POLIISI
POLIISIAMMATTIKORKEAKOULU

Mitä skimmaus on?

Jonne Kunelius

4/2017

POLIISIAMMATTIKORKEAKOULUN OPINNÄYTETYÖ / AMK

Tiivistelmä

Tekijä	Tutkinto/kurssi ja opinnäytetyö/nimike
Jonne Kunelius	Poliisi (AMK) 20141
Julkaisun nimi Mitä skimmaus on?	Julkisuusaste Julkinen
Ohjaajat ja opintoaine/opetustiimi Mari Koskelainen / yleisvalmiudet	Opinnäytetyön muoto Kartoitus

Tiivistelmä

Tässä opinnäytetyössä käsitellään maksukorttirikollisuuteen kuuluvaa skimmausta, joka on tullut Suomeen 2000-luvulla. Skimmauksella tarkoitetaan erillisellä käteis- ja maksuautomaatteihin asennettavalla laitteella, skimmerillä, tapahtuvaa maksukorttien magneettijuovan kopioimista. Suomessa epäiltyjä skimmaustapauksia on vuonna 2016 kirjattu 81 kappaletta RikiTrip- järjestelmän mukaan.

Opinnäytetyön tavoitteena on tarjota kattava tietopaketti skimmauksesta kiinnostuneille. Ymmärtääkseen skimmausta, on lukijan hyvä ymmärtää siihen vaikuttavia yksittäisiä tekijöitä. Opinnäytetyössä esitellään maksukortin rakennetta ja toimintaa, maksuautomaatilla tapahtuvaa maksuprosessia sekä pankkiautomaatin toimintaa yleisellä tasolla. Maksukorttia käsittelevässä luvussa kerrotaan lisäksi magneettijuovan ja sirullisten maksukorttien toiminnasta. Tämän lisäksi opinnäytetyön lopussa esitellään skimmausrikollisuuden tutkimiseen liittyvää lainsäädäntöä.

Itse skimmaus esitellään perusteiden lisäksi myös poliisin järjestelmistä haettujen tilastojen avulla. Työn loppupuolella esitellään muutamia Suomesta löydettyjä skimmauslaitteita valokuvien avulla. Niiden avulla lukija saa hyvän kuvan, millaisia erilaisia skimmauslaitteita on olemassa.

Työn lähteinä on käytetty internetistä löytyviä englanninkielisiä artikkeleja, poliisin tietojärjestelmän Rikitripin tilastoja sekä keskusrikospoliisin kyberrikosyksikön ja Europolin maksuvälinerikollisuuden parissa työskentelevien asiantuntijoiden haastatteluja.

Sivumäärä	Tarkastuskuukausi ja vuosi	Opinnäytetyökoodi (OPS)
48	5/2017	Amk2014ONT

Avainsanat

maksukorttirikollisuus, maksukortti, skimmaus, skimming, skimmer

Sisällysluettelo

KUVIOT

KUVAT

LYHENTEET

RL	Rikoslaki
PolL	Poliisilaki
PKL	Pakkokeinolaki
KRP	Keskusrikospoliisi
EMV	Maksukortista löytyvä siru
Rikitrip	Poliisin tietokanta
RTL	Rikostekninen laboratorio
SEPA	Single Euro Payments Area
NFC	Near field communication

1. JOHDANTO

Skimmaus on Suomeen 2000-luvulla rantautunut maksukorttirikollisuuden muoto, johon kuka tahansa voi törmätä maksaessaan kylmäasemalla tai nostaessaan rahaa pankkiautomaatilta. Ajatus skimmauksesta opinnäytetyön aiheeksi valikoitui oman kiinnostukseni vuoksi. Olen kiinnostunut rikostutkinnan monimuotoisuudesta ja etenkin rikostutkintaan osana kuuluvasta teknisestä tutkinnasta. Teknistä tutkintaa on mahdollista päästä tekemään esimerkiksi silloin, kun rikokseen liittyy joitakin elektronisia laitteita. Näitä rikoksia tutkittaessa on mahdollista perehtyä perinpohjaisesti rikoksiin liittyvien laitteiden toimintaan sekä siten kasvattaa omaa tietotaitoa aiheesta. Tämä tietotaitoa on mahdollista hyödyntää myöhemmin samankaltaisia rikoksia tutkittaessa.

Työskentelin harjoittelun aikana nuoremman konstaapelin virassa Turun pääpoliisiasemalla. Tutkintajakson aikana törmäsin ensimmäistä kertaa skimmauslaitteeseen erään tehtävän yhteydessä. Laite oli minulle uusi ja aiempi tietoni siitä pohjautui uutisista lukemaani. Kysyttäessä kollegoilta laitteesta, vastaus oli poikkeuksetta, ettei kukaan tiennyt aivan perusteita lukuun ottamatta mitään kyseisistä laitteista. Saamani ohje oli viedä laite tekniikkaan, jossa se hoidettaisiin eteenpäin. Jäin kuitenkin pohtimaan yleisesti heikkoa tietopohjaa skimmauslaitteista, joiden toimintaperiaate alkoi kiinnostaa minua. Päätin opinnäytetyössäni perehtyä asiaan tarkemmin, jotta jokaisella työni lukeneella olisi opinnäytetyöni lukemisen jälkeen käsitys skimmauksesta sekä siihen liittyvistä laitteista. Skimmauslaite määritellään tarkemmin opinnäytetyön luvussa viisi.

Vaikka opinnäytetyöni ajatuksena on ollut keskittyä pääasiassa kentällä työskentelevälle poliisille hyödyllisiin tietoihin skimmauksesta, on työstä hyötyä myös muille aiheesta kiinnostuneille, esimerkiksi rikoksen uhreille. Tietoa skimmauksesta on ollut aiemmin saatavilla suomen kielellä hyvin vähän, mikä on tehnyt aiheeseen perehtymisestä haastavaa. Omakohtainen esimerkkini on ajalta ennen poliisiopintoja, jolloin hyvä ystäväni huomasi tililtään hävinneen pienehkön summan rahaa, vaikkei hän ollut ostanut mitään. Nosto oli tehty ulkomailla. Myöhemmin selvisi, että hänen korttinsa oli todennäköisesti skimmattu huoltoasemalla tankkauksen yhteydessä. Etsimme yhdessä tuolloin tietoa skimmauksesta, mutta sitä ei juuri ollut saatavilla.

Luvuissa kolme ja neljä tutustutaan lisäksi tarkemmin erilaisiin maksukortteihin, niistä löytyviin ominaisuuksiin, maksuprosessiin, pankki- ja maksuautomaatteihin sekä niiden toiminaan. Edellä mainitut seikat liittyvät läheisesti skimmaukseen ja skimmauslaitteiden toimintaan. Lisäksi niiden ymmärtäminen auttaa ymmärtämään myös skimmausta aiempaa kokonaisvaltaisemmin. Skimmauksen lisäksi luvussa kaksi käsitellään maksukorttirikollisuutta yleisellä tasolla, sillä skimmaus on tapa maksukorttitietojen anastamiseen ja niiden käyttämiseen maksuvälinepetoksen toteuttamiseksi.

Tavoitteenani on opinnäytetyön kautta saavuttaa parempi ymmärrys skimmauksesta sekä maksuvälinerikollisuudesta, jotta voin tulevaisuudessa hyödyntää tietoa käytännön tehtävissä. Yleisesti opinnäytetyön tavoitteena on koota monipuolinen tietopaketti skimmauksesta siitä kiinnostuneille.

Pääasiallisena lähteenä opinnäytetyössä on käytetty verkkolähteitä. Skimmaus on harvinaisempaa Suomessa kuin esimerkiksi Yhdysvalloissa. Tästä syystä internetistä löytää ajankohtaisempaa tietoa kuin Suomesta saatavissa olevasta aineistosta. Näiden lisäksi työn lähteenä on käytetty kahta skimmaukseen perehtynyttä asiantuntijaa. Keskusrikospoliisin Kyberrikos- torjuntayksikössä työskentelevää rikosinsinööriä Juha Lampista ja Europolin Cyber Crime Centerissä (ECCC) Seconded National Expertin tehtävissä työskentelevää Tero Toivosta.

2. MAKSUKORTTIRIKOLLISUUS SUOMESSA

Nykyaikana yhä useammat ostokset maksetaan maksukorteilla. Käteisen rahan käyttö vähenee jatkuvasti ja myös internetiä käytetään kauppapaikkana yhä useammin erilaisten verkkokauppojen kasvattaessa suosiotaan. Luonnollisesti korttien käytön kasvaessa, kasvaa myös maksukortteihin kohdistuva rikollisuus. Rikollisten tavoitteena on saada itselleen kortilta löytyvät tiedot, joiden avulla he pääsevät käsiksi kortinhaltijan pankkitilillä oleviin varoihin. Tämä toiminta tunnetaan yleisesti termillä maksukorttirikollisuus.

2.1 Erilaisia tapoja korttitietojen anastamiseksi

Rikollisten motivaationa on raha. Maksukorteilla on suora yhteys rahaan. Siksi maksukorttirikollisuus on niin houkutteleva rikollisuuden laji rikollisten näkökulmasta. Maksukorttitietojen anastamiseen on monia tapoja. Tässä kappaleessa luetellaan niistä tyypillisimpiä.

Skimmaus

Skimmauksella tarkoitetaan maksukortin magneettiraidan kopioimista. Kopiointi tapahtuu tyypillisesti pankkiautomaattiin asennetulla laitteistolla. Kopioidun magneettiraidan ja urkitun PIN-koodin avulla rikolliset voivat nostaa rahaa ulkomailta, jossa pankkiautomaatti ei edellytä sirukorttia käteisen rahan nostamiseen. (Laurio 2009.)

Tietomurrot

Tietomurroilla tarkoitetaan sitä, että rikolliset käyttävät joko haittaohjelmia tai tunkeutuvat suoraan hakkeroimalla johonkin dataa sisältävään palvelimeen. Palvelimelta rikolliset etsivät maksuvälinerikosten toteuttamiseen soveltuvaa dataa. (Poliisi, Maksukorttirikollisuus on kasvava ilmiö. Luettu 5.2.2017.)

Haittaohjelmat

Haittaohjelmia ovat muun muassa virukset, madot, Troijan hevoset ja vakoiluohjelmat. Haittaohjelmien tarkoitus on aiheuttaa vahinkoa kohteeseen, johon ne on saatu asennettua. Esimerkiksi vakoiluohjelma voi kerätä henkilökohtaista tietoa käyttäjästä, kuten

pankkitietoja, joita voidaan käyttää myöhemmin rikollisessa tarkoituksessa. (Tietoturvapalvelu, Haittaohjelmat ja muut uhat. Luettu 12.3.2017.)

Tietojenkalastelu eli phishing

Phishingillä tarkoitetaan huijaamista varten lähetettyjä sähköpostiviestejä. Niillä pyritään yleisesti urkkimaan tietoja sähköpostin saajasta. Sähköpostit lähetetään yleensä jonkin luotettavan tahon nimissä, ja vastausta pyydetään joko sähköpostitse tai ohjaamalla vastaanottaja väärennetylle internet-sivustolle. Sivusto muistuttaa ulkoisesti jonkun luotettavan tahon sivustoa. Phishing-viestejä voidaan lähettää esimerkiksi pankkien nimissä, jolloin tarkoituksena on saada viestin vastaanottajan pankkitunnukset urkittua. (OP, Tunnusten kalastelu – Mitä on phishing eli tunnusten kalastelu. Luettu 20.03.2017.)

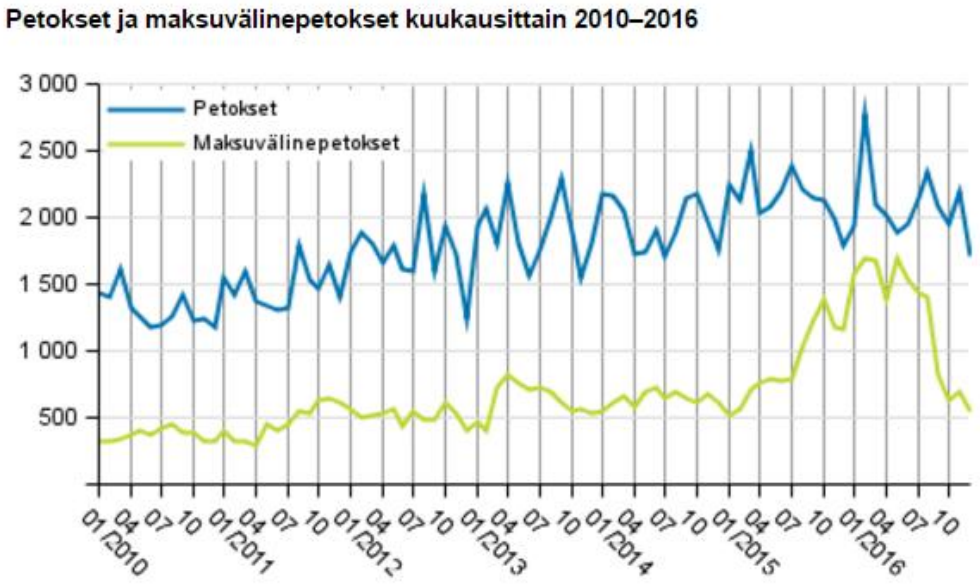
Korttivarkaudet

Saadakseen pankkitietoja haltuunsa rikolliset voivat myös yksinkertaisesti anastaa pankkikortin. Tällöin kuitenkin kortinhaltija todennäköisesti tietää joutuneensa rikoksen uhriksi ja osaa toimia niin, ettei hänen maksukorttiaan välttämättä ehditä käyttämään rikolliseen tarkoitukseen. Muissa edellä mainituissa tavoitteissa uhri harvoin tietää että hänen korttitietonsa on anastettu. Korttivarkauksia kohdistetaan esimerkiksi etenkin vanhuksiin ja yökerhoissa vahvasti päihtyneisiin asiakkaisiin. (Yle.fi, Poliisi varoittaa ulkomaalaisista rahansieppaajista – uhrina etenkin vanhukset. Luettu 20.03.2017)

2.2 Tilastoja maksukorttirikollisuudesta

Maksukorttirikollisuuden määrän on kasvanut voimakkaasti Suomessa lyhyessä ajassa. Tämä johtuu siitä, että erilaisten maksukorttien käyttö on kasvanut suhteessa käteisen rahan käyttöön. Rikolliset ovat rahan perässä, ja tekevät niitä rikoksia, joilla pääsee helposti rahaan kiinni. Tässä kappaleessa olevien tilastojen on tarkoitus hahmottaa kuvaa Suomessa tällä hetkellä esiintyvästä maksuvälinerikollisuuden määrästä. Koska kyseessä on poliisin tilasto, täytyy muistaa, että todellisten rikosten lukumäärä on todennäköisesti huomattavasti suurempi. Kaikki rikokset eivät tule poliisin tietoon, vaan jäävät niin sanotusti ”pimeiksi”.

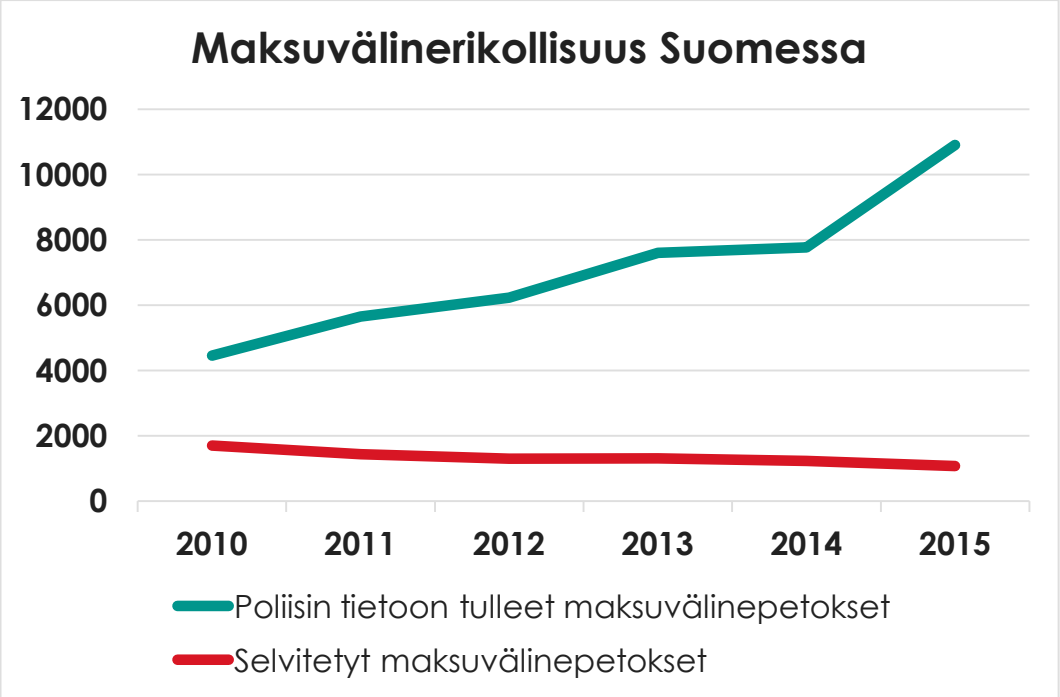
Kuviossa 1 kuvataan kuukausittain vuodesta 2010 lähtien petosrikollisuuden ja maksuvälinepetosten kehittymistä. Kuten kuviosta näkyy, on maksuvälinepetosten lukumäärä lähtenyt jyrkkään nousuun vuonna 2015.



Kuvio 1. Petosten ja maksuvälinepetosten kehittyminen kuukausittain 2010-2016 (Tilastokeskus, 2017).

Kuviossa 2 havainnollistetaan poliisin tietoon tulleiden maksuvälinerikosten määrää vuosittain. Samassa kuviossa näkyy myös selvitettyjen maksuvälinepetosten lukumäärä vuosittain suhteessa tietoon tulleisiin maksuvälinpetoksiin. Kuviosta käy ilmi, että maksuvälinepetosten määrän kasvaessa, on selvitettyjen rikosten lukumäärä laskenut samanaikaisesti. Taustalla tähän kehitykseen voisi olla se, että harva poliisi osaa esimerkiksi tutkia verkossa tapahtunutta maksuvälinepetosta. Lisäksi maksukorttirikolliset käyttävät hyväkseen kansallisen viranomaistoiminnan hitautta ja lainsäädäntöjen eroja. Maksukorttidata kiertää maapallon muutamassa sekunnissa, mutta jälkikäteen ilmitulleen rikoksen tutkinnassa kestää todella kauan. Tutkintaan tarvittavat tiedot kuuluvat yleensä pankkisalaisuuden piiriin ja niiden saaminen edellyttää vähintäänkin oikeusapupyynnön. (Poliisi, Maksukorttirikollisuus on kasvava ilmiö. Luettu 5.2.2017.)

Taulukossa oleviin lukuihin sisältyy lievien, perusmuotoisten ja törkeiden maksuvälinepetosten lisäksi maksuvälinepetoksen valmistelu.



Kuvio 2. Poliisin tietoon tulleet maksuvälinepetokset vs. selvitetyt maksuvälinepetokset 2010-2015 (Tilastokeskus, 2017).

3. MAKSUKORTIT

Skimmaus kohdistuu maksukortteihin. Tästä syystä on tärkeää tuntea erilaiset maksukorttityypit, maksukortin rakenne sekä maksukortin toiminta, jotta pystyy paremmin ymmärtämään myös skimmausta ja skimmauslaitteiden toimintaa.

Maksukortti on yleisnimitys erilaisille maksamiseen ja käteisen rahan nostamiseen tarkoitetuille korteille. Maksukortteja on monenlaisia ja valikoima vaihtuu pankeittain asiakkaiden toiveiden ja tarpeiden mukaisesti. Tässä luvussa käsitellään maksukortin rakennetta, erilaisia maksukorttityyppejä ja tarkastellaan niiden välisiä eroja. Lisäksi luvussa avataan maksukorttien toimintaperiaatetta.

3.1 Maksukortin rakenne

Nykyään melkein jokaiselta löytyy jonkinlainen maksukortti. Oli kortti miltä yritykseltä tahansa, on korteissa paljon samankaltaisuuksia. Tämä johtuu siitä, että kortit valmistetaan tietyn standardin mukaisesti. Kortin ulkoiset mitat ovat esimerkiksi löydettävissä ISO/IEC 7810 ID-1 -standardista. ”ISO” tulee sanoista International Organization for Standardization. Se kehittää ja ylläpitää kansainvälisesti sovittuja standardeja, joidenka mukaisesti standardeja koskevat asiat tehdään. Maksukortin ominaisuuksia sääteleviä standardeja löytyy edellä mainitun standardin lisäksi useita. Lähteenä on käytetty Ray, Daniel P. & Rodriguesz Juan 2014: Anatomy of credit card- julkaisua.

Kuvio 3. Visa- maksukortti (Visa).

Maksukorteista löytyy kuvion 3 mukaiset asiat:

1. **Koko**

   85.60 mm × 53.98 mm, paksuus 0,76 mm, pyöristetyt reunat.

2. **Materiaali**

   Maksukortit tehdään laminoimalla useita kerroksia muovia päällekkäin.

3. **Pankin logo**

   Erilaisia pankkeja ovat mm: Nordea, Osuuspankki jne…

4. **Kortin logo**

   Erilaisia luottokorttiyhtiöitä ovat mm: Visa, MasterCard, American Express jne…

5. **EMV-siru**

   Sirun nimi tulee sen kehittäneiden yritysten, Europay, MasterCard ja Visa nimistä. EMV:llä tarkoitetaan myös yleisesti standardia, joka määrittelee millainen siru ja siinä oleva tekniikka kortista löytyy. Sirua käytetään kortin varmennukseen.

   EMV-siru parantaa kortin turvallisuutta, ja se onkin kehitetty korttiväärennösten ja maksuvälinpetosten vaikeuttamiseksi. Sirun ansiosta jokainen maksutapaus on erilainen, eikä edellisistä maksutapauksista mahdollisesti kopioitua tietoa voi käyttää uudelleen petollisessa tarkoituksessa.

6. **Maksukortin numero**

Numeroiden määrä vaihtelee kortin mukaan. Visa- ja MasterCard- kortissa on 16 numeroa. American Express- kortissa 15. Numeroita voi olla maksimissaan 19. Numerosarja kertoo kortista muutamia asioita. Kortissa olevat numerot eivät ole sattumanvaraisia, vaikka ne siltä aluksi voivat vaikuttaa, vaan ne perustuvat Luhn-kaavaan. Nimi tulee kaavan keksijän, Hans Peter Luhnin mukaan.

Numerosarjan ensimmäistä numeroa kutsutaan termillä ”major industry identifier” (MII). Se kertoo kortin myöntäjästä. Esimerkiksi numero 1 on varattu lentoyhtiöille, numero 3 matkailu ja viihde- yrityksille ja numero 4 pankeille. Numerosarjan ensimmäistä kuutta numeroa (sisältää MII) kutsutaan termillä ”issuer identifier number” (IIN). Se kertoo, mikä yhtiö on myöntänyt kortin. Esimerkiksi hyvin tunnetuista kortin myöntäjistä Visan numerosarja on muotoa 4xxxxx ja American Expressin 34xxxx tai 37xxxx.

Seuraavaksi numerosarjasta löytyy tunnusnumero. Tunnusnumerossa olevien numeroiden lukumäärä riippuu kortissa olevan numerosarjan pituudesta. Siihen kuuluu MII:n ja IIN:n jälkeen kaikki loput numerot lukuun ottamatta viimeistä numeroa.

Viimeistä numeroa kutsutaan termillä ”check digit”, suomeksi tarkastusnumero. Tarkastusnumero muodostuu Luhn-kaavan mukaan. Numeron tarkoitus on varmistaa, että kortin numerosarja on todellinen. Tarkastusnumeron tarkoitus on lisäksi hankaloittaa maksukorttien numeroiden keksimistä, sillä vain yksi kymmenestä numerosta sopii Luhn-kaavaan.

7. Voimassaolo aika

Voimassaolo aika vaihtelee korteittain ja pankeittain. Ilmoitetaan yleisesti muodossa kk/vvvv.

8. Kortinhaltijan nimi

Kortinhaltijan nimi löytyy kortin edestä kohokirjaimin kirjoitettuna. Nimen täytyy vastata kortissa olevaa, kun korttia käytetään Internetissä ostamiseen.

9. Hologrammi

Hologrammi on turvaominaisuus, jota ei löydy kaikista korteista. Sen tehtävä on vaikeuttaa kortin väärentämistä.

10. Magneettijuova

Magneettijuova koostuu pienen pienistä magneettisista hiukkasista, joidenka avulla raitaan voi tallentaa tietoa. Tämä tieto välittyy laitteisiin, joilla pystyy lukemaan magneettijuovan. Magneettijuovaa käytettiin maksamiseen ennen EMV-sirua. Esimerkiksi Yhdysvalloissa magneettijuovaa käytetään edelleenkin.

11. Allekirjoitus

Joissain tapauksissa myyjä voi pyytää kortinhaltijan allekirjoitusta kaupan yhteydessä. Allekirjoituksen täytyy vastata kortin takana olevaa allekirjoitusta. Muussa tapauksessa on syytä epäillä, että korttia saatetaan käyttää petostarkoituksessa. Monissa korteissa onkin ehtona, että se on käyttökelpoinen vasta allekirjoitettuna.

12. Turvakoodi (CCV, CVV2, CVC2, CID)

Kortin takaa löytyvä kolme tai neljä numeroinen luku. Lukua kysytään usein esimerkiksi Internetissä ostoksia tehdessä. Luvun on tarkoitus ehkäistä petoksia, ja oletettavasti vain kortin haltija tietää tuon luvun.

13. Pankin yhteystiedot

Pankin postiosoite ja asiakaspalvelun puhelinnumero.

14. Kadonneen kortin löytäjälle

Kehotetaan löytäjää palauttamaan löytynyt kortti kortin myöntäneelle pankille ja muistutetaan väärinkäytön olevan rikos.

3.2 Maksukorttityypit

Maksukorttityyppejä on useita erilaisia. Kaikki niistä toimivat hieman eri lailla toisiinsa verrattuna ja kaikilla on oma käyttötarkoituksensa. Jokaiselle löytyy varmasti itselle sopiva kortti omien halujen ja tarpeiden mukaan.

Debit-kortti tunnetaan yleisesti myös nimillä pankkikortti tai käteiskortti. Debit- korttia voi

verrata käteiseen maksuvälineenä, sitä käyttämällä maksu veloitetaan kortinhaltijan tililtä parin päivän sisällä. Debit-kortilla ei siis saa ostoksille maksuaikaa eikä luottoa, vaan maksu veloitetaan käyttäjän tililtä olevista varoista. Tyypillisimpiä debit-kortteja ovat Visa Debit, Visa Electron sekä MasterCard Debit. (Financer.com, 2016.)

Credit-kortti, eli luottokortti on maksuväline, jonka käyttäjä saa ostoksia varten luottoa kortin myöntäneeltä pankilta. Credit-kortti toimii siis ikään kuin lainana ja sillä voi ostaa ostokset velaksi pankin lukuun. Ostokset kerryttävät kortin käyttäjän velkaa ja velka maksetaan takaisin yleensä kuukauden päästä. Useimmiten ostoksille saa noin 30 päivää korotonta maksuaikaa, tämän jälkeen ostoksista täytyy kuitenkin maksaa korkoa. Tyypillisimpiä luottokortteja ovat Visa Credit ja MasterCard Credit. (Financer.com, 2016.)

Yhdistelmäkortilla tarkoitetaan edeltävien korttien yhdistelmää. Se sisältää sekä credit- ja debit-korttien ominaisuudet. Yhdistelmäkortista käytetään myös nimeä Debit/Credit-kortti. Korttia käyttäessä saa valita, maksetaanko ostokset luotolla vai käytetäänkö käyttäjän tilillä olevia varoja. (Financer.com, 2016.)

Prepaid-kortilla tarkoitetaan korttia, jolle ladataan rahaa ennen kuin korttia voi käyttää. Konsepti on monille tuttu prepaid-kännykkäliittymistä. Kortilla maksaessa ei saa siis luottoa, eikä maksuja veloiteta tililtä, vaan kortille ladatuista varoista. (Financer.com, 2016.)

3.3 Maksuprosessi ja korttimaksamisen eri osapuolet

Maksuprosessi voi aluksi vaikuttaa hyvin yksinkertaiselta: asiakas laittaa kortin lukijaan, näppäilee tunnusluvun ja hetken päästä maksu on suoritettu. Jokaisen maksun takana on kuitenkin luultua monimutkaisempi prosessi. Kortin käyttäminen lukijassa ja kuitin saaminen ovat vain ensimmäinen ja viimeinen osa tätä prosessia. Vaikka prosessi kestää parhaillaan vain muutamia sekunteja, on prosessin takana useita eri vaiheita ja toimijoita.

Maksuprosessiin kuuluu yhteensä neljä eri osapuolta. Nämä ovat kortinhaltija (asiakas), kauppias, kauppiaan maksuja vastanottava pankki, eli acquirer sekä kortinhaltijan maksukortin myöntänyt pankki, eli issuer. Itse maksuprosessin taas voi jakaa kolmeen eri

vaiheeseen. Nämä kolme eri vaihetta ovat selitetty alhaalla auki, ja niitä myös kuvataan havainnollistavien kuvioiden (4, 5 ja 6) avulla.

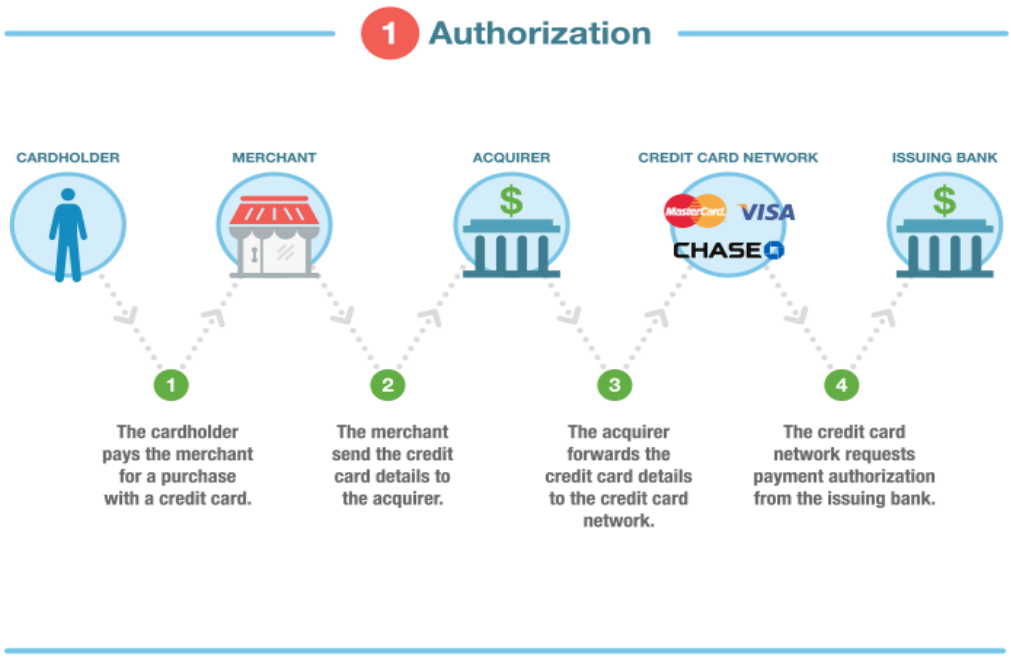
Auktorisointi

1. Kortinhaltija laittaa kortin lukijaan ja näppäilee tunnusluvun.

2. Kortin tiedot lähetetään Internetin välityksellä acquirerille.

3. Acquirer välittää kortin tiedot luottokorttiyhtiölle.

4. Luottokorttiyhtiö lähettää auktorisointi-pyynnön issuerille.



Kuvio 4. Auktorisointi (Papadimitriou 2009).

Autentikointi

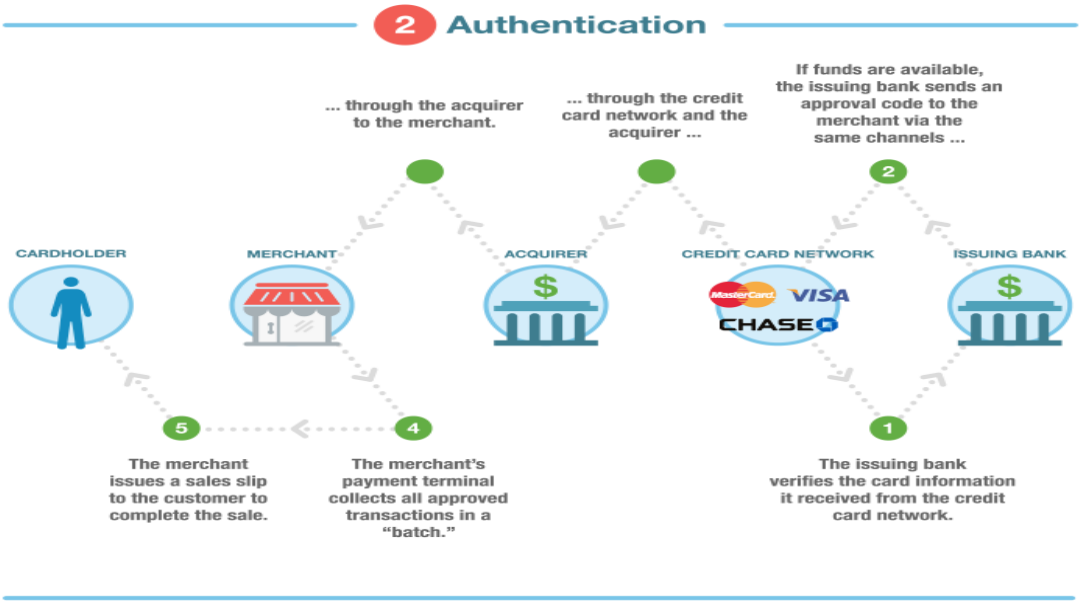
1. Issuer saa auktorisointi-pyynnön luottokorttiyhtiöltä.

2. Issuer varmistaa kortin numeron ja muut tiedot oikeellisiksi. Lisäksi se tarkastaa kortinhaltijan käytössä olevat varat.

3. Issuer joko hyväksyy tai hylkää pyynnön, ja lähettää vastauksen takaisin kauppiaalle samaa polkua pitkin, kuin mitä viesti issuerille päätyi.

4. Kauppias saa tiedon maksun hyväksymisestä ja issuer siirtää kortinhaltijan varoista maksun suuruisen summan syrjään.

5. Kauppias antaa asiakkaalle kuitin onnistuneen maksun merkiksi.



Kuvio 5. Autentikointi (Papadimitriou 2009).

Clearing & Settlement, eli viimeistely

1. Kauppapäivän lopuksi kauppias siirtää tiedon kaikista onnistuneista maksuista acquirerille.

2. Acquirer välittää tiedot luottokorttiyhtiöille.

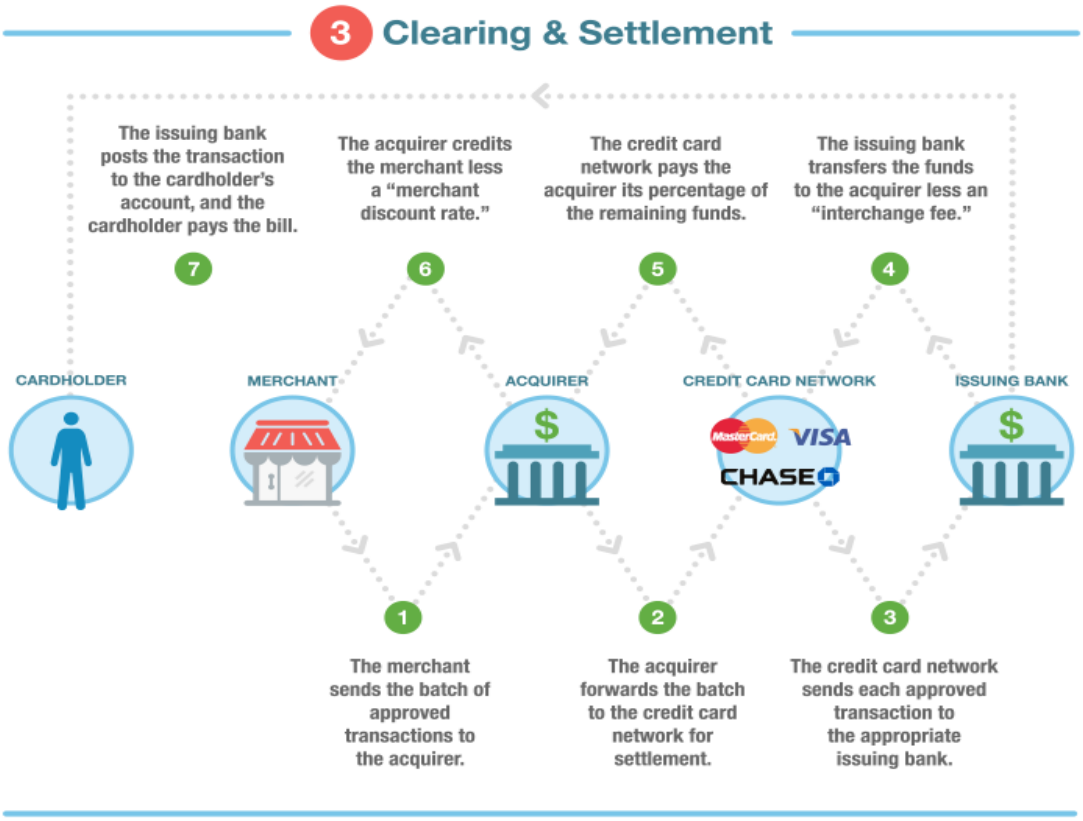
3. Luottokorttiyhtiöt välittävät tiedot kullekin eri issuerille.

4. Useimmiten noin 24-48 tunnin aikana issuer siirtää varat luottokorttiyhtiöille. Issuer ottaa summasta tietyn suuruisen palkkion.

5. Luottokorttiyhtiöt siirtävät maksun acquirerille. Luottokorttiyhtiöt ottavat summasta tietyn suuruisen palkkion.

6. Acquirer siirtää varat kauppiaan tilille. Acquirer ottaa tietyn suuruisen palkkion itselleen.

7. Rahan siirtyminen näkyy kortinhaltijan tilillä.



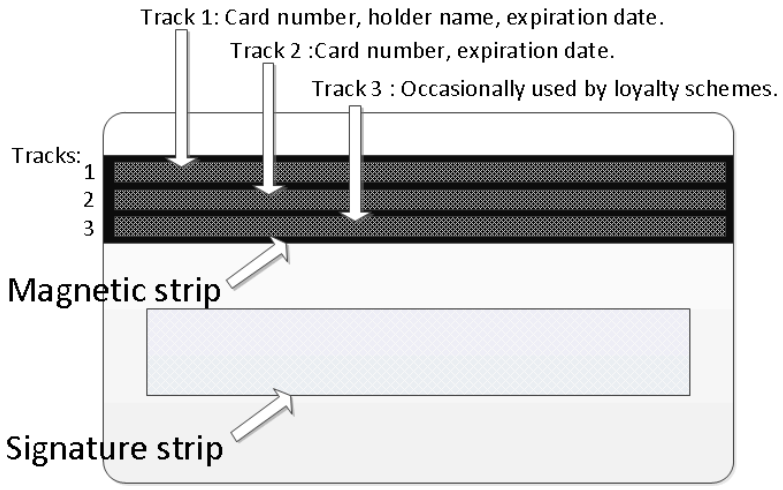
Kuvio 6. Viimeistely (Papadimitriou 2009).

3.4 Lisätietoa magneettijuovasta ja EMV-sirusta

Magneettijuova

Magneettijuovan toiminta perustuu siihen, että juovasta löytyy pienen pieniä magneettisia hiukkasia, jotka voidaan magnetisoida joka pohjoiseen tai etelään päin. Tämän tekniikan ansiosta magneettijuovaan voi tallentaa tietoa. Tieto ”kirjoitetaan” juovaan siihen suunnitellulla laitteella. Magneettijuova on jaettu kolmeen eri osaan, joita kutsutaan ”track”- nimityksellä. Suomeksi voidaan käyttää termiä raita.

- Track 1 sisältää korttinumeron, voimassaoloajan ja kortinhaltijan nimen
- Track 2 sisältää korttinumeron ja voimassaoloajan
- Track 3 ei yleensä käytetä



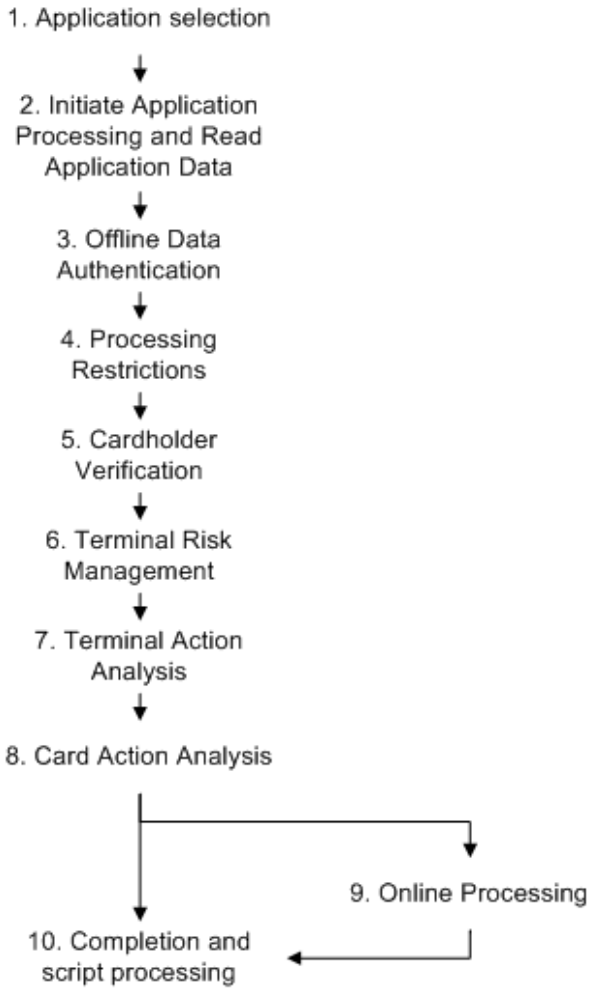
Kuvio 7. Magneettijuovan trackit (Gundert 2014).

Maksukortin magneettijuovaa käytettäessä maksupääte lukee yleensä jommankumman raidan kahdesta ensimmäisestä, tai molemmat, jos jostain syystä maksupääte ei saa luettua toista raitaa kunnolla. Tämän vuoksi molemmista raidoista löytyy tarvittavat tiedot maksuprosessin onnistumisen kannalta. Magneettijuova on jo vanhaa tekniikkaa, eikä siinä ole merkittävää suojausta, jonka vuoksi se on varsin helppo kopioida. Tämän heikkouden korjaamiseksi on kehitetty uusi turvallisempi tapa käyttää korttia EMV- sirun avulla. (Gundert 2014.)

EMV- siru

EMV- siru on kehitetty korttimaksamisen turvallisuuden kehittämiseksi. Sen nimi tulee sen kehittäneiden yhtiöiden, Europayn, MasterCardin ja Visan mukaan. EMV-sirukorttistandardia ylläpitää ja kehittää EMVco. Standardi määrittelee muun muassa kortin mekaanisia ja sähköisiä ominaisuuksia, kortin ja terminaalin välistä tietoliikennettä, kortissa käytettäviä salausmenetelmiä sekä kortilla toimivia sovelluksia. EMV standardi mahdollistaa myös Near Field Communication (NFC) siirtotekniikan. Tekniikan avulla korttia voi käyttää langattomasti lähimaksamiseen, jos kortista edellä mainittu ominaisuus löytyy.

EMV- kortilla tapahtuva maksutapahtuma etenee kuvion 8 mukaisesti:



Kuvio 8: EMV- maksutapahtuman vaiheet (EMVco, 2014).

1. Valitaan sovellus. Debit / Credit.

2. Sovelluksen valinnan jälkeen terminaali lukee kortilla olevan datan.

3. Siirretään kortilta terminaaliin transaktion vaativat tunnistetiedot.

4. Suoritetaan erilaisia tarkastuksia, jotta kortilla voidaan tehdä kyseinen maksutapahtuma, eli transaktio.

5. Kortinhaltija varmennetaan jollain menetelmällä. Suomessa yleisin varmennus menetelmä on PIN-koodi.

6. Terminaali tekee erilaisia tarkastuksia ja tekee päätöksen tarvitaanko online varmennusta.

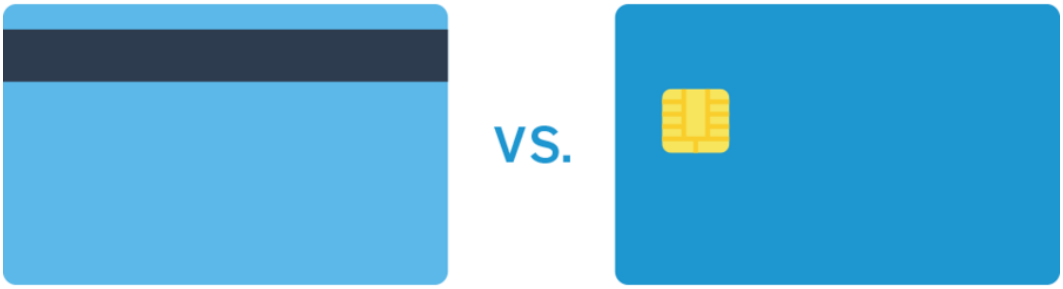
7. Edellisten tarkastuksen perusteella tehdään joko offline päätös transaktion hyväksymisestä tai hylkäämisestä, tai siirrytään online tilaan.

8. Kortin liikkeellelaskijan säätämien asetusten perusteella tehdään päätös transaktion hyväksymisestä tai hylkäämisestä tai online tilaan siirtymisestä.

9. Siiryttiin online prosessointiin. Kortti ja transaktio varmennetaan online tilassa.

10. Transaktion lopetus. Transaktio on joko hyväksytty/hylätty.

Miksi EMV- tekniikka on turvallisempi kuin magneettijuova?



Kuvio 9. Magneettijuova vs EMV-siru (Squareup, 2016).

1. Magneettijuova on todella vanhaa tekniikkaa. Se on otettu käyttöön jo 1960- luvulla. EMV- siru on paljon uudempi ja on suunniteltu turvallisuus mielessäpitäen. Sen tarkoitus on vähentää korttien väärinkäyttöä.

2. Magneettijuovassa oleva data on vakioitu. Se ei vaihdu mitenkään, vaan transaktioon tarvittava data pysyy samana. EMV- korttia käytettäessä transaktion aikana käytettävä data vaihtelee. Se ei ole koskaan samanlainen. Yhdestä transaktiosta kopioitua dataa ei voi käyttää myöhemmin petostarkoituksessa.

3. Magneettijuovallisen kortin terminaaliin lähettämä data ei ole suojattua. Terminaali salaa datan heti kun se vastaanottaa sen. EMV- sirullisen kortin ja terminaalin välinen datanvaihto on salattua alusta loppuun.

4. PANKKIAUTOMAATIT

Maksukorteilla on mahdollista nostaa käteistä rahaa pankkiautomaateista. Suomessa suurinta osaa pankkiautomaateista ylläpitää Automatia pankkiautomaatit Oy. Erilaisia Otto-automaatteja löytyy Suomesta Automatian kotisivujen mukaan yli 1500. Tässä luvussa käsitellään tarkemmin pankkiautomaatteja ja niiden toimintaa.

4.1 Pankkiautomaatin rakenne ja toiminta

Pankkiautomaatteja löytyy useita toisistaan eroavia malleja, mutta jokainen niistä toimii samalla periaatteella. Ulkoiset seikat voivat hieman erota toisistaan, mutta pääpiirteittäin niistä kaikista on löydettävissä samat asiat. Alla oleva kuva 1 on otettu Suomessa yleisesti käytössä olevasta pankkiautomaatista.

Kuva 1. Otto- automaatti (Kunelius 2017).

Ulkoisesti pankkiautomaatti näyttää käyttäjälle kuvan 1 mukaiselta. Siitä löytyy:

1. Monitori

Monitori kertoo, mitä sinun täytyy tehdä käyttääksesi laitetta

2. Valintanäppäimet

Valintanäppäimistä valitaan monitorin esittämistä vaihtoehdoista haluttu toiminto.

3. Numeronäppäimistö

Numeronäppäimistön avulla näppäillään PIN-koodi kortin syötön jälkeen laitteen käyttämiseksi.

4. Sirukortinlukija

Sirukortti syötetään tähän aukkoon. Kortti ei mene kokonaan sisään, vaan jää aina hieman ulos.

5. Magneettijuovanlukija

Käytettiin kortin magneettijuovan lukemiseen, kun korteissa ei ollut vielä sirua. Nykyään ei hyväksy sirukortteja, vaan ne on syötettävä sirukortinlukijaan.

6. Kuittitulostin

Tulostaa halutessa kuitin tapahtuman loputtua.

7. Aukko, josta setelit tulevat ulos

Setelit tulevat täältä ulos noston onnistuttua. Aukossa on ”elektroninen silmä”, joka laskee setelit.

8. Kaiutin

Mahdollistaa automaatin käyttöön liittyvät äänet.

9. Kamera

Kuvaa jokaisen automaattia käyttävän henkilön. Toisinaan poliisi voi tarvita näitä kuvia rikoksen selvittämiseksi.

Lisäksi joistain Otto-automaatti malleista löytyy mahdollisuus tallettaa käteistä. Silloin niistä löytyy luukku, johon talletettavat setelit ja kolikot laitetaan.

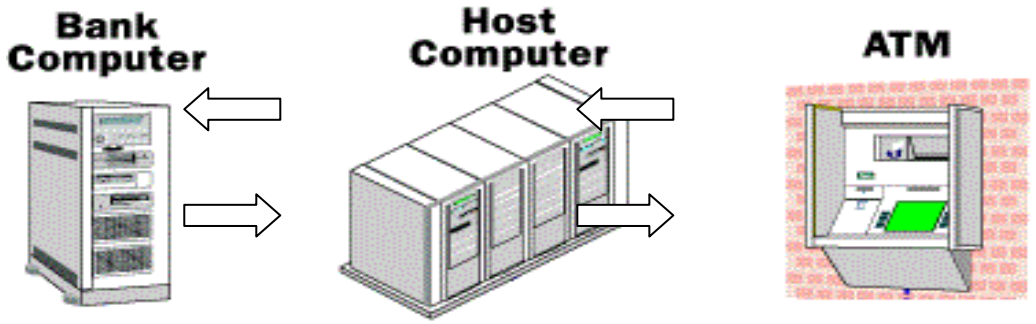
Toiminta

Nostettaessa käteistä automaatista, kortti syötetään lukijaan, näppäillään tunnusluku, seurataan ruudulta löytyviä ohjeita ja hetken kuluttua poistutaan paikalta haluttu määrä käteistä taskussa. Rahan nostaminen vaikuttaa yksinkertaiselta prosessilta, joka kestää vain hetken. Oletko kuitenkaan tullut ajatelleeksi, miten automaatti saa tietonsa siitä, paljonko

rahaa sinulla on tililläsi ja nostoon tarvittavista muista tiedoista?

Otto-automaatti on terminaali, joka on yhdistetty tietokoneeseen. Tämä tietokone toimii normaalilla Windowsin käyttöjärjestelmällä ja on yhteydessä automaatin ylläpitäjän järjestelmään. Järjestelmä ottaa yhteyttä kortinhaltijan pankkiin ja ilmoittaa kortinhaltijan haluavan nostaa tietyn summan käteistä. Kortinhaltijan pankki tarkistaa, että tilillä on tarpeeksi katetta ja lähettää tarvittavan summan automaatin ylläpitäjän tilille. Kun tuo siirto on tapahtunut, antaa automaatti vastaavan summan käteistä kortinhaltijalle. Prosessi on valmis, eikä se vienyt kuin muutaman sekunnin. (Bowen 2000.)

Kuvio 10 havainnollistaa edellä selittyä prosessia.



Kuvio 10. Pankkiautomaatin toiminta (Seksaria 2000).

5. SKIMMAUS

”Poliisi varoittaa skimmauslaitteesta bensa-asemalla Salossa” on uutisoitu mtv.fi-verkkosivustolla 26.2.2017. Uutisessa kerrotaan poliisipartion löytäneen Salossa sijaitsevan kylmäaseman maksuautomaatista kortinkopiointilaitteen, eli niin sanotun skimmauslaitteen.

Useille termi ”skimmaus” on entuudestaan tuttu. Henkilö on saattanut kuulla siitä uutisissa, lehdessä, internetissä tai hänellä saattaa olla omakohtaista kokemusta asiasta esimerkiksi lähipiirin kautta. Yleinen tietoperusta skimmauksesta rajoittuu kuitenkin vain kopiointilaitteeseen pankkiautomaatilla tai kylmäasemalla ja anastettujen varojen myöhempään käyttöön ulkomailla. Tässä luvussa kerrotaan yleisesti skimmauksesta, tarkastellaan skimmauksen tilannetta Suomessa ja esitellään erilaisia skimmauslaitteita ja niiden toimintaa.

Skimmaus- sana tulee englannin kielisestä sanasta ”skimming” ja sillä tarkoitetaan pinnalla liukumista. Termi tulee siitä, että rikolliset asentavat maksu- tai pankkiautomaattiin laitteen, joka liukulukijalla lukee maksukortin magneettijuovan. Kyseessä olevaa laitetta kutsutaan skimmauslaitteeksi, tai lyhyemmin skimmeriksi. (Toivonen 2017.)

Nykyaikaisista maksukorteista löytyy kaksi eri teknistä sovellusta, jotka välittävät maksutapahtumaan tarvittavaa dataa, joka yksilöi kortin. Rikolliset siis pyrkivät skimmauksella kopioimaan toisen näistä sovelluksista, eli maksukortin magneettijuovan, ja tavalla tai toisella urkkimaan kyseessä olevan kortin PIN-koodin. Magneettijuovan ja korttiin kuuluvan PIN-koodin avulla rikolliset voivat nostaa rahaa jossain päin maailmaa. (Toivonen 2017.)

Korttiautomaattien skimmauksessa on kyse siitä, että tekijät ovat tarkoin suunnitelleet toteutettavan rikoksen jo etukäteen. Kohdeautomaatti on tutkittu tarkkaan, ja rikolliset ovat tehneet juuri kohteena olevaan automaattiin sopivan sähköteknisen laitteen, joka asennetaan automaatissa olevien alkuperäisten komponenttien päälle manipuloimatta niitä. Automaattiin asennetun laitteen tehtävä on kopioida siinä käytettävän maksukortin tiedot ja PIN-koodi sisältämälleen muistikortille. Myöhemmin rikolliset hakevat nämä tallennetut

tiedot itselleen, ja tekevät niiden avulla korttikopioita, joilla sitten tekevät käteisnostoja ulkomailla. (Poliisi, Maksukorttirikollisuus on kasvava ilmiö. Luettu 5.2.2017.)

Skimmaus on täysin ammattimaista ja järjestäytynyttä rikollisuutta ja tästä järjestäytyneestä rikollisorganisaatiosta löytyy jokaiseen eri tehtävään omat tekijänsä. On olemassa toiminnan rahoittajat, johtajat, jotka johtavat koko toimintaa, rekrytoijat, jotka etsivät sopivia henkilöitä mukaan joukkoon ja tiedustelijat, jotka etsivät ja ”scouttaavat” kohteet etukäteen. Tiedustelijat lähettävät automaattien tiedot eteenpäin henkilöille, jotka valmistamat automaatteihin sopivat skimmauslaitteet. Valmiit skimmauslaitteet toimitetaan henkilöille, jotka asentavat ne automaatteihin, ja hakevat ne tietyn ajan kuluttua pois. Skimmauslaitteisiin tallentuneet tiedot välitetään nopeasti eteenpäin henkilöille, jotka tekevät näiden tietojen avulla korttikopiota ja nostavat kopioiden avulla rahaa automaateista ulkomailla. Näin jouhevasti toimii skimmausorganisaatio. Henkilöt jotka jäävät kiinni ovat lähinnä niitä jotka tulevat maahan asentamaan laitteet automaatteihin. (Toivonen 2017.)

Skimmaus toiminnan luonteeseen on otettu mallia yritystoiminnan piiristä ja riskien hajauttaminen kuuluu osaksi myös rikollismaailmaa. Kun korttidatan väärinkäyttäjä on eri henkilö kuin korttidatan kaappaaja, ja datan väärinkäyttö tapahtuu eri maassa, vältetään turhat riskit ja pyritään hankaloittamaan poliisin työtä rikoksen torjumiseksi. (Poliisi, Maksukorttirikollisuus on kasvava ilmiö. Luettu 5.2.2017.)

Datan väärinkäyttö ulkomailla ei pelkästään johdu riskien välttelystä. Todellisuudessa se johtuu EU:n alueella käytössä olevasta turvallisesta EMV- sirutekniikasta ja käteisautomaateista, jotka ovat yhteensopivia niiden kanssa. Uudet automaatit ja EMV-sirulla varustetut kortit ovat teknisesti erittäin turvallisia, mutta EU:n ulkopuolella on vieläkin käytössä automaatteja, jotka mahdollistavat rahan noston pelkän magneettijuovan avulla. Tästä syystä etenkin Yhdysvallat on rikollisten suosiossa korttiväärennöksen käytössä. (Poliisi, Maksukorttirikollisuus on kasvava ilmiö. Luettu 5.2.2017.)

Jotkin rikolliset tekevät voittoa myymällä skimmauslaitteita. Laitteita myydään pimeän verkon sivuilla eri kauppapaikoilla ja ostajia ohjeistetaan laitteiden käytössä. Laitteiden tekijät myös julkaisevat videoita esimerkiksi youtube- verkkosivustolle

havainnollistaakseen skimmauslaitteiden käyttöä. (Krebs 2016.)

5.1 Skimmaus Suomessa

Skimmaus ei ole uusi asia Suomessa. Sitä on esiintynyt vaihtelevissa määrin vuosien saatossa ja poliisin järjestelmistä löytyy tietoa skimmaustapauksista jo vuodelta 2008. Tässä kappaleessa tarkastellaan skimmausta ja esiintymistä Suomessa tilastojen avulla vuosina 2011-2016.

Suomessa tapahtuva maksukorttien skimmauksen määrä vaihtelee paljon. Toisinaan sitä esiintyy kausiluonteisesti vuodenaikojen mukaan, toisinaan ei ollenkaan ja toisinaan tasaisesti läpi vuoden. Suomessa tuohon vaihteluun vaikuttavat esimerkiksi vuodenajat. Talvella voi olla paljonkin pakkasta ja skimmauslaitteissa olevat akut eivät kestä tarpeeksi kauan pakkasella. (Lampinen 2017.) Skimmauksen vaihteleva määrä selittyy myös osittain skimmausrikollisuuden luonteen avulla. Toimintaa tehdään siellä, missä päästään rahoihin käsiksi kaikista varmimmin ja helpoimmin. Esimerkiksi aikanaan Saksassa oli noin 3000 skimmaustapausta vuodessa. Kun Saksassa otettiin käyttöön mahdollisuus korttien geoblokkaukseen, jolla tarkoitetaan kortin käyttämisen rajausta jollekin tietylle maantieteelliselle alueelle, väheni skimmaus noin puoleen entisestä. Samalla Sveitsissä, missä tuolloin ei esiintynyt skimmausta juuri lainkaan, skimmauksen määrä kasvoi rajusti. Oli siis havaittavissa, että rikollisuus siirtyi Saksasta muualle. Rikollisuuden siirtymisestä käytetään niin sanottua fraud migration- termiä. Termillä kuvataan myös yleisesti korttien väärinkäytön siirtymistä Euroopan Unionin alueelta Yhdysvaltoihin. (Toivonen 2017.)

Kuviossa 11 on havainnollistettu poliisin tietojärjestelmästä, Rikitripistä, haettua tietoa suomalaisiin kohdistuneesta skimmauksesta. Hakusanana on käytetty ”skimmaus or skimmausta or skimmeri or skimmauslaite” ja rikosnimikkeistö on rajoitettu maksuvälinepetoksen eri muotoihin.

Kuvio 11. Epäillyt skimmaustapaukset 2011-2016 (Rikitrip, 2017).

Kuvio 11 on vain suuntaa antava, sillä siitä ei voi päätellä skimmaus- rikosten todellista määrää Suomessa. Tämä johtuu siitä, että yleensä maksuvälinepetoksen kirjaamiseksi mahdolliseksi skimmaukseksi riittää, kun rikosilmoituksen tekijä näin poliisille kertoo. Todellisuudessa tilastosta varmasti löytyy myös rikoksia, joissa kortinhaltijan korttitiedot ovat päätyneet rikollisille jollain muulla tavoin kuin skimmauksella. He ovat vain kuulleet skimmauksesta ja olettavat, että kun tililtä on hävinnyt rahaa, on kysymys automaattisesti siitä. Luonnollisesti sama logiikka toimii myös toisin päin. Mistä voidaan tietää, ettei korttitietojen joutuminen rikollisille johdu skimmauksesta? Täysin varmoja ei voida myöskään olla siitä, onko mahdollinen skimmaus tapahtunut Suomessa tai mahdollisesti ulkomailla. Lisäksi poliisin tietoon ei luonnollisesti tule kaikki rikollisuus, vaan osa siitä jää niin sanotusti pimeäksi. Yleisesti voidaan todeta, että Suomessa esiintyvä skimmaus on varmasti vähäisempää, kuin taulukossa näkyvät luvut. Huolimatta näistä seikoista, taulukko antaa viitteitä skimmaustilanteen kehityksestä ja muutoksista viime vuosina.

Kuviossa 11 on nähtävissä selkeä lasku vuosina 2013 ja 2014. Yksi syy tähän on se, että 2012 vuonna Automatia korvasi Otto-automaatin vanhan kortinlukijan uuteen. Uudessa

kortinlukijassa maksukortti ei mennyt kokonaan lukijan sisään, vaan jäi selvästi näkyviin. Kopioinnin onnistumiseksi täytyy kortti saada koko matkalta lukijan sisään. Uudistus vähensi skimmauksen mielekkyyttä Suomessa. (Lappeenrannan Uutiset, Otto-automaatit uusitaan. Luettu 5.3.2017.)

Skimmauksen massiivinen kasvu vuonna 2015 selittyy rajusti nousseen maksuvälinerikollisuuden vuoksi. Ilmiö voi selittyä osin sillä, että usein rahan hävitessä tililtä, se ilmoitetaan poliisille epäiltynä skimmauksena. Ei ole epäilystäkään, etteikö skimmauksen määrä olisi kasvanut vuonna 2015 vuoteen 2014 verrattuna, mutta todellinen nousu ei varmasti ole noin suuri, kuin taulukko antaa ymmärtää.

Kuvion 11 avulla voidaan todeta, että skimmaus on Suomessa harvinainen rikos. Paljon todennäköisempää onkin, että maksukortti häviää tai se varastetaan, kuin että joutuisi skimmauksen uhriksi Suomessa. (Poliisi, Maksukorttirikollisuus on kasvava ilmiö. Luettu 5.2.2017). Skimmauksen mielekkyyttä Suomessa heikentää se, että skimmauksen voidaan sanoa olevan hallinnassa. Poliisi, öljy-yhtiöt ja pankit tekevät saumatonta yhteistyötä rikollisuuden kitkemiseksi. Kun kylmäasemalta löytyy skimmauslaite, ilmoitetaan siitä välittömästi pankkiin, jossa tarkastetaan, mitä kortteja automaatilla on lähiaikoina käytetty. Nämä kortit suljetaan tarvittaessa, jottei vahinkoa pääse syntymään. Skimmauksessa rikokselle altistuneet kortit ovat lukumäärältään vähäisiä, joten näin voidaan toimia. Esimerkiksi tietomurroissa, joissa kohteena voi olla kymmeniä tuhansia kortteja, on kynnys korttien sulkemiseen paljon suurempi. Lisäksi Suomen poliisi tekee hyvää työtä skimmaustapausten selvittämiseksi. Poliisilla on käytössä hyvät pakkokeinot ja valtuuden tapausten tutkimiseksi. Selvitysprosentit ovat korkeita ja rikolliset saadaan useimmiten kiinni. (Toivonen 2017.)

5.2 Skimmaus muualla

European ATM Security Team (EAST) julkaisee vuosittain useita raportteja maksuvälinerikollisuuden sen hetkisestä tilasta. Viime vuonna on julkaistu raportti

kokonaisuudessaan vuodesta 2015. Raportista selviää, että skimmaustapauksia raportoitiin tuona vuonna 4131 kappaletta. Tulos oli laskenut 27% viime vuoden raportoiduista 5631 skimmaustapauksesta.

Automaatteihin kohdistuneesta petosrikollisuudesta (sisältää myös muut automaattiin kohdistuneen rikoksen tekotavat kuin skimmauksen) aiheutuneet kustannukset olivat kasvaneet vuoden 2014 summasta 280 milj.€ summaan 327 milj. €. Suurin vaikutus tähän nousuun oli 15% nousu skimmauksen aiheuttamista tappioista kansainvälisellä tasolla. Nousu oli 238 milj.€ → 274 milj.€. Suurin osa näistä tappiosta kertyi Yhdysvalloista ja Aasiasta. Euroopan sisäiset skimmauksesta aiheutuneet tappiot kasvoivat 37 milj.€ → 44 milj.€ eli yhteensä 19%. Kehitys on huolettava, ja EAST tekeekin yhteistyötä Europolin kanssa kasvattaakseen tietoa asiantuntijoiden keskuudessa tästä rikollisuudesta Amerikassa. (European ATM Security Team - Card skimming losses continue to rise outside Europe. Luettu 7.3.2017)

5.3 Skimmauksen torjuminen ja tappioiden korvaaminen

Vaikka kortinhaltija olisi kuinka huolellinen korttinsa käyttämisessä, silti voi joutua skimmauksen uhriksi. Jotkin skimmauslaitteet ovat niin kehittyneitä, ettei korttia käytettäessä ole mahdollisuutta skimmauslaitteen havaitsemiseen. Onneksi kortinhaltijan huolellisuus ei ole ainoa tapa, jolla ehkäistään skimmausta.

Pankilta löytyy omat järjestelmänsä pankkikortin väärinkäytön ehkäisemiseksi. Järjestelmän on tarkoitus hälyttää, mikäli se havaitsee epäilyttäviä korttitapahtumia tililläsi. Esimerkki epäilyttävästä tapahtumasta olisi se, jos käytät korttiasi Suomessa ja vähän ajan päästä sitä käytetäänkin toisella puolella maailmaa. Tällaisessa tapauksessa pankki sulkee kortin ja ilmoittaa mahdollisesta väärinkäytöstä kortinhaltijalle.

Pankki- ja maksuautomaateilla torjutaan myös skimmausta erilaisin tavoin. Pankkiautomaatteja suunnitellaan ja päivitetään siten, että skimmauksesta tehdään

mahdollisimman vaikeaa. Lisäksi pankkiautomaateista löytyy kamera, jota tarkkailemalla näkyy jos joku yrittää vaikuttaa sen toimintaan. Joistain automaateista löytyy myös hälytin, joka hälyttää jos automaattia yrittää avata. Öljy-yhtiöt yrittävät panostaa skimmauksen torjuntaan tarkastamalla automaattien toiminnan ja kunnon säännöllisin väliajoin. Kylmäasemilta löytyy myös kamerat, jotka valvovat, ettei automaateille tehdä mitään epäilyttävää.

Maksukorttirikollisuuden määrä ja muodot sopeutuvat kuitenkin nopeasti uusien tietoturvallisuusstandardien luomiin olosuhteisiin. Skimmaajalla voi olla käytössään aivan uudenlainen laite, josta ei vielä tiedetä mitään. Rikollisten kehittäessä koko ajan uusia menetelmiä petosten toteuttamiseksi, on turvallisuusmenettelyn syytä kehittyä ja pysyä vauhdissa mukana. (Toivonen 2017.)

Edellä mainituista turvallisuus menettelyistä huolimatta, tärkeäksi pointiksi nousee kortinhaltijan huolellisuus. Kaikista tehokkaimmin petoksen uhriksi joutumisen voi välttää olemalla itse huolellinen ja varovainen maksukortin käytössä. Tehokkain tapa skimmauksen ehkäisemiseksi onkin peittää kädelläsi näppäimistö samalla kun näppäilet tunnuslukusi. Lisäksi on syytä kiinnittää huomiota itse automaattiin. Näyttääkö automaatti jotenkin epäilyttävältä, onko jokin osa uudemman näköinen toiseen verrattuna tai toimiiko automaatti jotenkin poikkeuksellisesti? Jos pienikin epäilys herää, voi soittaa automaatista löytyvään päivystysnumeroon. Ei haittaa, vaikka kyseessä olisikin väärä hälytys. Aina kannattaa ennemmin katsoa kuin katua. (Korttiturvallisuus.fi.)

Joskus kaikesta huolimatta saattaa käydä vahinko ja rikokset onnistuvat saamaan korttitiedot itselleen. Tässä tapauksessa ei kannata kuitenkaan panikoida, vaan ottaa yhteyttä omaan pankkiinsa ja kertoa heille tilanteesta. Pankki kyllä selvittää asian ja korvaa skimmauksesta aiheutuneet tappiot.

5.4 Skimmauslaitteet ja niiden toiminta

Skimmauslaitteita löytyy useita erilaisia. Maailmassa on paljon eri mallisia pankki- ja maksuautomaatteja ja rikolliset suunnittelevat skimmereitä jotka sopivat milloin mihinkin malliin, johon skimmeri on tarkoitus asentaa. Skimmauslaitteiden suunnittelijat tekevät laitteet alusta loppuun ja toimittavat laitteet henkilöille, jotka asentavat ne automaatteihin. Skimmereitä voidaan tehdä esimerkiksi 3D- tulostimen avulla. Skimmauslaitteiden suunnittelu ja valmistus on ammattimaista rikollista toimintaa Itä- ja Kaakkois-Euroopassa. (Lampinen 2017.)

European ATM Security Team (EAST) on tehnyt listan, missä eri skimmeri tyypit lajitellaan sen perusteella, mihin ne kiinnittyvät pankki- tai maksuautomaateissa. Lista on englannin kielellä, mutta suomennan tässä siinä olevat pääkohdat.

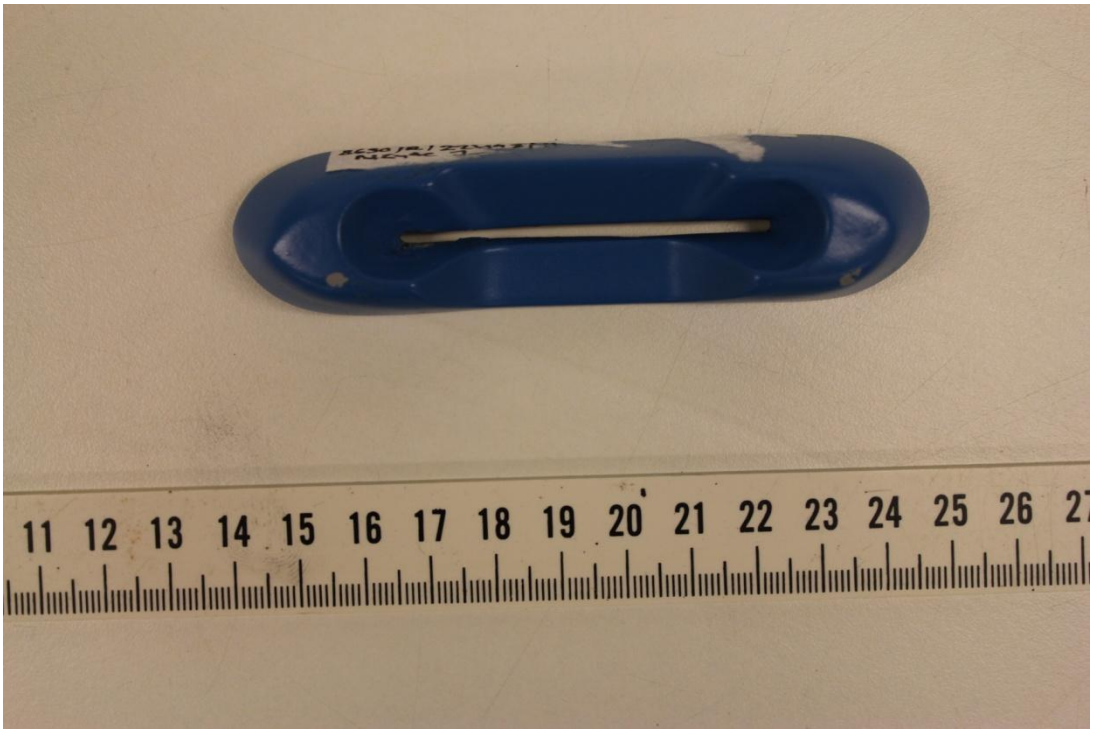
M- kirjaimella tarkoitetaan moottoroitua kortinlukijaa. Käyttäjä laittaa kortin aukolle, ja lukija imaisee kortin sisäänsä.
D- kirjaimeilla tarkoitetaan lukijaa, missä kortti työnnetään lukijan sisään. Kortti ei mene kokonaan laitteen sisään, vaan sen saa itse otettua pois.
E- kirjaimella tarkoitetaan laitetta, joka kytketään kortinlukijan omaan lukijaan tai sen osaan. Laite ikään kuin ”vakoilee” tietoa joka kulkee kortin ja lukijan välillä.
S- kirjaimella tarkoitetaan laitetta, joka asennetaan lukijan sisään.
M ja **D** kirjaimissa luvulla **1** tarkoitetaan alkuperäisen lukijan päälle tulevaa skimmauslaitetta. **E** kirjaimen osalta luvulla **1** tarkoitetaan laitetta, joka sijaitsee ennen moottoroidun kortinlukijan varsinaista lukupäätä.
M ja **D** kirjaimissa luvulla **2** tarkoitetaan skimmauslaitetta, joka tulee lukijan sisälle. **E** kirjaimen osalta luvulla **2** tarkoitetaan laitetta, joka sijaitsee kortinlukija lukupäässä.
M ja **D** kirjaimissa luvulla **3** tarkoitetaan skimmauslaitetta, joka asennetaan syvälle lukijan sisälle. Skimmauslaitetta ei ole mahdollista havaita laitetta käyttäessä. **E** kirjaimen osalta luvulla **3** tarkoitetaan skimmauslaitetta, joka asennetaan lukijan piirilevyyn.
E- kirjaimessa luvulla **4** tarkoitetaan laitetta, joka asennetaan lukijassa olevaan liittimeen.

Type of Device	Description
M1. Overlay Skimming Device	The read head on this type of overlay device is external to the fascia and the motorised card reader throat (entrance) or covers the whole of the motorised card reader entrance.
M2. Throat Inlay Skimming Device	The read head on this type of device is placed inside the throat of the ATM or inside the legitimate bezel and in every case in front of the card reader shutter.
M3. Card Reader Internal Skimming Device	The read head on this type of device is placed at various locations inside the motorised card reader behind the shutter. This type of device is also sometimes referred to as a “deep insert” skimming device.
D1. Overlay Skimming Device	The read head on this type of overlay device is external to the fascia and the DIP card reader throat (entrance) or covers the whole of the dip card reader entrance.
D2. Throat Inlay Skimming Device	The read head on this type of device is placed inside the DIP card reader throat in front of the card reader read head
D3. Card Reader Internal Skimming Device	The read head on this type of device is placed inside the DIP card reader throat behind the card reader read head
E1. Pre-read Head Eavesdropping Device:	This type of device is connected to the pre-read head of a motorised card reader.
E2. Read Head Eavesdropping Device.	This type of device is connected to the read head of the card reader.
E3. PCB Eavesdropping Device	This type of device is attached to the PCB of the card reader.
E4. Communication Eavesdropping Device:	This type of device is connected to the communication interface (e.g. USB interface) of the card reader.
S1. Card Reader Internal Shimming Device	This type of device is placed inside the card reader

Kuvio 12: Skimmauslaitteiden luokittelu tyypeittäin: (EAST, 2017).

Vaikka skimmauslaitteiden mallit eroavat toisistaan, toimivat ne kaikki kuitenkin hyvin pitkälti samalla periaatteella. Kuten mikä tahansa elektroninen laite, tarvitsee skimmauslaite virtaa toimiakseen. Tästä syystä skimmauslaite toimii akun varassa. Akun lisäksi laitteesta löytyy elektroniikka, joka ohjaa skimmerin toimintaa. Skimmereistä löytyy myös muistipaikka, johon skimmerin lukemat tiedot tallentuvat. Muistipaikan asemassa voi toimia esimerkiksi normaali pienikokoinen muistikortti. Näiden lisäksi laitteesta löytyy itse lukija, joka lukee kortin magneettiraidan. Magneettiraidan tietojen lisäksi rikolliset tarvitsevat maksukortin PIN-koodin. PIN-koodi urkitaan kameran avulla. Kamera voi kuulua itse skimmauslaitteeseen, tai sitten se voi olla erikseen asennettuna eri kohtaan automaattia. Kameran sijasta PIN-koodin urkkimiseen voidaan käyttää automaatin oikean näppäimistön päälle asennettavaa valenäppäimistöä. (Lampinen 2017.)

Seuraavaksi esitellään kuvien avulla erilaisia Suomesta löytyneitä skimmauslaitteita:



Kuva 2. D1- luokan skimmauslaite (Kunelius 2017).

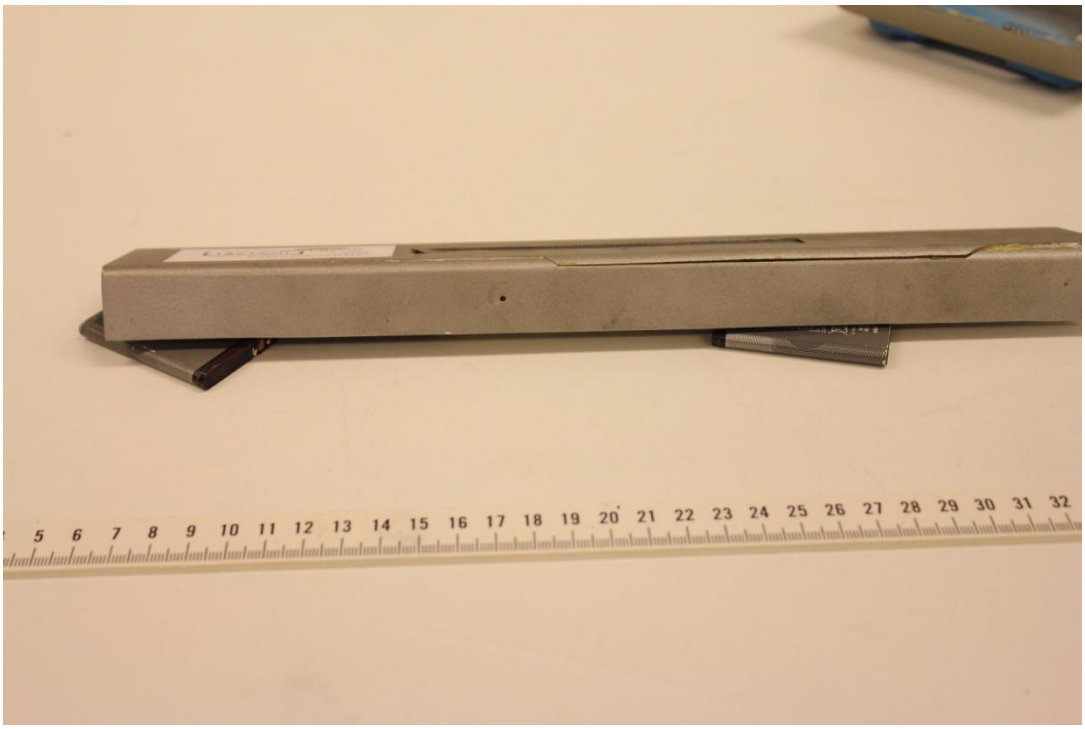
Kuvassa 2 oleva skimmauslaite on suunniteltu vastaamaan vanhan Otto- automaatin sinistä kortinlukijaa. Skimmeri on liimattu automaatin oman lukijan päälle.

Kuva 3. D1- luokan skimmauslaite 2 (Kunelius 2017).

Kuvassa 3 on hieman aikaisempaa isompi paneeli, joka on tarkoitus asentaa Otto-automaatin oman lukijan päälle. Tästä skimmauslaitteesta löytyy myös kamera, joka sijaitsee paneelin vasemmassa alareunassa.

Kuva 4. Erillinen kamerapaneeli (Kunelius 2017).

Kuvassa 4 on kamerapaneeli, joka sijaitsee sellaisessa paikassa, josta paneelissa oleva kamera onnistuu urkkimaan käyttäjän PIN-koodin. Löydätkö sinä kameran tästä paneelista?



Kuva 5. Kamerapaneeli (Kunelius 2017).

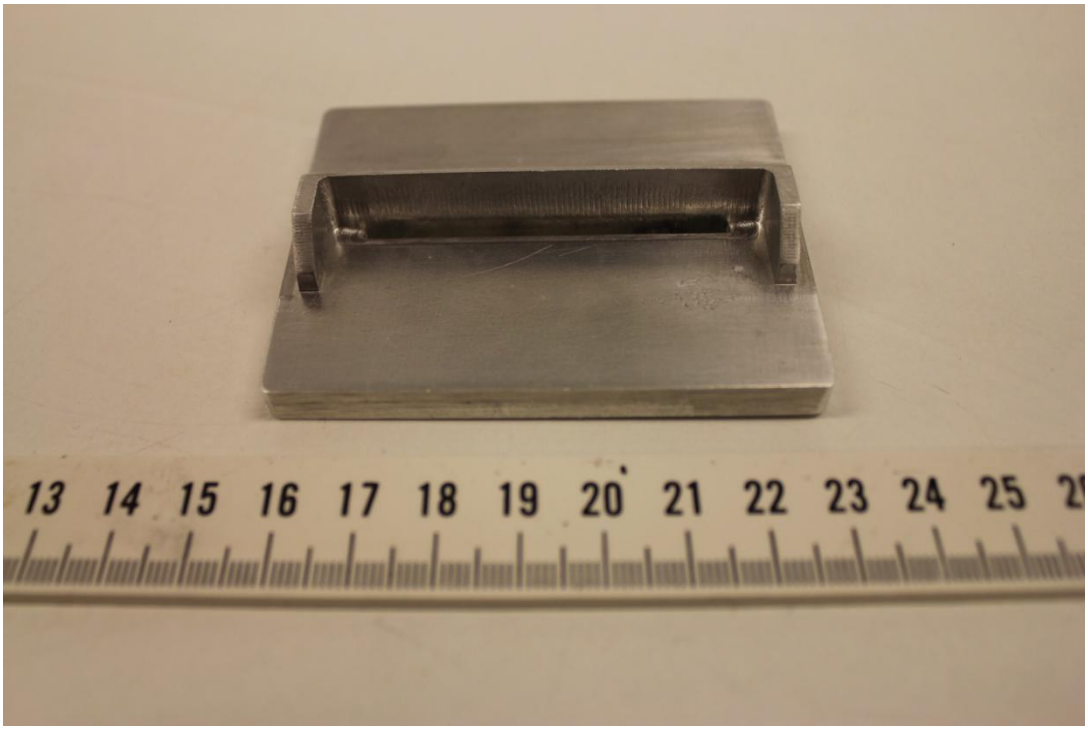
Kuvassa 5 on tarkempi kuva äskeisestä paneelista. Kamera löytyy paneelin alaosasta.

Kuva 6. Valenäppäimistö (Kunelius 2017).

Kuvassa 6 on valenäppäimistö, joka sijoitetaan varsinaisen näppäimistön päälle. Se tallentaa käyttäjän näppäilemän PIN-koodin muistiin.

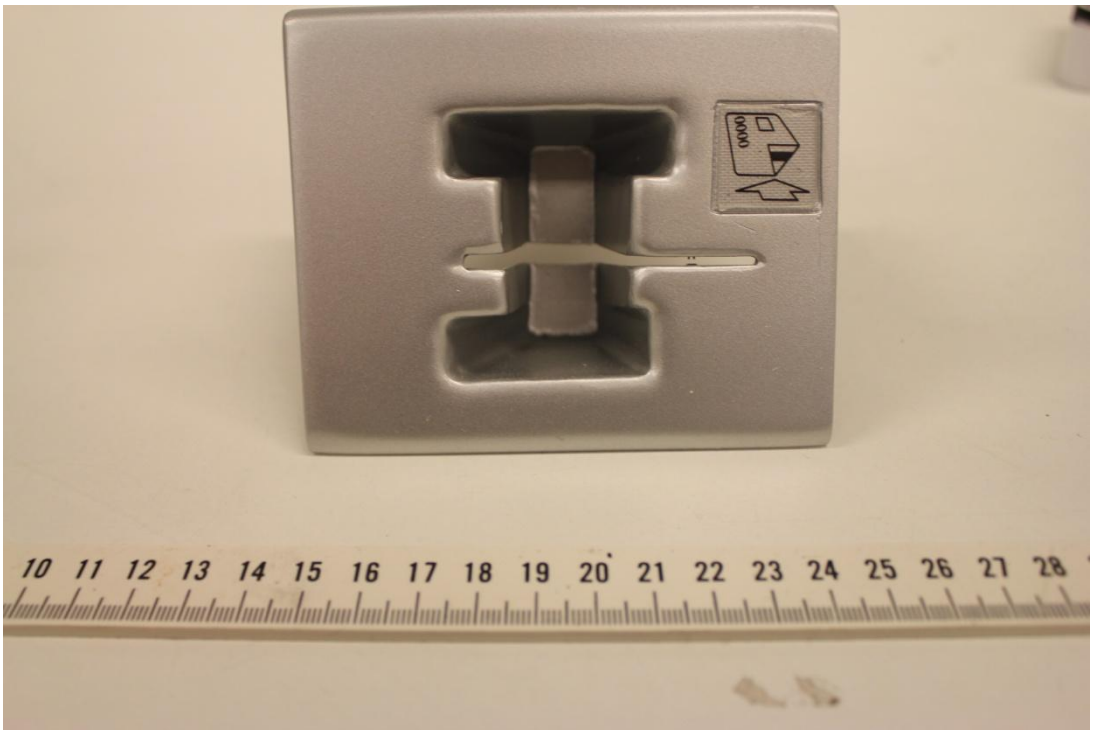
Kuva 7. Oven avaaja skimmauslaite (Kunelius 2017).

Kuvassa 7 on hieman tavallisesta poikkeava skimmauslaite. Aiemmin pankkien sisälle pääsi automaatille maksamaan laskuja. Sisälle päästäkseen piti käyttää korttia oven avaamiseksi. Tämä skimmeri oli sijoitettuna oven avaamiseen tarkoitettuun lukijaan.



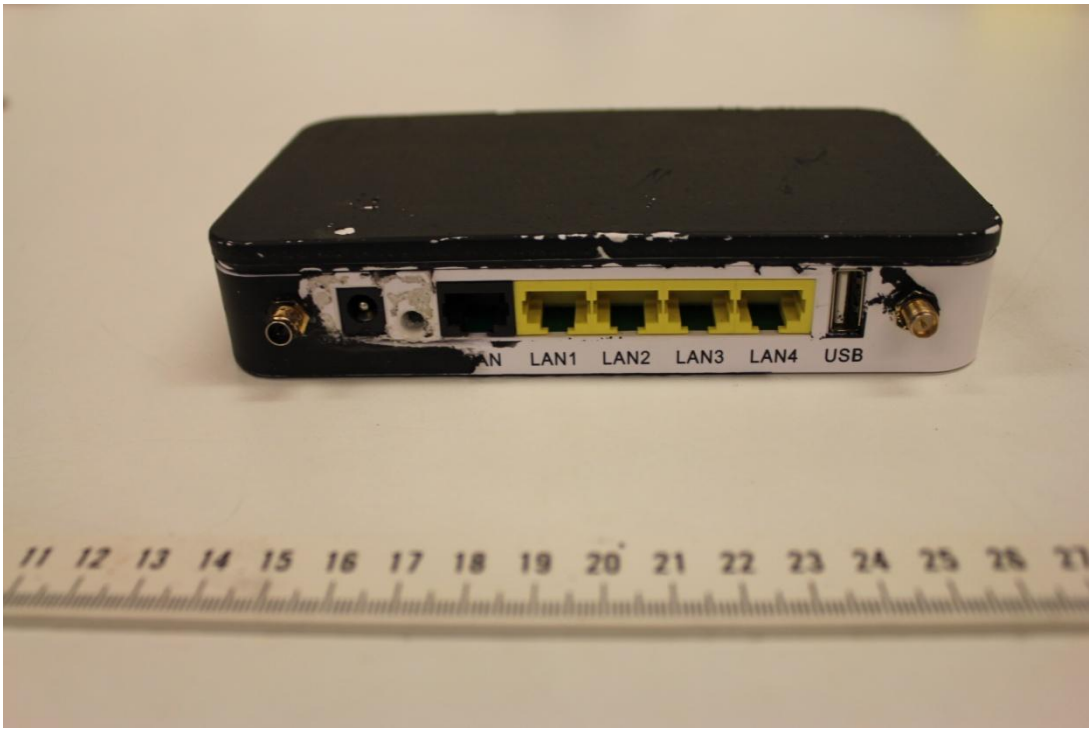
Kuva 8. M1-luokan skimmauslaite (Kunelius 2017).

Kuvassa 8 on laite, joka asennetaan kylmäasemilla käytössä olevan maksuautomaatin kortinlukijan päälle.



Kuva 9. Salosta löytynyt skimmauslaite (Kunelius 2017).

Kuvassa 9 on Salosta 2017 löytynyt skimmauslaite. Laite oli asennettu kylmäaseman maksuautomaattiin. Korttiaukon oikeassa reunassa nähtävissä magneettijuovan lukija. Tästä skimmeristä löytyy myös kamera, joka sijaitsee laitteen oikean puoleisella sivulla.



Kuva 10. Modeemi skimmauslaite (Kunelius 2017).

Kuvasta 10 löytyy hyvin poikkeuksellinen skimmauslaite Suomessa. Laite oli asennettu maksupäätteen ja tietoliikennettä välittävän verkkokytkimen väliin. Laite luki dataa, jota liikkui maksukortin ja maksupäätteen välillä. Asiakkaalle ei ole mahdollisuutta havaita tällaista laitetta.

6. LAINSÄÄDÄNTÖ

Rikoksista ja niistä seuraavista rangaistuksista säädetään Suomen rikoslaissa. Suomessa tehtyihin rikoksiin sovelletaan Suomen rikoslakia, mutta sitä sovelletaan myös ulkomailla tapahtuneisiin rikoksiin, jotka ovat kohdistuneet Suomen kansalaiseen, suomalaiseen yhteisöön, säätiöön tai muuhun oikeushenkilöön taikka Suomessa pysyvästi asuvaan ulkomaalaiseen. Lisäehtona tähän on, että teosta saattaa seurata yli kuuden kuukauden vankeusrangaistus.

Maksukorttirikokset ovat kriminalisoitu rikoslain 37. luvussa. Rikosnimikkeitä ovat:

1. maksuvälinepetos
2. lievä maksuvälinepetos
3. törkeä maksuvälinepetos
4. maksuvälinepetoksen valmistelu.

Skimmaus voi täyttää minkä tahansa yllä mainitun rikoksen tunnusmerkistön. Hyvin paljon riippuu siitä, missä vaiheessa rikolliset jäävät kiinni. Jos skimmaaja jää kiinni, ennen kuin hän, tai joku muu jolle tiedot on lähetetty, on ehtinyt väärinkäyttää skimmauksella saatua maksukortti dataa, syyllistyy hän maksuvälinepetoksen valmisteluun. Jos taas tietoja on ehditty käyttää väärin, tulee pääsääntöisesti kyseeseen perusmuotoinen maksuvälinepetos tai törkeä maksuvälinepetos.

Perusmuotoisen maksuvälinepetoksen tunnusmerkistö täyttyy, jos rikollinen käyttää toisen laillisesti hallinnoimaa maksuvälinettä ilman kyseisen maksuvälineen haltijan lupaa. Rikollinen syyllistyy maksuvälinepetokseen myös, jos hän luovuttaa maksuvälineen tai siihen liittyviä tietoja muille hankkiakseen itselle tai toiselle oikeudetonta hyötyä. Maksuvälinepetoksesta voidaan tuomita sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Lievä maksuvälinepetos eroaa perusmuotoisen rikoksen tunnusmerkistöstä siten, kokonaisuutena arvostellen tavoiteltu hyöty, tai aiheutetun vahingon määrä on vähäinen. Vähäisenä summana pidetään usein alle 500€, kuten omaisuusrikoksissa yleisesti on

tapana. Lievästä maksuvälinepetoksesta voidaan määrätä sakkorangaistus.

Törkeän maksuvälinepetoksen tunnusmerkistössä taas edellytetään, että rikoksella aiheutetaan huomattavaa vahinkoa, rikos tehdään erityisen suunnitelmallisesti ja teko on myös kokonaisuutena arvostellen törkeä. Huomattavan vahingon rajana on yleisesti pidetty tuhansia euroja. Törkeän maksuvälinepetoksen tekijä on määrättävä vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi vankeuteen.

Myös maksuvälinepetoksen valmistelu on kriminalisoitu. Maksuvälinepetoksen valmisteluun syyllistyy, jos hankkii tietoonsa maksuvälinekorttien tietoja, muttei ole vielä ehtinyt väärinkäyttää niitä. Lisäksi valmisteluksi lasketaan, jos tekijä hankkii, vastaanottaa, valmistaa tai pitää hallussaan maksuvälinelomakkeita tai laitteita, joilla voi niitä valmistaa. Maksuvälinepetoksen valmistelusta tuomitaan sakkoa tai vankeutta enintään yhdeksi vuodeksi.

Yllä mainittujen rikosnimikkeiden lisäksi maksuväline rikollisuuteen liittyy hyvin yleisesti myös rahanpesu ja kätkemisrikokset. Niihin liittyvät rikosnimikkeet löytyvät rikoslain 32. luvusta.

6.1 Skimmauksen tutkiminen

Poliisin tehtävät määritellään poliisilain (PolL) ensimmäisessä luvussa. Niihin kuuluu oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen. Lisäksi poliisin tehtäviä ovat rikosten ennalta estäminen, paljastaminen, selvittäminen ja niiden syyteharkintaan saattaminen. Tämän säädöksen vuoksi poliisin tehtävä on selvittää skimmausrikollisuutta siinä missä kaikkea muutakin rikollisuutta.

Esitutkintalain (ETL) perusteella poliisin on toimitettava esitutkinta, kun sille tehdyn ilmoituksen perusteella tai muuten on syytä epäillä, että on tehty rikos. Esitutkinnassa taas on selvitettävä epäilty rikos, sen teko-olosuhteet, aiheutettu vahinko, saatu hyöty sekä rikoksen asianosaiset. Skimmaus ei eroa millään tavalla muista rikoksista, vaan näiden säännösten perusteella poliisi tutkii skimmaustapausta, kuin mitä tahansa muutakin rikosta.

Skimmaus- rikoksen tutkimisessa poliisin käyttöön tulee pakkokeinolain (PKL) mukaiset pakkokeinot, kunhan niille asetetut edellytykset täyttyvät. Skimmaustapausten tutkinnassa merkittävimpiä pakkokeinoja ovat laite-etsintä, takavarikko, paikanetsintä ja kotietsintä. Lisäksi törkeämpien rikosten tutkinnassa mahdollistuu salaisten pakkokeinojen, kuten telekuuntelun käyttö.

Koska maksukorttirikollisuus on monimuotoinen, kasvava ja yleensä rajat ylittävä rikollisuuden ala, jossa tietoverkkoa hyödynnetään tehokkaasti, tulee kysymykseen virka-avun pyyntö toisen valtion viranomaisilta. Virka-avun saaminen ja -antaminen on tärkeää maksuvälinerikosten ratkaisemiseksi, sillä kyseessä on hyvin usein rajat ylittävää rikollisuutta, ja vain yhteistyötä tekemällä on mahdollista tehdä rikollisten toiminnasta hankalampaa.

7. POHDINTAA

Opinnäytetyöprosessin aikana sain mahdollisuuden perehtyä hyvin rajattuun rikollisuuden lajiin, skimmaukseen. Skimmauksen kokonaisvaltainen ymmärtäminen ja sen hahmottaminen osaksi suurempaa kokonaisuutta vaatii useiden seikkojen ymmärtämistä. Ilmiön lisäksi koin mielenkiintoiseksi juuri yksityiskohtiin, kuten maksukortin rakenteeseen perehtymisen.

Opinnäytetyötäni varten luin useita artikkeleita ja uutisia liittyen skimmaukseen. Lisäksi etsin tutkimuksia Rikitripistä ja haastattelin kahta aiheeseen perehtynyttä asiantuntijaa. Mielestäni oli yllättävää huomata, kuinka vähän aiheeseen perehtyneitä poliiseja lopulta Suomessa on. Toisaalta tulos oli ennustettavissa jo omien harjoittelussa saamieni kokemusten pohjalta. Skimmaukseen liittyvien tilastojen löytämisen havaitsin todella haastavaksi. Myös artikkeleja hakiessani huomasin skimmauksesta saatavan tiedon erot suomenkielisissä ja englanninkielisissä lähteissä. Englanniksi tietoa oli saatavilla huomattavasti enemmän, mikä osaltaan edesauttoi skimmauksen kansainvälisen tilan hahmottamista.

Opinnäytetyöprosessin aikana koin erityisen mielenkiintoiseksi vierailun keskusrikospoliisin kyberrikosyksikköön. Olin aiemmin kuvitellut skimmauslaitteiden kanssa työskentelevät ammattilaiset koulutetuiksi poliiseiksi, jotka vain ovat erikoistuneet tekniikkaan. Todellisuudessa ammattilaiset olivat kuitenkin rikosinsinöörejä. Heitä haastattelemalla sain hyvin kattavan kuvan skimmauslaitteiden toiminnasta ja laitteiden konkreettinen näkeminen auttoi omalla kohdalla hahmottamaan kokonaiskuvaa. Poliisin näkökulmaa skimmaukseen ja erityisesti kansainväliseen tilanteeseen sekä Suomen tilanteeseen sain Europolissa työskentelevältä Tero Toivoselta.

Skimmaustapausten määrä ja niiden suhde yhteiskunnassa tapahtuneisiin muutoksiin, kuten maksukorttiautomaattien uusimiseen, antoi aihetta myös uusille töille tästä aiheesta. Tulevaisuudessa maksaminen erilaisilla välineillä, kuten matkapuhelimella tai sovelluksien kautta, yleistyy. Maksuvälineiden muuttuessa myös maksukorttirikollisuuden on muututtava ja pysyttävä mukana kehityksessä. Skimmauksen kohdalla tämä tarkoittaa

myös muutoksia konkreettisten maksuautomattikäyntien mahdollisesti vähentyessä. Mielestäni sopivia opinnäytetyön aiheita aiheeseen liittyen ovatkin skimmauksen muuttuminen ja kehittyminen maksamisen muuttuessa. Kansainvälisellä tasolla Yhdysvalloissa ollaan kovaa vauhtia siirtymässä EMV- siru tekniikan käyttöön. Tälläkin on varmasti vaikutuksia skimmaukseen. Jännä nähdä, miten se heijastuu skimmaukseen.

Lopuksi lainaan vielä Toivosen kommenttia, kun keskustelimme skimmausrikollisuuden mahdollisesta häviämisestä. ”Skimmaus on sellainen rikollisuuden laji, joka osattaisiin varmasti estää kokonaan, jos se vain haluttaisiin estää. Tämä vain vaatisi suuria muutoksia ja panostusta nykyään käytössä oleviin järjestelmiin. Korttimaailma on tasapainoilua turvallisuuden ja käytettävyyden välillä. Jos toista lisätään, laskee toinen samalla”. (Toivonen 2017.)

Jostain vain on löydettävä ”kultainen keskitie”, jossa kortin käytettävyys on hyvällä tasolla ja olemassa olevat riskit ovat tiedostettava ja hyväksyttävä.

8. LÄHTEET

Verkkolähteet

Automatia: Turvallista tekniikkaa
Luettavissa: https://otto.fi/otto/nain-ottopiste-toimii/ Luettu: 30.1.2017

Bowen, Jim 2000: How ATMs work?
Luettavissa: http://money.howstuffworks.com/personal-finance/banking/atm.htm Luettu: 2.3.2017

EAST 2016: Card skimming losses continue to rise outside Europe
Luettavissa: https://www.european-atm-security.eu/card-skimming-losses-continue-rise-outside-europe/ Luettu:14.2.2017

EAST 2016: Terminology for locations of CDC Devices at ATMs
Luettavissa: https://www.european-atm-security.eu/industry-information/terminology-locations-cdc-devices-atms/ Luettu: 14.2.2017

EMVco: A Guide to EMV Chip Technology
Luettavissa: http://www.emvco.com/best_practices.aspx?id=217 Luettu: 17.2.2017

Financer: Kortteja on erilaisia – mikä niistä on paras?
Luettavissa: https://financer.com/fi/luottokortti/maksukorttityypit/ Luettu: 20.2.2017

Finanssivalvonta: Maksukortinkäyttö vaatii huolellisuutta:
Luettavissa:
http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Finanssialan_palveluita/Maksupalvelut/Maksuvalineet/Maksukortit/Pages/Default.aspx Luettu: 12.3.2017

Korttiturvallisuus: Automaatilla
Luettavissa: https://www.korttiturvallisuus.fi/Automaatilla/ Luettu: 15.3.2017

Gundert, Levi 2014: Detecting Payment Card Data Breaches Today to Avoid Becoming

Tomorrow’s Headline
Luettavissa: https://blogs.cisco.com/security/detecting-payment-card-data-breaches-today-to-avoid-becoming-tomorrows-headline Luettu: 5.3.2017

Krebs, Brian 2016: ATM Insert Skimmers In Action
Luettavissa: http://krebsonsecurity.com/2016/06/atm-insert-skimmers-in-action/ Luettu: 20.2.2017

Lappeenrannan uutiset, 2012: Otto-automaatit uusitaan
Luettavissa: http://www.lappeenrannanuutiset.fi/artikkeli/94089-otto-automaatit-uusitaan Luettu: 5.3.2017

Laurio, Juha-Matti 2009: Sisälle PCI-terminologian saloihin –Mitä onkaan skimmaus?
Luettavissa: https://www.nixu.com/fi/blogi/2009-11/sis%C3%A4lle-pci-terminologian-saloihin-%E2%80%93-mit%C3%A4-onkaan-skimmaus Luettu: 25.2.2017

MTV: Poliisi varoittaa skimmauslaitteesta bensa-asemalla Salossa
Luettavissa: http://www.mtv.fi/uutiset/rikos/artikkeli/poliisi-varoittaa-skimmauslaitteesta-bensa-asemalla-salossa/6325880 Luettu: 1.3.2017

Nykänen, Helmi 2017: Poliisi varoittaa ulkomaalaisista rahansieppaajista – uhrina etenkin vanhukset
Luettavissa: http://yle.fi/uutiset/3-9425624 Luettu: 20.3.2017

OP: Tunnusten kalastelu - Mitä on phishing eli tunnusten kalastelu?
Luettavissa: https://www.op.fi/op/usein-kysyttya/usein-kysyttya/tietoturva?cid=151724922&_pageLabel=page_ap_sisaltoalue&srcpl=3 Luettu: 20.3.2017

Papadimitriou, Odysseas 2009: How Credit Card Transaction Processing Works: Steps, Fees & Participants
Luettavissa: https://wallethub.com/edu/credit-card-transaction/25511/ Luettu: 10.2.2017

Poliisi: Maksukorttirikollisuus on kasvava rikosilmiö:
Luettavissa: https://www.poliisi.fi/rikokset/rikosilmioita/maksukorttirikollisuus Luettu: 5.2.2017

Ray, Daniel P. & Rodriguesz Juan 2014: Anatomy of credit card
Luettavissa: http://www.creditcards.com/credit-card-news/anatomy-of-a-credit_card-1267.php Luettu: 20.2.2017

Seksaria, Kalpit 2016: How do ATM machines work internally?
Luettavissa: https://www.quora.com/How-do-ATM-machines-work-internally Luettu: 23.2.2017

Squareup: Chip Card Security: Why Is EMV More Secure?
Luettavissa: https://squareup.com/townsquare/why-are-chip-cards-more-secure-than-magnetic-stripe-cards Luettu:7.3.2017

Tietoturvapalvelu: Haittaohjelmat ja muut uhat
Luettavissa: http://www.tietoturvapalvelu.info/johdanto/haittaohjelmat_ja_muut_uhat Luettu: 12.3.2017

Järjestelmät ja rekisterit:

Poliisin tietojärjestelmä RikiTrip, sisäinen lähde.

Suomen virallinen tilasto (SVT) 2017: Rikos- ja pakkokeinotilasto

Henkilölähteet:

Lampinen, Juha 2017: Rikosinsinööri, Keskusrikospoliisi
Haastattelu: 28.2.2017

Toivonen, Tero 2017: Seconded National Expert, Europol Cyber Crime Center
Puhelin haastattelu 2.3.2017