

Käyttäjän todentaminen on äärimmäisen tärkeä toiminto mobiilimaksamisen turvallisuuden kannalta. Mobiililaitteet sisältävät jo itsessään usein todentamistapoja, joihin kuuluvat esimerkiksi Personal Identification Number (PIN) ja Personal Unblocking Key (PUK). Nämä todentamistavat hyödyntävät mobiililaitteissa yleistä SIM-korttia. Yleinen toimintatapa on hyödyntää yksinkertaisesti käyttäjänimeä ja salasanaa. (Kadhiwal & Zulfiquar, 2007)

Monivaiheinen todentaminen on huomattavasti turvallisempi kuin perinteiset salasanat ja vastaavat, jotka voivat alttiita arvaamiselle ja väsytyshyökkäyksille (eng. *brute-force attack*). Monivaiheiset järjestelmät käyttävät kahta tai useampaa itsenäistä tekijää osana käyttäjän tunnistetietoja ja lisäävät siten ylimääräisiä turvallisuuskerroksia käytössä olevaan todentamisprosessiin tuoden siihen lisää vahvuutta. (Jain & Shanbhag, 2012) Käyttäjältä voidaan esimerkiksi pyytää kertakäyttöistä todentamiskoodia palveluun kirjautumisen yhteydessä uudella laitteella. Tämän jälkeen käyttäjän kyseinen koodi lähetetään käyttäjän rekisteröimään sähköpostiosoitteeseen. (Wang ym., 2016)

Mobiilimaksamisessa myös biometrinen tunnistautuminen voi olla toimiva ratkaisu mobiililaitteiden multimediavalmiuksien myötä. Biometrisiä tunnistusmenetelmiä ovat esimerkiksi sormenjäljen, äänen ja kasvojen tunnistus. (Gao ym. 2005; Derawi, Nickel, Bours & Busch, 2010) Biometristen tunnistautumistapojen merkittävin etu salasanoihin ja vastaaviin on se, että niitä ei voi unohtaa tai varastaa. Biometriikan avulla voidaan muodostaa eksplisiittinen linkki käyttäjän identiteettiin. Yleisimmin näiden tunnistautumistapojen käyttö vaatii käyttäjältä selkeän toimen, kuten sormen laittamisen sormenjäljenlukijalle.

Fyysisten ominaisuuksien käyttäminen ei kuitenkaan ole ainut vaihtoehto biometrisissä menetelmissä. Käyttäjä voidaan todentaa myös esimerkiksi käve-

lytyylin perustella, sillä eri tieteenalojen tutkimusten mukaan jokaisen ihmisen kävelytyyli sisältää yksilöllisiä malleja. Käyttäjän kävelytyyliä voidaan tarkkailla monista mobiililaitteista nykyisin löytyvien kiihtyvyysantureiden avulla. Tämän tapaisia todentamismenetelmiä kutsutaan huomaamattomiksi, sillä ne eivät vaadi käyttäjältä aktiivista toimintaa. Huomaamattoman todentamisen on havaittu olevan muita tapoja käyttäjäystävällisempää. (Derawi ym., 2010)

Erittäin vahva käyttäjän todentaminen voidaan toteuttaa multimodaalisen todentamisen avulla. Tämä tarkoittaa kahden tai useamman tunnistusmenetelmän käyttämistä yhdessä, esimerkiksi sormenjäljen ja äänen yhdistelmää. Multimodaalisella todentamisella voidaan laskea merkittävästi järjestelmän virheprosenttia. (Bigun, Fiérrez-Aguilar, Ortega-Garcia & Gonzalez-Rodriguez, 2003)

4.3 Haittaohjelmien tunnistaminen ja torjunta

Haittaohjelmat kuuluvat suurimpiin huolenaiheisiin mobiilimaksamisen turvallisuuden kannalta. Vaikka haittaohjelmien havaitsemiseen ja torjuntaan on käytetty useita eri tapoja, ovat ne silti löytäneet tapoja levittäytyä mobiililaitteissa. (Wang ym., 2016)

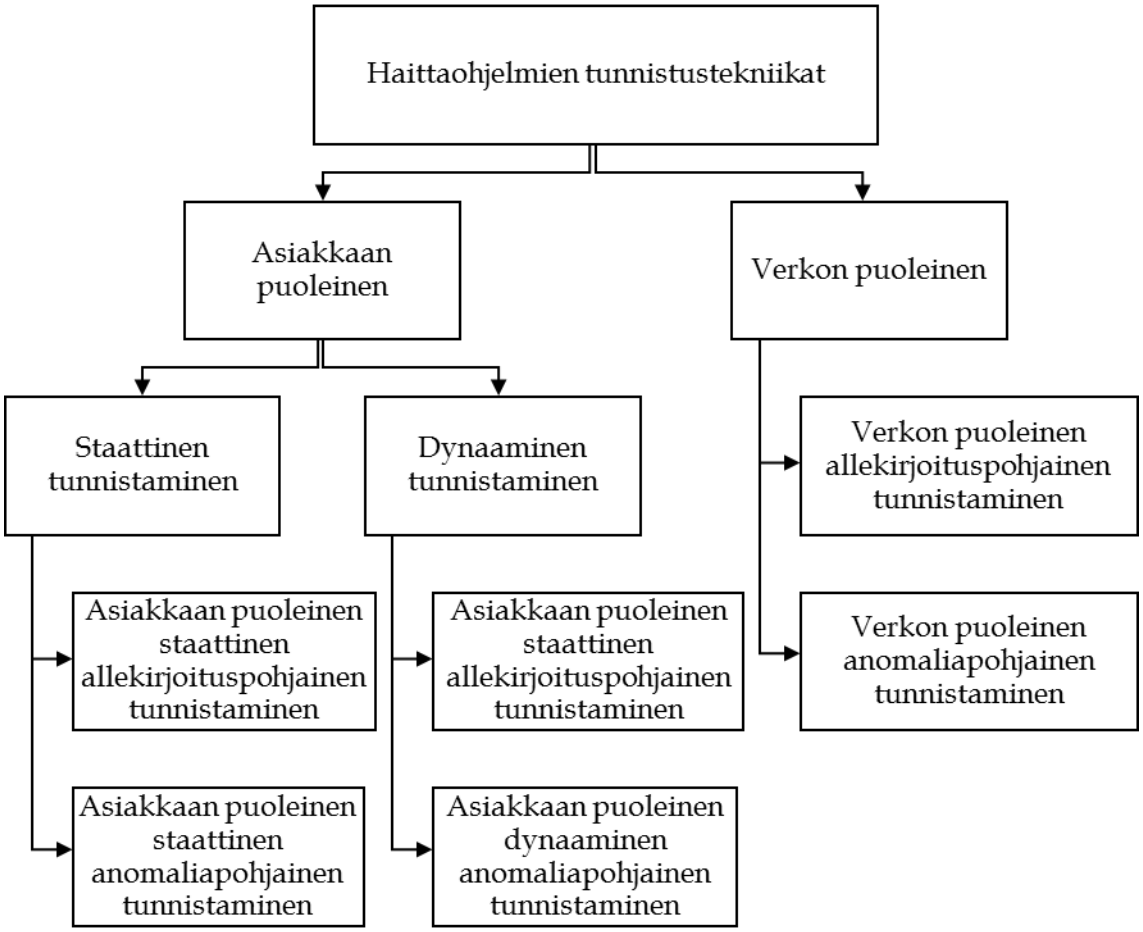
Mobiilihaittaohjelmien tunnistustekniikat voidaan jakaa ryhmiin niiden ominaispiirteiden mukaan (ks. kuvio 3). Toimintaperiaatteen tasolla jako tehdään kahteen ryhmään, allekirjoitus- ja anomaliapohjaisiin. Allekirjoituspohjaisissa tekniikoissa tunnettujen haittaohjelmien käytös tallennetaan niiden jättäminä allekirjoituksina. Haittaohjelma voidaan siten tunnistaa, kun sen allekirjoitus havaintaan jossakin. Anomaliapohjaisissa tekniikoissa sen sijaan mallinnetaan aluksi järjestelmän normaali toiminta. Tämän jälkeen haittaohjelmat voidaan havaita poikkeuksina eli anomalioina järjestelmän normaalissa käytöksessä.

Haittaohjelman tunnistaminen voi perustua joko staattiseen tai dynaamiseen analyysiin. Staattisessa analyysissä koodi tai sovellus analysoidaan ilman, että sitä suoritetaan, mikä on tyypillisesti nopeaa ja yksinkertaista. Dynaamisessa analyysissä puolestaan valvotaan sovelluksen käytöstä eristetyssä ympäristössä, keräten samalla tietoa sovelluksen ajonaikaisesta toiminnasta. Dynaaminen analyysi keskittyy siihen, miksi ja kuinka usein tietyt epäilyttävät operaatiot suoritetaan.

Tunnistustekniikat voidaan jakaa kahteen luokkaan myös sen perustella, tapahtuuko tunnistaminen asiakkaan vai verkon puolella. Asiakkaan puolella toimivat tekniikat voivat toimia joko paikallisesti isäntäkoneessa, eli mobiililaitteessa, tai hyödyntää pilvipalveluja. Suurin osa mobiililaitteessa paikallisesti toimivista tunnistustyökaluista perustuvat allekirjoituspohjaiseen tunnistamiseen, joka vaatii suuren, ajantasaisen tietokannan eri haittaohjelmista. Tallennustilan ja laskentatehon pieni määrä ovat mobiililaitteiden suurimpia heikkouksia tehokkaiden tunnistusmenetelmien käytön kannalta, mutta tätä rajoi-

tetta voidaan kiertää pilvipalveluiden avulla. Pilvipalveluita hyödyntävien järjestelmien etuna on myös se, että ne voivat käyttää sekä allekirjoitus- että anomaliapohjaisia tunnistusmenetelmiä yhtäaikaisesti.

Verkon puolella toimivat järjestelmät voivat tarjota suojaa käyttäjälle, joka ei ole tietoinen suojan tarpeesta tai ei halua asentaa mobiilihaittaohjelmien tunnistamiseen käytettävää ohjelmistoa. Tällaiset järjestelmät pyrkivät havaitsemaan haittaohjelmat tarkkailemalla verkkoliikennettä ja mobiililaitteista peräisin olevia tapahtumia. (He, Chan & Guizani, 2015)



KUVIO 3 Haittaohjelmien tunnistustekniikat (mukaillen He, Chan & Guizani, 2015)

Mobiilihaittaohjelmien torjunnassa on neljä keskeistä sidosryhmää ja tasoa: sovellusten kehittäjät, palvelut, laitteiden käyttäjät ja laitteet. On äärimmäisen tärkeää, että turvallisuus toteutetaan jokaisella tasolla ja jokaisen sidosryhmän osalta.

Sovellusten kehittäjien täytyy seurata turvalliseen ohjelmointiin ja yksityisyyteen liittyviä käytäntöjä. Tarpeettomaan informaatioon ei tulisi olla käyttöoikeuksia ja arkaluontoinen tieto on salattava sekä paikallisesti että palvelimilla.

Palveluiden, kuten sovellusten myyntialustojen, on suoritettava kunnollinen seulontaprosessi ja poistettava epäilyttävät sovellukset. Palveluilla on oltava hyvät turvallisuuskäytännöt ja suunnitelma mahdollisten häiriötilanteiden varalle.

Mobiililaitteen käyttäjän on huolehdittava, että he asentavat laadukkaan mobiiliturvallisuusratkaisun ja lataavat sovelluksia vain luotetuista kauppapaikoista. Ennen minkään sovelluksen asentamista on tehtävä tutkimusta kyseisestä sovelluksesta, esimerkiksi arvioita lukemalla. Lisäpalvelut, kuten Wi-Fi ja Bluetooth, on pidettävä pois päältä, kun niitä ei käytetä. Käyttäjän ei myöskään kannata ”jailbreakata” järjestelmää, sillä se tekee laitteesta haavoittuvaisemman. Jailbreak termillä viitataan käyttöjärjestelmän muokkaamiseen poistamalla sen estävät rajoitukset.

Laitteen tasolla on vaatimuksena käyttöjärjestelmän suojaus. Turvallisuusperiaatteet, kuten rajalliset oikeudet ja prosessien eristäminen hillitsevät turvallisuutta loukkaavia sovelluksia. (Ramu, 2012)

5 YHTEENVETO JA POHDINTA

Tutkielmassa käsiteltiin kirjallisuuskatsauksen keinoin mobiilimaksamista ja sen turvallisuutta. Mobiilimaksamiseen liittyvien turvallisuusuhkien lisäksi esiteltiin keskeisimpiä tapoja näiden uhkien torjumiseksi. Aiheen tutkiminen on tärkeää alan kannalta, sillä mobiilimaksupalvelun täytyy pystyä turvaamaan käyttäjiensä rahaliikenteeseen liittyviä tietoa henkilötietojen ohella. Turvallisuus onkin mobiilimaksupalvelun menestyksen kannalta elintärkeää, sillä useiden tutkimusten mukaan turvallisuus on helppokäyttöisyyden ohella merkittävimpiä tekijöitä, jotka vaikuttavat palvelun käyttöönottoon.

Tutkimuskysymyksenä tässä tutkielmassa oli *"Mitä ovat mobiilimaksamisen turvallisuusuhat ja kuinka niitä voidaan torjua?"* Tärkeimpiä tavoitteita oli selvittää, mistä tekijöistä mobiilimaksamisen turvallisuus muodostuu, millaisia turvallisuusuhkia mobiilimaksamiseen liittyy ja mitkä ovat keskeisimpiä tapoja torjua näitä uhkia. Kirjallisuudessa keskeisimmiksi turvallisuusuhiksi nousivat SSL/TLS-protokollien haavoittuvuudet, Man in the Middle-tyyppiset datan kaappaamiseen pyrkivät hyökkäykset ja vuosi vuodelta yleistyvämmät mobiilihaittaohjelmat. Uhkien torjunnassa tärkeimpiä seikkoja ovat datan laadukkaasti toteutettu salaaminen, käyttäjän luotettava tunnistaminen ja haittaohjelmien tunnistaminen ja torjunta erilaisia menetelmiä ja sovelluksia hyväksi käyttäen.

Tutkielmassa mobiilimaksamisella tarkoitettiin maksua, jossa vähintään yhtä mobiililaitetta käytetään maksuprosessin jossakin vaiheessa ja käytetään hyväksi langattomia verkkoteknologioita. Tällä hetkellä yleisin laite mobiilimaksussa on älypuhelin, mutta se voi varsin hyvin olla mikä tahansa muukin langattomiin verkkoihin yhdistyvä mobiililaite, kuten älykello tai kannettava pelikonsoli. Mobiilimaksuja voidaan luokitella monella tavalla, esimerkiksi niiden suuruuden, laskutuksen ajoituksen tai maksupalvelua tarjoavan organisaation mukaan. Mobiilimaksujen siirtäminen voidaan toteuttaa useiden eri teknologioiden avulla, joilla on omat hyvät ja huonot puolensa. Myös useamman teknologian käyttäminen yhdessä on mahdollista ja tekninen toteutus riippuukin täysin palvelusta.

Mobiilimaksamisen turvallisuus muodostuu objektiivisesta ja subjektiivisesta turvallisuudesta, eli toisin sanoen teknisestä ja koetusta turvallisuudesta. Objektiivisesti turvallinen mobiilimaksujärjestelmä huolehtii luottamuksellisuudesta, todentamisesta, eheydestä, valtuuttamisesta, kiistattomuudesta ja saatavuudesta. Subjektiivisesti turvallinen palvelu sen sijaan luo käyttäjälle turvallisen vaikutelman.

Alan tutkimusten perusteella keskeisimpiin turvallisuusuhkiin kuuluvat haittaohjelmat, joiden määrä mobiililaitteissa on noussut jatkuvasti viime vuosien aikana. Haittaohjelmia on useita eri tyyppejä ja niiden vaikutus vaihtelee ammattirikollisten kehittämistä erikoistuneista työkaluista grayware-tyyppisiin sovelluksiin, jotka eivät ole välttämättä edes pahantahtoisia vaan voivat olla vain huolimattomasti suunniteltuja. Haittaohjelmien lisäksi esimerkiksi Man in the Middle-tyyppiset hyökkäykset, joissa hyökkääjä salakuuntelee tai kaappaa asiakkaan ja palvelimen väliseksi tarkoitettua dataa, ovat osa keskeisiä turvallisuusuhkia.

Myös olemassa olevien ja itsessään toimivien turvallisuusominaisuuksien, kuten SSL/TLS-protokollien, virheellinen tai puutteellinen toteutus voidaan katsoa turvallisuusuhaksi. Tietojärjestelmiä kehittäessä on aina mahdollista tapahtua virheitä ja hakkerit ovat luonnollisesti huomattavan kiinnostuneita rahaliikenteeseen liittyvistä järjestelmistä. Näistä syistä mobiilimaksamisen potentiaalisista turvallisuusuhista ja niiden mahdollisista torjuntatavoista on syytä olla erityisen kiinnostunut.

SSL/TLS-protokollien huolellisen toteuttamisen ohella turvallisuusuhkien torjunnassa merkittävä rooli on salaustekniikoilla. Vahvat salaustekniikat antavat turvaa langattomia viestintätekniikoita käytettäessä. Mobiililaitteiden suojaaminen haittaohjelmilta on myös äärimmäisen tärkeää. Haittaohjelmien havaitsemiseen ja torjuntaan onkin tarjolla erilaisia malleja ratkaisuja. Käyttäjän todentaminen on monille loppukäyttäjille tutuin ja näkyvin turvallisuusmekanismi. Se voidaan toteuttaa esimerkiksi käyttäjätunnuksen ja salasanan avulla tai vaikkapa biometrisiä menetelmiä, kuten sormenjälkeä, hyödyntäen.

Teknologian kehittyminen avaa myös uusia mahdollisuuksia mobiilimaksamisen ja sen turvallisuuden tutkimiselle. Mobiililaitteiden jatkuvasti kasvava laskentateho, puettavan teknologian yleistyminen ja lähitulevaisuudessa häämöttävät, entistä nopeammat 5G-mobiiliverkkoyhteydet luovat paitsi uusia mahdollisuuksia niin myös haasteita alan toimijoille. Jos mobiilimaksamisen suosio kasvaa ennusteiden mukaan länsimaissakin, voidaan myös olettaa, että rikollisten mielenkiinto sitä kohtaan kasvaa. Turvallisten maksujärjestelmien suunnittelun merkitys tuleekin korostumaan entisestään. Muita kiinnostavia tutkimusaiheita ovat esimerkiksi pilvipalveluiden käyttö mobiilimaksujärjestelmissä, sekä tehokkuuden että turvallisuuden näkökulmasta. Mobiiliympäristössä tapahtuva haittaohjelmien tunnistaminen vaatii myös lisätutkimusta, jotta se yleistyisi loppukäyttäjien keskuudessa. Samaa voidaan sanoa myös elliptisten käyrien salausmenetelmistä, joita ei ole toistaiseksi juuri hyödynnetty tutkimusmaailman ulkopuolella.

LÄHTEET

Andow, B., Nadkarni, A., Bassett, B., Enck, W. & Xie, T. (2016). A study of grayware on google play. (s. 224-233) IEEE.

Au, Y. A. & Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications, 7*(2), 141-164.

Blank, A. G. (2004). *TCP/IP foundations*. Alameda: Wiley. Haettu osoitteesta http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=267310

Bhalla, M. R. & Bhalla, A. V. (2010). Generations of mobile wireless technology: A survey. *International Journal of Computer Applications*, *5(4)*

Bigun, J., Fiérrez-Aguilar, J., Ortega-Garcia, J. & Gonzalez-Rodriguez, J. (2003). Multimodal biometric authentication using quality signals in mobile communications. (s. 2-11) IEEE.

Carr, M. (2007). Mobile payment systems and services: An introduction. (s. 12)

Clarke, R. (2008). A risk assessment framework for mobile payments. *BLED 2008 Proceedings,* 40.

Curran, K., Millar, A. & Mc Garvey, C. (2012). Near field communication. *International Journal of Electrical and Computer Engineering, 2(3)*, 371.

Dahlberg, T., Guo, J. & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications, 14(5)*, 265-284.

Dahlberg, T., Mallat, N., Ondrus, J. & Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications, 7*(2), 165-181.

Dahlberg, T., Mallat, N. & Öörni, A. (2003). Trust enhanced technology acceptance model - consumer acceptance of mobile payment solutions: Tentative evidence. *Stockholm Mobility Roundtable, 22*, 23.

Dahlman, E., Parkvall, S. & Skold, J. (2016). *4G, LTE-advanced pro and the road to 5G*. Academic Press.

Derawi, M. O., Nickel, C., Bours, P. & Busch, C. (2010). Unobtrusive user-authentication on mobile phones using biometric gait recognition. (s. 306-311) IEEE.

Gannamaneni, A., Ondrus, J. & Lyytinen, K. (2015). A post-failure analysis of mobile payment platforms. (s. 1159-1168) IEEE.

Gao, J., Cai, J., Patel, K. & Shim, S. (2005). A wireless payment system. (s. 8 pp.) IEEE.

Gujrathi, S. (2014). Heartbleed bug: AnOpenSSL heartbeat vulnerability. *International Journal of Computer Science and Engineering, 2(5)*, 61-64.

Harris, I., Hillebrand, F., Holley, K. & Trosby, F. (2010). *Short message service (SMS) : The creation of personal text messaging*. Chichester, West Sussex, U.K. ; Hoboken, NJ: Wiley. Haettu osoitteesta http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=480469

He, D., Chan, S. & Guizani, M. (2015). Mobile application security: Malware threats and defenses. *IEEE Wireless Communications, 22(1)*, 138-144

Isaac, J. T. & Sherali, Z. (2014). Secure mobile payment systems. *IT Professional, 16(3),* 36-43.

ITU-R. (2008). *Report ITU-R M.2134. Requirements related to technical performance for IMT-advanced radio interface(s)*

Jain, A. K. & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional, 14(5),* 28-33.

Jette, J. (2005, Feb 14,). Ka-ching! mobile commerce gets closer. Haettu osoitteesta https://hbswk.hbs.edu/archive/ka-ching-mobile-commerce-gets-closer

Järvinen, P. (2005). *Salausmenetelmät* (2. p.). Jyväskylä: Docendo. Haettu osoitteesta https://jyu.finna.fi/Record/jykdok.974991

Jovanovic, M. & Muñoz-Organero, M. (2011). Analysis of the latest trends in mobile commerce using the NFC technology. *Cyber Journals*

Kadhiwal, S. & Zulfiquar, A. U. S. (2007). *Analysis of mobile payment security measures and different standards* doi://doi.org/10.1016/S1361-3723(07)70077-5

Karnouskos, S. & Fokus, F. (2004). Mobile payment: A journey through existing procedures and standardization initiatives. *IEEE Communications Surveys & Tutorials, 6(4)*

Kazan, E. & Damsgaard, J. (2014). An investigation of digital payment platform designs: A comparative study of four European solutions. *Proceedings of the 2014 European Conference on Information systems*

Kreyer, N., Pousttchi, K. & Turowski, K. (2002). Standardized payment procedures as key enabling factor for mobile commerce. (s. 400-409) Springer.

Lerner, T. (2013). *Mobile payment*. Wiesbaden: Springer Fachmedien Wiesbaden. Haettu osoitteesta http://dx.doi.org/10.1007/978-3-658-03251-7

Linck, K., Pousttchi, K. & Wiedemann, D. G. (2006). Security issues in mobile payment from the customer viewpoint. *European Conference on Information Systems (ECIS), 14*

McDermott-Wells, P. (2004). What is Bluetooth? *IEEE Potentials, 23*(5), 33-35.

Me, G. (2003). Security overview for m-payed virtual ticketing. (s. 844-848) IEEE.

Merz, M. (2002). *E-commerce und E-business: Marktmodelle, anwendungen und technologien* dpunkt-Verlag.

Ondrus, J. & Pigneur, Y. (2009). Near field communication: An assessment for future payment systems. *Information Systems and E-Business Management, 7*(3), 347-361.

Oppliger, R. (2016). *SSL and TLS : : Theory and practice* (Second edition). Norwood, MA: Artech House. Haettu osoitteesta http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1498635

Oppliger, R., Hauser, R. & Basin, D. (2006). SSL/TLS session-aware user authentication–Or how to effectively thwart the man-in-the-middle. *Computer Communications, 29*(12), 2238-2246.

Parkvall, S., Dahlman, E., Furuskar, A., Jading, Y., Olsson, M., Wanstedt, S. & Zangi, K. (2008). *LTE-advanced-evolving LTE towards IMT-advanced.* (s. 1-5) IEEE.

Ramu, S. (2012). Mobile malware evolution, detection and defense. *EECE 571B, Term Survey Paper*

Sanou, B. (2016). ICT facts and figures 2016. *International Telecommunication Union*

Shirey, R. (2003). RFC 2828–Internet security glossary, 2000. *URL: Http://Www.Faqs.Org/Rfcs/rfc2828.Html,*

Symantec. (2018). *Symantec 2018 internet security threat report*

Synopsys. (2014, 29.4.). The Heartbleed bug. Haettu osoitteesta http://heartbleed.com/

Taylor, E. (2016). Mobile payment technologies in retail: A review of potential benefits and risks. *International Journal of Retail & Distribution Management, 44*(2), 159-177.

Viestintävirasto. (2011, 28.09.). Man in the middle -hyökkäyksen torjunta. Haettu osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2011/09/ttn201109281253.html

Wang, Y., Hahn, C. & Sutrave, K. (2016). Mobile payment security, threats, and challenges. (s. 1-5) IEEE.

Wang, Y., Streff, K. & Raman, S. (2012). Smartphone security challenges. *Computer, 45*(12), 52-58.

Wu, J., Liu, L. & Huang, L. (2016). Exploring user acceptance of innovative mobile payment service in emerging market: The moderating effect of diffusion stages of WeChat payment in china. (s. 238)

Xia, H. & Brustoloni, J. C. (2005). Hardening web browsers against man-in-the-middle and eavesdropping attacks. (s. 489-498) ACM.

Zhou, T. (2013). An empirical examination of continuance intention of mobile payment services. *Decision Support Systems, 54*(2), 1085-1091.

Zmijewska, A., Lawrence, E. & Steele, R. (2004). Classifying m-payments–a user-centric model. *Proceedings of the Third International Conference on Mobile Business, M-Business 2004*