Otto Laitinen

KYBERTOIMINTAYMPÄRISTÖN HIERARKKISEN RAKENNEMALLIN HYÖDYNTÄMINEN ÄLYPUHELIMISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Laitinen, Otto
Kybertoimintaympäristön hierarkkisen rakennemallin hyödyntäminen älypuhelimissa.
Jyväskylä: Jyväskylän yliopisto, 2023, 69 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Älypuhelimien käyttäjämäärä on kasvanut huomattavasti viimeisimpien vuosien aikana ja suurin osa ihmisistä ympäri maailmaa omistaa älypuhelimen jossakin vaiheessa elämäänsä. Älypuhelimien suosion kasvu on tuonut mukanaan alalle huomattavan määrän rikollisuutta ja valtiollista hyväksikäyttöä. Tässä pro gradu -tutkielmassa tutkittiin kybertoimintaympäristön hierarkkista rakennemallia viitekehyksenä hyödyntäen mallin eri kerroksissa esiintyviä kyberuhkia.

Kybertoimintaympäristön hierarkkista rakennemallia muotoiltiin tutkimusta varten niin, että sitä pystyttiin käyttämään älypuhelimien kontekstissa. Tutkielman teoriaosassa selvisi, että älypuhelimiin kohdistuvien kyberuhkien määrä on huomattavassa nousussa. Älypuhelimiin kohdistuvien hyökkäysvektorien määrä ja laatu vastaavat tänä päivänä jo tietokoneisiin suunnattuja hyökkäysvektoreita.

Ennusteet älypuhelimien tulevasta kehittymisestä osoittavat myös sen, että kybertoimintaympäristöön on ennustettavissa tulevan uusia, vieläkin suurempia uhkia älypuhelimille ja älypuhelimien käyttäjille. Tutkielman empiirinen osa suoritettiin laadullisena sisällönanalyysinä ja aineisto kerättiin puolistrukturoiduilla haastatteluilla. Haastatteluiden tuloksista selvisi, että verrattuna aiempiin tutkimuksiin, älypuhelinkäyttäjien tietoturvatuntemus ja valmius erilaisia tietoturvauhkia vastaan on pääosin hyvällä tasolla.

Asiasanat: kyberturvallisuus, kyberuhka, kybertoimintaympäristön hierarkkinen rakennemalli, tietoturva, turvallisuus, älypuhelin

ABSTRACT

Laitinen, Otto
Utilization of the hierarchical structural model of the cyber environment in smartphones
Jyväskylä: University of Jyväskylä, 2023, 69 pp.
Cyber Security, Master's Thesis
Supervisor: Lehto, Martti

The number of smartphone users has grown significantly in recent years, and most people around the world own a smartphone at some point in their lives. The increase in the popularity of smartphones has brought with it a significant amount of cybercrime and state-sponsored exploitation in the field. This master's thesis examined a hierarchical structural model of the cyber environment, utilizing the model's various layers as a framework for understanding cyber threats that occur in the context of smartphones.

The hierarchical structural model of the cyber environment was tailored for the research, making it suitable for use in the context of smartphones. The theoretical part of the thesis revealed that the number of cyber threats targeting smartphones is on a significant rise. The quantity and quality of attack vectors targeting smartphones now correspond to those directed at computers. Predictions about the future development of smartphones also indicate that there are expected to be new, even greater threats to smartphones and smartphone users in the cyber operational environment. The empirical part of the thesis was conducted as a qualitative content analysis, and the data was collected through semi-structured interviews. The results of the interviews revealed that compared to previous studies, smartphone users' knowledge of and preparedness against various cybersecurity threats are generally at a good level.

Keywords: cybersecurity, cyber threat, hierarchical structural model of the cyber environment, information security, security, smartphone

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Puhelin on kehittynyt puheviestinnän välineestä taskukokoiseksi tietokoneeksi, älypuhelimeksi. Älypuhelimen kautta voi päästä käsiksi laitteen käyttäjän hyvinkin henkilökohtaisiin tietoihin, kuten käyttäjän asuinpaikkaan, työpaikkaan, maksutietoihin, henkilötietoihin, käyttäjän lähipiiriin tai vaikkapa älykodin avaimiin sekä kaikkiin asunnossa oleviin laitteisiin. Älypuhelimien yleistyttyä, mobiilikäyttöjärjestelmistä on tullut erinomainen esimerkki digitaalisen ja fyysisen maailman yhdistymisestä. (Davis & Samani, 2018; Rauhala, 2022.) Tässä tutkielmassa käytetyn määritelmän mukaan älypuhelin on laite, jossa on normaalien puhelinominaisuuksien lisäksi internetselain, pääsy sähköpostiin ja muita tietokoneelle tyypillisiä ominaisuuksia, kuten mahdollisuus ladata sovelluksia eli applikaatioita (Kielitoimiston sanakirja, 2020; Peda, 2020). Ensimmäisenä älypuhelimen käyttöjärjestelmänä voidaan pitää japanilaisen NTT DoCoMo:n kehittämää ja vuonna 1999 julkaisemaa i-modea, jolla pystyi käyttämään sähköpostia sekä internetselainta. Älypuhelimien kehityksessä huomattava harppaus tapahtui vuonna 2007, jolloin Applen ensimmäinen iPhone julkaistiin. (Islam & Want, 2014.)

Älypuhelimien käyttö on yleistynyt huomattavasti etenkin Suomessa, mutta myös maailmanlaajuisesti. Vuonna 2018 16–89-vuotiaista suomalaisista 80 prosentilla oli älypuhelin omassa käytössään. Älypuhelimien merkittävyydestä suomalaisten arjessa kertoo myös se, että 75 prosenttia suomalaisista käyttää internetiä älypuhelimella. Älypuhelin on myös yleisin internetin käyttölaite suomessa. (Tilastokeskus, 2018.) Älypuhelimien käyttäjämäärän kasvu on myös maailmanlaajuisesti huomattavaa. Vuonna 2016 maailmassa oli 2,5 miljardia älypuhelimen käyttäjää, kun taas vuonna 2019 käyttäjämäärä oli jo 3,2 miljardia. Vuonna 2021 älypuhelimien käyttäjiä odotetaan olevan maailmassa 3,8 miljardia. (Statista, 2019.) Juhani Rauhalan (2022) mukaan vuonna 2022 älypuhelimia käytti arviolta jopa 6,4 miljardia ihmistä.

Älypuhelimien käyttäjämäärien kasvusta ja kehityksen vauhdista voidaan päätellä, että älypuhelin tulee olemaan lähitulevaisuudessa merkittävimpiä, ellei merkittävin käytössä oleva laite ympäri maailmaa. Älypuhelimen odotetaan esimerkiksi korvaavan perinteiset tietokoneet, jolloin laitetta voidaan käyttää

telakoimalla älypuhelin erilliseen näyttöön ja näppäimistöön (Islam & Want, 2014). Älypuhelimien kehityksellä ja käyttäjämäärän kasvulla on myös negatiivisia vaikutuksia, sillä se on herättänyt rikollisten mielenkiinnon kohdistaa hyökkäyksensä juuri älypuhelimiin (Becher, Freiling, Hoffmann, Holz, Ullenbeck & Wolf, 2011; Jiang & Zhou, 2012; Leavitt, 2011; Maslennikov, 2011; Peng, ym., 2014; Rastogi, Chen & Jiang, 2014; Rauhala, 2022; Wright, Dawson, & Omar, 2012). Älypuhelimiin liittyvästä, kasvavasta käyttäjämäärästä ja rikollisuudesta johtuen, älypuhelimien haavoittuvuuksien tutkiminen ja niiden paikkaamiseen tarvittavien keinojen etsiminen on tärkeää.

Älypuhelimiin kehitetään jatkuvasti uusia ominaisuuksia, jotka ovat lähtökohtaisesti hyödyllisiä, mutta ne voivat mukanaan luoda vakavia haavoittuvuuksia. Yksi tällainen ominaisuus on älypuhelimen käytöstä poistaminen tai tuhoaminen etänä. Ominaisuus on tarkoitettu estämään laitteen väärinkäyttöä, mikäli älypuhelin varastetaan tai käyttäjä hukkaa laitteen. Mikäli laite poistetaan käytöstä, laitetta ei pystytä enää avaamaan, mutta sen fyysiset komponentit säilyvät ehjänä ja datan palauttaminen on mahdollista ja se jättää taitavalle hyökkääjälle mahdollisuuden anastaa laitteeseen tallennettu data. Mikäli laite tuhotaan, myös sen fyysiset komponentit tuhoutuvat, jolloin älypuhelimen massamuistiin ei ole enää pääsyä. Ominaisuus on lähtökohtaisesti hyödyllinen käyttäjän tietoturvan kannalta. Kuitenkin tapauksessa, jossa käyttäjän laitteeseen on samanaikaisesti esimerkiksi huollon yhteydessä asennettu luvattomia tai väärennettyjä osia, kuten akku tai näyttö, ja älypuhelin on saastunut haittaohjelman takia, voivat seuraukset olla jopa katastrofaaliset. Mikäli haittaohjelman tarkoituksena on käynnistää laitteen itsetuhoasetus, laitteeseen asennettu panos, väärennetty ja heikosti lämpöä kestävä akku, näyttö tai kotelo voivat aiheuttaa laitteessa ylikuumenemisen takia akkupalon tai räjähdyksen. Tämän seurauksena käyttäjälle voi koitua stressiä, fyysistä haittaa tai jopa kuolema. (Rauhala, 2022.) Rauhalan (2022) mukaan tutkimuksissa on todettu, että älypuhelimen kadottaminen tai laitteen hajoaminen aiheuttaa ihmisissä lähes yhtä paljon stressiä, kuin terrorismin uhka.

Älypuhelimien suosio on tuonut markkinoille myös väärennettyjä älypuhelimia. Väärennettyjen ja kopioitujen älypuhelimien tuotannossa ei noudateta yleistä laadunvalvontaa tai säätelyitä, siksi niiden tuottaminen ja ostaminen on huomattavasti halvempaa kuin aitojen älypuhelimien. Väärennetyn elektroniikkatuotannon koko markkinat ovat arvoltaan noin 100 miljardia dollaria, joka kattaa noin 10 prosenttia koko elektroniikkatuotannosta. Väärennettyjen älypuhelimien markkinat ovat taas arvoltaan noin 48 miljardia dollaria (Rauhala, 2022).

Tässä tutkielmassa hyödynnetään viisikerroksista kybertoimintaympäristön hierarkkista rakennemallia (Lehto, Pöyhönen & Lehto, 2019). Kybertoimintaympäristön hierarkkinen rakennemalli on muokattu Martin Libicikn (2007) luomasta kybermaailman rakenteesta, joka taas perustuu seitsemänkerroksiseen OSI-malliin (Open Systems Interconnection Reference Model). Kybertoimintaympäristön hierarkkisen rakennemallin kerrokset ovat:

- Kognitiivinen kerros
- Palvelukerros
- Semanttinen kerros
- Syntaktinen kerros
- Fyysinen kerros

Kybertoimintaympäristön hierarkkisen rakennemallin jokainen kerros käyttää alemman kerroksen palveluita ja tarjoaa palveluita ylemmälle kerrokselle (Lehto, ym. 2019). Kybertoimintaympäristön rakennemallia on käytetty aiemmin eri tutkimuksissa viitekehyksenä. Esimerkiksi Jouni Pöyhönen (2020) on käyttänyt rakennemallia väitöstyössään. Vaikka Pöyhösen (2020) työssä kybertoimintaympäristön hierarkkista rakennemallia käytetäänkin kriittisen infrastruktuurin tutkimiseen ja kehittämiseen, rakennemallin perusperiaate on sama. Älypuhelimen kohdalla kognitiivinen kerros sisältää itse käyttäjän, palvelukerroksessa on puhelimeen ladatut ohjelmistot ja sovellukset (applikaatiot), semanttisessa kerroksessa on laitteeseen tallennettu informaatio, syntaktinen kerros sisältää laiteohjelmiston (engl. firmware) ja toiminnanohjausjärjestelmät, joilla laite liittyy osaksi verkkoa ja viimeisenä on fyysinen kerros, joka sisältää itse fyysisen laitteen komponentteineen.

Tässä tutkielmassa kybertoimintaympäristön hierarkkista rakennemallia hyödynnetään älypuhelimissa olevien haavoittuvuuksien tutkimiseen. Tutkielman kirjallisuuskatsauksessa tarkastellaan älypuhelimien haavoittuvuuksia kaikissa kybertoimintaympäristön hierarkkisen rakennemallin kerroksissa ja sitä, miten haavoittuvuudet vaikuttavat toisten kerrosten toimintaan ja turvallisuuteen. Tutkielman empiirisessä osassa on tarkoituksena tutkia erityisesti käyttäjän oman toiminnan vaikutuksia laitteen haavoittuvuuksiin, siksi tutkimus kohdistuu lähtökohtaisesti kognitiiviseen kerrokseen ja sen suoriin relaatioihin muiden kerrosten kanssa. Kuten monissa muissakin kyber- ja tietoturvaympäristöissä, myös älypuhelimien kohdalla käyttäjää ja hänen toimintaansa pidetään yleisesti suurimpana haavoittuvuutena (Das & Khan, 2016). Vaikka älypuhelimen käyttäjän toimintoja on lähtökohtaisesti rajoitettu sekä iOS- että Android-käyttöjärjestelmissä enemmän kuin esimerkiksi tietokoneen Microsoft Windows-käyttöjärjestelmissä, voi älypuhelimen käyttäjän oma toiminta aiheuttaa suuriakin turvallisuusriskejä. Esimerkiksi Androidin virallisen sovelluskaupan, Google Playn, haittasovellusten tunnistusohjelman Google Play Protectin on todettu sisältävän huomattaviakin puutteita. Tämä tarkoittaa sitä, että haittasovelluksen lataaminen älypuhelimeen on mahdollista myös virallisesta sovelluskaupasta (Davis & Samani, 2018).

Lisäksi kyberrikoksista puhuttaessa tietojen kalastelu on merkittävä ongelma, jota voidaan helposti kohdistaa myös älypuhelimien käyttäjiin. Näistä syistä empiirinen tutkimus on tärkeää kohdistaa älypuhelimien käyttäjiin. Kognitiivista kerrosta tutkiessa, tutkimus toteutetaan laadullisena aineiston analyysinä. Laadullisella aineiston analyysillä on tarkoituksena tarkastella aiempia tutkimuksia aiheeseen liittyen ja saada haastatteluiden kautta

ymmärrystä siitä, miten käyttäjät suojaavat älypuhelimiaan ja miten vakavasti he suhtautuvat älypuhelimiin kohdistuviin uhkiin. Haastateltavat rajataan työssäkäyviin henkilöihin, joilla on käytössään työpuhelimena älypuhelin. Rajauksen tarkoituksena on saada ymmärrystä siihen, vaikuttaako käyttäjän työpaikan määrittämät mahdolliset ohjeistukset ja politiikat työpuhelimen ja vapaa-aikana käytettävän puhelimen käyttöön.

Haastateltavien henkilöiden työpuhelin ja vapaa-ajan puhelin saavat kuitenkin olla sama laite. Haastateltavan henkilön koulutustausta tai työnkuva eivät vaikuta haastattelun pitämiseen, eli haastateltavan ei tarvitse olla tietoturva- tai mobiililaiteasiantuntija. Tutkimuksen tarkoituksena on vastata seuraavaan tutkimuskysymykseen:

- Minkä tasoinen on älypuhelinkäyttäjien tietoturvatuntemus?

Lisäksi tutkimuksessa käytetään kahta apututkimuskysymystä, jotka täydentävät päätutkimuskysymystä:

- Millä osa-alueilla älypuhelinkäyttäjien toimet aiheuttavat eniten uhkia?
- Millä osa-alueilla älypuhelinkäyttäjien toimet aiheuttavat vähiten uhkia?

2 KYBERTOIMINTAYMPÄRISTÖN HIERARKKINEN RAKENNEMALLI

Tutkielman ensimmäisessä pääluvussa esitellään tarkemmin kybertoimintaympäristön hierarkkinen rakennemalli sekä kerrotaan, miten kybertoimintaympäristön hierarkkinen rakennemalli on kehitetty. Luvussa tutustutaan tarkemmin jokaiseen rakennemallin kerrokseen. Kerrokset esitellään käyttämällä kahta aiempaa tutkimusta, joissa kybertoimintaympäristön hierarkkista rakennemallia on käytetty omassa kontekstissaan.

2.1 Hierarkkisen rakennemallin esittely

Kybertoimintaympäristön hierarkkinen rakennemalli sisältää viisi eri kerrosta, kognitiivinen kerros, palvelukerros, semanttinen kerros, syntaktinen kerros ja fyysinen kerros (Lehto, ym., 2019). Kybertoimintaympäristö voidaan mieltää tilana, joka on samaan aikaan yhdistetty ja erotettu fyysisestä maailmasta, kuten maasta, ilmasta, vedestä ja avaruudesta. Kybertoimintaympäristö on siis ihmisen luoma ympäristö, joka perustuu elektroniseen teknologiaan, ohjelmistoihin, laiteohjelmistoihin ja komponenttisovelluksiin, jotka on erityisesti suunniteltu muokkaamaan elektromagneettista energiaa salatuksi viestinnäksi (Lehto, 2018). Sanaa kyber- käytetään etuliitteenä tietokoneisiin ja elektromagneettiseen spektriin liittyvissä tapahtumissa. Kyberympäristö sisältää paitsi internetiin liitetyt laitteet, mutta myös organisaatioiden sisäverkot / intranetit, matkapuhelinverkot, valokuitukaapelit ja avaruusperusteisen viestinnän (engl. space-based communication). Esimerkiksi sodankäynnissä, kybervoiman (engl. cyber power) käyttö voi johtaa haluttuun lopputulokseen niin kybertoimintaympäristössä, kuin myös kybertoimintaympäristön ulkopuolella (Lehto, 2018).

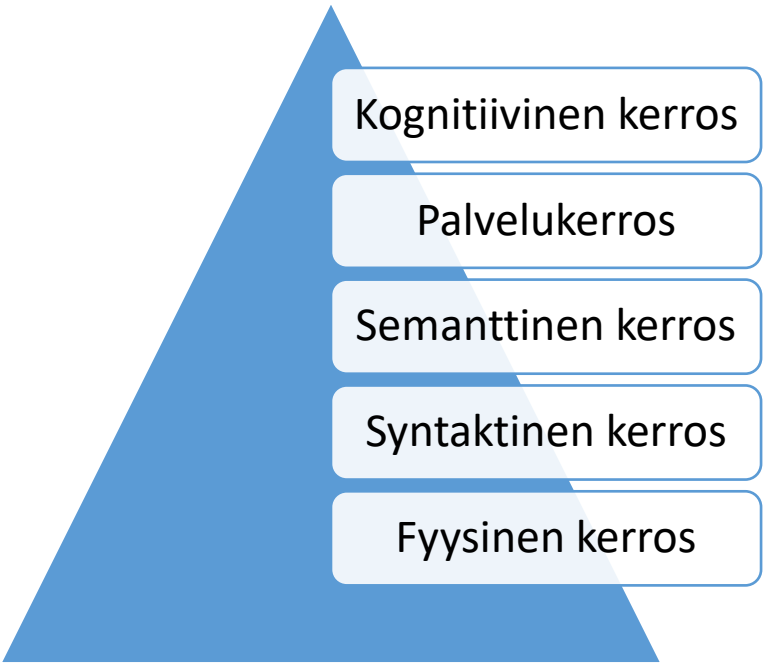
Kybertoimintaympäristön hierarkkinen rakennemalli on muokattu Libickin (2007) neliosaisesta kybermaailman rakenteesta, joka on jaettu käyttö-, semanttiseen, syntaktiseen ja fyysiseen kerrokseen (Norri-Sederholm, Laitinen,

Lehto & Kari, 2019). Libickin luoma kybermaailman rakenne perustuu OSI-malliin. OSI-malli on ISO:n (International Organization for Standardization) standardoima seitsemänkerroksinen malli, jolla kuvataan tiedonsiirtoprotokollien toimintaa. OSI-mallin jokainen kerros käyttää alemman kerroksen palveluita hyväkseen, samalla kun tarjoaa palveluita ylemmälle kerrokselle. OSI-mallin kerrokset ovat ylhäältä alas seuraavat:

- Sovelluskerros,
- Esitystapakerros,
- Istuntokerros,
- Kuljetuskerros,
- Verkkokerros,
- Siirtokerros,
- Fyysinen kerros (Li, Li & Cui, 2011).

Kuviossa 1 on esitettynä kybertoimintaympäristön hierarkkinen rakennemalli. Mallin ajatus on sama kuin OSI-mallilla, eli jokainen kerros hyödyntää alemman kerroksen palveluita ja samalla tarjoaa palveluitaan yhtä kerrosta ylemmäs. OSI-malli ja kybertoimintaympäristön hierarkkinen rakennemalli eroavat kerrosten lukumäärässä ensinnäkin siksi, että osa OSI-mallin kerroksista on sulautettu yhteen kybertoimintaympäristön hierarkkista rakennemallia luodessa. Tämän tutkimuksen kannalta tärkeimpänä eroavaisuutena on kognitiivinen, eli käyttäjäkerros. Koska OSI-mallia käytetään kuvaamaan tiedonsiirtoprotokollien toimintaa, ei kognitiivinen kerros ole siinä tarpeellinen. Kybertoimintaympäristöä tarkasteltaessa ihminen, eli käyttäjä, on erittäin suuressa roolissa ja siksi se on lisätty kybertoimintaympäristön hierarkkisen rakennemallin ylimmäksi kerrokseksi.

Kybertoimintaympäristön hierarkkista rakennemallia on käytetty viitekehyksenä useammassakin erialisessa tutkimuksessa. Esimerkiksi Finnish journal of eHealth and eWelfare artikkelissa terveydenhuolto ja kyberuhkat sekä artikkelissa Cyber Security in Healthcare Systems kybertoimintaympäristön hierarkkista rakennemallia käytetään kybermaailman haavoittuvuuksien ja hyökkäyksien havainnointiin, joissa painotetaan sairaalajärjestelmiä (Lehto, Neittaanmäki, Pöyhönen, 2022; Norri-Sederholm, ym., 2019). Kybertoimintaympäristön hierakkista rakennemallia käytetään myös artikkelissa The modern strategies in the cyber warfare, joka taas käsittelee modernia sodankäyntiä (Lehto, 2018).



KUVIO 1 Kybertoimintaympäristön hierarkkinen rakennemalli (Lehto, ym., 2019)

2.1.1 Fyysinen kerros

Norri-Sederholmin ym. (2019) ja Lehto ym. (2022) mukaan fyysinen kerros sisältää langattomat ja kiinteät yhteydet sekä verkkoon liitetyt, tässä tapauksessa lääkinnälliset laitteet. Fyysisen kerroksen haavoittuvuuksia aiheuttaa muun muassa puutteet laitteiden fyysisessä suojauksessa, avoimet WLAN-verkot, aukot verkkosalauksessa ja laitteiden tekninen suojaamattomuus. Puhuttaessa fyysisestä kerroksesta, tarkoitetaan kuitenkin laitetta, jota pystytään fyysisesti käsittelemään. Tästä syystä, jos hyökkääjän kohteena on fyysinen kerros, voidaan sillä tarkoittaa esimerkiksi laitteen tuhoamista tai varastamista (Norri-Sederholm, ym., 2019). Aiempia tutkimuksia hyödyntäen, esimerkiksi sodankäynnissä fyysinen kerros sisältää kaikki fyysiset välineet ja tietoverkot, joita armeija käyttää kommunikointiin. Jotta kybertoimintaympäristön voi rakentaa, ensimmäinen vaatimus sille on fyysisen kerroksen muodostaminen. Fyysinen kerros sisältää kaikki laitteistot ja komponentit, joita tarvitaan tiedon ja datan lähettämiseen, vastaanottamiseen ja tallentamiseen sekä vuorovaikuttamiseen kybertoimintaympäristössä. Tämä infrastruktuuri sisältää muun muassa kaapeleita, reitittimiä, lähettimiä, vastaanottimia, kovalevyjä, tietokoneita ja rajapintakomponentteja. Fyysinen kerros on silta, jota käytetään kybertoimintaympäristössä radioaaltojen, kupari- tai valokuitukaapelien, sekä syntaktisen kerroksen välityksellä (Lehto, 2018).

2.1.2 Syntaktinen kerros

Syntaktinen kerros sisältää järjestelmien hallinta- ja ohjausohjelmistoja, liityntäteknologioita, verkkoprotokollia ja muita toimintoja, joilla verkkoon kytketyt laitteet ovat vuorovaikutuksessa keskenään (Lehto, ym., 2022; Norri-Sederholm, ym., 2019). Syntaktinen kerros sisältää ohjelmistot, jotka tarjoavat käyttökomennot fyysiselle kerrokselle (Lehto, ym., 2022). Haavoittuvuuksia syntaktiseen kerrokseen luovat esimerkiksi heikot valvontajärjestelmät ja heikot järjestelmien suojaustasot, verkkoon kytketyt laitteet, jotka ovat puutteellisesti suojattuja ja käyttäjätunnistamisessa olevat puutteet. Syntaktisen kerrokseen suunnatut hyökkäykset voidaan toteuttaa käyttäen hyväksi puutteellista käyttäjävarmennusta, jolloin hyökkääjä pääsee kirjautumaan järjestelmään jonkun olemassa olevan käyttäjän tiedoilla tai profiililla. Lisäksi hyökkäys voidaan tehdä hyödyntämällä haittaohjelmia, joiden tarkoituksena on joko ottaa laite haltuun tai saastuttaa se (Norri-Sederholm, ym., 2019). Esimerkiksi sodankäynnissä syntaktinen kerros muodostuu useista sotilasjärjestelmien ohjaus- ja johtamisjärjestelmistä sekä ominaisuuksista, jotka helpottavat verkkoon kytkettyjen laitteiden vuorovaikutusta. Syntaktinen kerros käyttää protokollia ja sovelluksia, jotka on luotu lähettämään, vastaanottamaan, tallentamaan, muodostamaan ja esittämään dataa fyysisessä kerroksessa. Syntaktinen kerros voidaan jakaa myös alikerroksiin, kuten 7-kerroksisessa OSI-mallissa on tehty (Lehto, 2018). Nämä kerrokset ovat OSI-mallin neljästä alemmasta kerroksesta kolme, siirtokerros, verkkokerros ja kuljetuskerros, poislukien fyysinen kerros (Li, Li & Cui, 2011).

2.1.3 Semanttinen kerros

Semanttisessa kerroksessa sijaitsee käyttäjille kuuluva informaatio sekä käyttäjän itsellään hallussa oleva toimintojen ohjaus (Lehto ym., 2022; Norri-Sedeholm, ym., 2019). Semanttiseen kerrokseen kuuluu myös tässä tapauksessa kaikki sairaalan palvelimilla ja pilvipalveuista löytyvä informaatio ja tietosisältö (Lehto, ym., 2022). Haavoittuvuuksia semanttisessa kerroksessa luovat erilaiset virheet ohjelmistoissa, kuten puutteet tietosuojauksessa ja ohjelmistosuunnittelussa. Semanttiseen kerrokseen kohdistetut hyökkäykset liittyvät pitkälti järjestelmästä löytyvään informaatioon. Hyökkäyksen seurauksena tietoa voidaan esimerkiksi tuhota, väärentää tai anastaa, jonka jälkeen myös tiedolla kiristäminen on mahdollista (Norri-Sederholm, ym., 2019). Semanttinen kerros on koko ympäristössä käytettävän verkon ydin. Esimerkiksi sodankäynnissä semanttinen kerros sisältää kaiken informaation ja tietoaineistot tallennettuna armeijan tietovarastoihin, erilaisiin laaja-alaisiin tietojärjestelmiin ja päätelaitteisiin, kuten myös käyttäjän hallinnoimiin toimintoihin. Semanttisessa kerroksessa liikkuvan tiedon tulisi olla suojattua. Suojatun tiedon tulisi noudattaa tietoturvan periaatteita, joita ovat luottamuksellisuus, eheys, saatavuus, aitous ja kiistämättömyys (Lehto, 2018).

2.1.4 Palvelukerros

Lehdon , ym. (2022) ja Norri-Sederholmin, ym. (2019) artikkeleissa palvelukerroksesta puhuttaessa, tarkoitetaan sairaalan verkkopalveluita, kuten julkisia ja kaupallisia palveluita ja Kanta-palvelua. Haavoittuvuuksia palvelukerroksen palveluille luovat tässä tapauksessa puutteellinen kyberturvallisuuden johtaminen ja liian myönteinen kuva järjestelmän toimivuudesta hyökkäyksiä vastaan. Palvelukerrokseen kohdistuvat hyökkäykset ovat pitkälti palvelunestohyökkäyksiä, joiden tarkoituksena joko hidastaa tai estää palvelun käyttö. Esimerkiksi Kelan Kanta-palveluihin kohdistettiin vuonna 2017 palvelunestohyökkäys, joka esti palveluiden käytön muutamaksi tunniksi. Palvelunestohyökkäyksestä ei ole suoranaista uhkaa informaation katoamiselle. (Norri-Sederholm, ym., 2019.) Sodankäynnin näkökulmasta palvelukerros sisältää kaikki tietotekniikkaperusteiset asevoimien palvelut, joita käyttäjät käyttävät verkossa. Toiminnallisia palveluita ovat muun muassa johtamispalvelut, tiedustelu- ja valvontapalvelut, ohjauspalvelut, tulenjohtopalvelut, logistiikkapalvelut, henkilöstöpalvelut, rakennuspalvelut ja talouspalvelut. Yhteisiä ydinpalveluita ovat muun muassa palvelunhallinta, rekisteripalvelut, maantieteelliset palvelut, tiedonhallinta, yhteisöpalvelut ja tietoturva (Lehto, 2018).

2.1.5 Kognitiivinen kerros

Viimeinen, eli kognitiivinen kerros on itse käyttäjä. Se sisältää käyttäjän tiedot ja taidot sovellusten käyttämisestä sekä informaation omaksumisesta ja tulkinnasta (Lehto, ym., 2022; Norri-Sederholm, ym., 2019). Kognitiivinen kerros voidaan nähdä myös laajemmassa mittakaavassa, sen ollessa psyykkinen kerros (eng. mental layer). Psyykkinen kerros sisältää käyttäjän kognitiivisen tietoisuuden ja tunnetietoisuuden (Lehto, ym., 2022). Haavoittuvuuksia kognitiiviseen kerrokseen tuovat käyttäjien koulutuksen puute ja organisaatioissa vaillinainen henkilöstön valvonta. Esimerkiksi haittaohjelmien leviäminen tapahtuu usein käyttäjän toimesta. Haittaohjelmien levityskanavina voivat toimia esimerkiksi haitalliset verkkosivut, sähköposti sekä sosiaalinen media. Kognitiiviseen kerrokseen suunnatut hyökkäykset kohdistuvat suoraan itse käyttäjään. Tällaisia hyökkäyksiä voivat olla esimerkiksi tietojen kalastelu ja identiteettivarkaudet. (Norri-Sederholm, ym., 2019.) Armeijan toiminnan näkökulmasta kognitiivinen kerros tarjoaa päättäjille ja taistelijoille tietoisuuden ympäristöstä, eli maailman jossa informaatiota tulkitaan ja jossa ymmärrys informaation asiayhteyteen luodaan. Kognitiivinen kerros voidaan nähdä laajemmassa mittakaavassa sen ollessa psyykkinen kerros, joka sisältää käyttäjän kognitiivisen tietoisuuden ja tunnetietoisuuden. Käsitteet, jotka ovat yhteydessä tunteisiin kuten luottamus, hyväksyntä ja kokemus, ovat keskeisiä tunnetietoisuudessa (Lehto, 2018).

Kuten huomataan, on eri kerroksien haavoittuvuuksilla ja toiminnoilla paljon päällekäisyyksiä, eikä haavoittuvuus yhdessä kerroksessa vaikuta ainoastaan kyseisen kerroksen turvallisuuteen. Esimerkiksi huolimaton toiminta kognitiivisessa kerroksessa voi vaikuttaa laajalti kybertoimintaympäristön

hierarkkisen rakennemallin kaikkiin kerroksiin järjestelmässä. Esimerkeissä käytettiin kolmea eri tutkimusta, joissa kybertoimintaympäristön hierarkkista rakennemallia on käytetty hyödyksi. Tutkimuksissa Norri-Sederholm, ym. (2019) ja Lehto , ym. (2022) esittelivät kybertoimintaympäristön hierarkkisen rakennemallin sairaalaympäristössä, kun taas Lehto (2018) esitteli mallin käyttöä armeijan toiminnan näkökulmasta. Näitä kahta erilaista ympäristöä käytettiin kybertoimintaympäristön hierarkkisen rakennemallin esittelyssä jotta tutkielman pohjaksi saadaan mahdollisimman kattava kuva siitä, mitä kybertoimintaympäristön hierarkkinen rakennemalli tarkoittaa.

Tässä tutkielmassa kybertoimintaympäristön hierarkkista rakennemallia käytetään viitekehyksenä älypuhelimien haavoittuvuuksien tutkimiseen. Luvussa 2.2 muodostetaan kuva siitä, miten kybertoimintaympäristön hierarkkinen rakennemalli muodostuu älypuhelimien kontekstissa.

2.2 Kybertoimintaympäristön hierarkkinen rakennemalli älypuhelimissa

Kybertoimintaympäristön hierarkkisen rakennemallin esittelyyn käytetyissä esimerkeissä Norri-Sederholm, ym. (2019) oli käyttänyt mallia suljetussa tai puolisuljetussa sairaalaympäristössä ja Lehto (2018) oli käyttänyt mallia tukemaan tutkimusta modernista sodankäynnistä. Molemmissa esimerkeissä älypuhelin laitteena asettuisi osaksi suurempaa ympäristöä, esimerkiksi fyysiseen kerrokseen. Siinä missä Norri-Sederholm, ym. (2019) ja Lehto (2018) käyttävät mallia laajemmassa ympäristössä, tässä tutkielmassa yksi laite, älypuhelin, muodostaa itsessään kokonaisen ympäristön. Tästä syystä hierarkkista rakennemallia muodostaessa älypuhelimen ympäristössä malli näyttää pintapuolisesti hieman erilaiselta, vaikka todellisuudessa perusperiaate kybertoimintaympäristön hierarkkiselle rakennemallille on sama (KUVIO 2).

KUVIO 2 Älypuhelimen kybertoimintaympäristön hierarkkinen rakennemalli

2.2.1 Fyysinen kerros

Älypuhelimien kybertoimintaympäristön hierarkkisessa rakennemallissa, fyysinen kerros pitää sisällään itse käsin kosketeltavan laitteen sekä laitteen sisällä olevat komponentit. Älypuhelimen suorituskyky alkaa tänä päivänä lähentyä perinteisten pöytätietokoneiden suorituskykyä, jolloin myös käytettävät komponentit ovat hyvin samankaltaisia. Kuten tietokoneesta, älypuhelimesta löytyy oma prosessorinsa (Gaw, 2019). Älypuhelimessa on välimuisti, joka on suoraan yhteydessä älypuhelimen prosessorin kanssa. Useimmissa älypuhelimissa on myös kaksi kameraa, edessä ja takana. Molempia kameroita voidaan käyttää perinteiseen tapaan valokuvaamiseen, mutta etukameraa voidaan usein käyttää myös käyttäjän varmentamiseen kasvojentunnistuksessa. Koska älypuhelin on mobiililaite, siinä on akku ja akun lataukseen sekä virran käyttöön vaadittavat komponentit (Gaw, 2019). Vaikka pilvitallennuksen suosio on yleistyvää, älypuhelimessa on myös oma muistinsa johon dataa ja informaatiota tallennetaan paikallisesti. Tiedonsiirtoa varten älypuhelimessa on useita eri sovittimia. Esimerkiksi verkkosovittimen avulla laitteen voi kytkeä langattomaan verkkoon ja esimerkiksi sitä kautta internetiin. Bluetooth-sovittimella älypuhelimen saa yhdistettyä muihin bluetoothia tukeviin laitteisiin (Gaw, 2019).

Älypuhelimessa on myös luonnollisesti puhelimelle kuuluvia komponentteja, kuten mikrofoni, kaiutin ja lähetinvastaanotin puhe- ja mobiilidataa varten. Älypuhelimen merkittävin ulospäin näkyvä komponentti on sen näyttö. Modernin älypuhelimen näyttö on useimmiten kosketusnäyttö, joka mahdollistaa laitteen käytön ilman erillistä näppäimistöä. Älypuhelin sisältää myös useita eri sensoreita kameran lisäksi, joilla voidaan mitata

esimerkiksi laitteen lämpöä, painetta tai liikettä (GPS). Sensoreita voidaan käyttää myös sormenjälkitunnistukseen, jolla käyttäjä verifioidaan. (Gaw, 2019.)

2.2.2 Syntaktinen kerros

Syntaktisessa kerroksessa toimivat laitteen firmware, eli laiteohjelmisto, laitteen käyttöjärjestelmä, sekä komponentit, joiden avulla älypuhelin liittyy osaksi verkkoa. Firmware on asennettuna komponenttitasolle ja se toimii sovellusten ja komponenttien rajapinnassa, ohjaten esimerkiksi prosessorin ja muistin käyttöä. (Yang, Choi, Kim & Chang, 2015.) Älypuhelin liittyy verkon osaksi verkkosovittimella, jolloin se on osa lähiverkkoa, joka voi olla yhdistettynä internetiin. Älypuhelin voi myös yhdistyä suoraan internetiin mobiiliverkkoa käyttäen, jolloin komponenttina toimii älypuhelimessa oleva lähetinvastaanotin (Gaw, 2019). Lehto ym. (2019) määrittelevät syntaktisen kerroksen muodostuvan ”erilaisista järjestelmien ohjaus- ja hallintaohjelmista, liityntäteknologioista sekä toiminnoista, joilla verkkoon kytketyt laitteet ovat vuorovaikutuksessa keskenään, kuten verkkoprotokollat, virheenkorjaus, käsittely jne.”. Tällä määritelmällä, älypuhelimien kontekstissa syntaktiseen kerrokseen lukeutuvat juuri laiteohjelmisto sekä ulkoiseen tai sisäiseen verkkoon liittymiseen vaadittavat komponentit. Kuten huomataan, syntaktisen kerroksen sisältö on pitkälti päällekkäistä fyysisen kerroksen kanssa, mutta haavoittuvuudesta tai hyökkäyksestä riippuen, ne voidaan jakaa omiin osiinsa.

Laitteen käyttöjärjestelmä voisi periaatteessa kuulua mihin tahansa viidestä kerroksesta, jopa fyysiseen kerrokseen. Älypuhelimien kontekstissa laitteen käyttöjärjestelmä toimii kuitenkin erittäin paljon rinnakkain älypuhelimen laiteohjelmiston kanssa, esimerkiksi laiteohjelmiston ja käyttöjärjestelmän päivitykset tapahtuvat samanaikaisesti. Tämä ei kuitenkaan poista sitä, etteikö laitteen käyttöjärjestelmä toimisi kybertoimintaympäristön hierarkkisessa rakennemallissa useammassa kerroksessa. Tutkimuksessa halutaan kuitenkin tuoda esille käyttöjärjestelmän merkitys ja näin ollen se on parasta asettaa syntaktiseen kerrokseen.

2.2.3 Semanttinen kerros

Semanttinen kerros sisältää kaiken datan ja informaation, mitä älypuhelimeen on tallennettu joko kiinteään massamuistiin tai pilvipalveluun, joka on käyttäjän itsensä hallinnassa. Tallennettu informaatio voi pitää sisällään esimerkiksi sähköposti-, teksti- ja Whatsapp-viestejä, tallennettuja dokumentteja ja kuvia tai muihin sovelluksiin tallennettua dataa. Älypuhelimen eri sovellukset ja sensorit keräävät laitteen käytöstä ja käyttäjästä dataa. Tällaista dataa voivat olla esimerkiksi paikkatiedot, laitteen käyttöajankohdat ja eri sovellusten käyttötottumukset (Keuch, Struminskaya, Antoun, Couper & Kreuter, 2019). Käyttäjä pystyy itse hallitsemaan osittain, miten passiivista dataa kerätään, esimerkiksi antamalla älypuhelinsovelluksille luvan käyttää puhelimen keräämiä paikkatietoja. Passiivisesti kerätyn datan voidaan osittain olettaa kuuluvan semanttiseen kerrokseen, koska sen keräämistä voi käyttäjä itse hallita.

Semanttinen kerros linkittyy syntaktiseen kerrokseen laiteohjelmiston avulla ja tämän lisäksi fyysiseen kerrokseen, kun informaatiota ja dataa tallennetaan laitteen muistiin.

2.2.4 Palvelukerros

Kybertoimintaympäristön hierarkkisen rakennemallin palvelukerros älypuhelimien kontekstissa tarkoittaa laitteen taustalla toimivia palveluohjelmistoja sekä erillisiä sovelluksia. Sovellukset voivat olla laitteen tai käyttöjärjestelmän tuottajan esiasentamia, kuten sähköposti ja internetselain tai ne voivat olla käyttäjän itse lataamia virallisesta sovelluskaupasta (Google Play, App Store), puhelimen selaimen avulla internetistä tai esimerkiksi ulkoisesta laitteesta, kuten tietokoneesta tai ulkoiselta kovalevyltä. Ladattavia sovelluksia löytyy tänä päivänä erittäin moneen eri käyttötarkoitukseen. Sovellukset voivat olla esimerkiksi pankki- ja tunnistautumispalveluita, askelmittareita ja muita liikunnan edistämiseen tarkoitettuja sovelluksia, pelejä ja sosiaalisen median sovelluksia. Myös perinteiset puhelimen toiminnot eli yhteystiedot, soittaminen ja tekstiviestit tapahtuvat älypuhelimissa sovellusten kautta. Palvelukerros linkittyy semanttiseen kerrokseen tallentamalla ja käyttämällä informaatiota ja dataa semanttisen kerroksen kautta. Palvelukerros on myös se, mistä kognitiivinen kerros, eli käyttäjä saa tarpeelliset välineet laitteen käyttöön.

2.2.5 Kognitiivinen kerros

Kognitiivisessa kerroksessa on laitteen käyttäjä ja käyttäjän inhimillinen käyttäytyminen, ongelmanratkaisukyky, tiedot ja taidot. Käyttäjä käyttää älypuhelinta pitkälti sovellusten avulla, jonka kautta kognitiivinen kerros yhdistyy palvelukerrokseen. Kognitiivinen kerros on siinä mielessä kriittinen, että toiminta tässä kerroksessa voi vaikuttaa suorasti tai melko suorasti kaikkiin kybertoimintaympäristön hierarkkisen rakennemallin kerroksiin. Kuten Norri-Sederholm, ym. (2019) ja Lehto (2018) toivat tutkimuksissaan esille, kognitiivinen kerros sisältää aina käyttäjän tietoineen ja taitoineen. Kognitiivinen kerros on siis aina hyvin pitkälti samanlainen kybertoimintaympäristöstä riippumatta.

3 ÄLYPUHELIMIEN HAAVOITTUVUUDET JA NIIHIN KOHDISTUVAT UHKAT

Tässä luvussa käsitellään kybertoimintaympäristön hierarkkisen rakennemallin avulla älypuhelimista löytyviä haavoittuvuuksia ja uhkia. Koska empiirinen tutkimus kohdistetaan lähtökohtaisesti käyttäjän toiminnan vaikutukseen kybermaailman hierarkkisen rakennemallin eri kerroksiin, painotetaan tässäkin luvussa käyttäjän oman toiminnan vaikutuksia eri kerrosten turvallisuuteen.

Älypuhelimet käyttävät mobiiliympäristönä niin kutsuttua hiekkalaatikkomallia. Hiekkalaatikolla tarkoitetaan sitä, että jokainen laitteen sovellus on jaettu omaan laatikkoonsa, jossa sillä on pääsy ainoastaan omistamaansa hakemistoon. Esimerkiksi sovellus A ei voi käyttää kameraa tai kameran tietoja, ellei sille ole erikseen annettu siihen lupaa. Hiekkalaatikkomallissa sovellukset, jotka käyttävät toistensa tietoja, tarvitsevat käyttöä varten sharedUserID:n, jonka molemmat sovellukset ovat hyväksyneet ja jonka on allekirjoittanut sama käyttäjä. Tämä tarkoittaa sitä, että sovellus A:n saadessa käyttää kameran hakemistoa ja sovellus B:n saadessa käyttää sovellus A:n hakemistoa, ei sovellus B saa automaattisesti lupaa käyttää kameran hakemistoa. Tällä estetään esimerkiksi fyysisen kerroksen sensorin (kameran) käyttö haitallisesti sovellus B:n toimesta. (Shabtai, Fledel, Kanonov, Elovici, Dolev & Glezer, 2010.) Hiekkalaatikkomallin perustoiminta on hyvä ymmärtää, kun tarkastellaan kognitiivisessa kerroksessa tapahtuvien toimintojen vaikutusta muihin kerroksiin.

3.1 Yleiset uhkatekijät

Edellä mainitusti, älypuhelimen mobiiliympäristössä käytetään hiekkalaatikkomallia. Kuten tietotekniikassa aina, ei hiekkalaatikkomallikaan ole täysin pitävä. Vuonna 2021 löydettiin useampia uusia haavoittuvuuksia, esimerkiksi CVE-2021-1905 ja CVE-2021-1906, joiden avulla hyökkääjä voi laitteelle tehdyn muistin vapauttamisen jälkeen päästä käsiksi root-, eli

pääkäyttäjäoikeuksiin. Nämä oikeudet mahdollistavat hyökkääjälle pääsyn kaikkialle laitteeseen. (Guri, 2021; National Vulnerability Database, 2022a; National Vulnerability Database 2022b.) Kuten muissakin kyberhyökkäyksissä, älypuhelimiin kohdistuvan hyökkäyksen tekijä voi olla yksittäinen hakkeri, hakkeriryhmä, valtiollinen toimija, yksityinen yritys, rikollisjengi tai -organisaatio (Rauhala, 2022).

Yksi merkittävä riskitekijä älypuhelimien turvallisuudelle on laajalle levittäytyneet väärennettyjen älypuhelimien markkinat. Väärennettyjen älypuhelimien markkinoiden kokonaisarvo on arviolta noin 48 miljardia dollaria (Rauhala, 2022). Väärennettyjen älypuhelimien suosio kasvaa, koska ne ovat verrattain halpoja ja niiden ostaminen verkkokaupasta on helppoa ympäri maailmaa. Hyvin valmistettu väärennös on lähes identtinen alkuperäisen kanssa, eikä tavallisella kuluttajalla ole mitään mahdollisuuksia tunnistaa väärennöstä alkuperäisestä. Vaikka osa kuluttajista ovatkin tietoisia väärennettyjen älypuhelimien käyttöön liittyvistä riskeistä, he silti käyttävät niitä tietoisesti. Koska väärennettyjen älypuhelimien tuottamista tai laatua ei valvota, voidaan niihin tuotantovaiheessa asentaa takaovia tai niiden mikrosiruihin voidaan implementoida esimerkiksi haittaohjelmia, joita kuluttajan on hankalaa, ellei jopa mahdotonta havaita (Rauhala, 2022). Vastatoimet väärennettyjen älypuhelimien, koteloiden ja komponenttien käyttöön voi olla haastavaa, sillä se vaatii paljon osallistumista alkuperäiseltä laitteen tuottajalta. Esimerkiksi väärennettyjen akkujen käytön estäminen on vaatinut huomattavasti salaustietoturvaan perustuvan teknologian kehittämistä (Rauhala, 2022).

Väärennetyt laitteet ovat usein tuotettuja alueilla, joissa valtiollinen laadun valvonta, säätely ja käytännöt ovat kyseenalaisia. Älypuhelimien lisäksi väärennetyt akut ja laturit ovat laajalti saatavilla, joiden vaihteleva laatu jo itsessään aiheuttavat oman vaaransa. Yhdessä väärennetty akku asennettuna alkuperäiseen älypuhelimeen, tai alkuperäinen akku asennettuna väärennettyyn älypuhelimeen, ja haittaohjelma voivat toimia erittäin vaarallisesti. Esimerkiksi haittaohjelmaksi tarkoitettu sovellus toimii kuten pitääkin, mutta haitallisesti muuttamalla laitteen aseeksi ja räjäyttämällä älypuhelimen. Tämä ei välttämättä ole ollut haittaohjelman tarkoitus, mutta se reagoi näin voimakkaasti koska haittaohjelma on voitu suunnitella alkuperäiselle akulle tai laitteelle. (Rauhala, 2022)

Viimeisimmät WikiLeaks paljastukset osoittavat myös, että älypuhelimien etähakkerointi on jo mahdollista ainakin Android- ja iOs-käyttöjärjestelmää käyttäville laitteille. WikiLeaks osoittaa, että tiedustelupalveluiden on mahdollista ohittaa laitteen laiteohjelmisto jo toimitusketjun aikana ja luoda takaportteja älypuhelimiin. Koska Androidien ja iPhonejen suosio on kasvanut huomattavasti, ovat ne myös nousseet kasvavassa määrin yksityisten hakkerien kohteeksi. Tästä syystä onkin jo kehitetty sovelluksia, joiden avulla hakkeri voi saada täyden kontrollin älypuhelimesta (Rauhala, 2022).

Rauhala (2022) on käyttänyt tutkimuksessaan Physical Weaponization of a Smartphone by a Third Party parametreja, jotka helpottavat arvioimaan

mahdollisten kolmannen osapuolen hyökkäysten aiheuttamat haitat. Näitä ovat esimerkiksi:

- Äkillinen vs. pitkäaikainen
  - Laitteen akun räjähtäminen on äkillinen, kun taas radioaaltojen vahvistuminen on pitkäaikainen
- Ilmeinen vs. piilotettu
  - Laitteen akun ylikuumentuessa, räjähtäessä tai syttyessä palamaan, vaikutus on ilmeinen
  - Radiotaajuuden tehostamisesta aiheutuvat päästöt ovat käyttäjälle piilotettuja
- Katastrofaalinen vs. havaitsematon
  - Katastrofaalinen vaikutus heikentää merkittävästi älypuhelimen käytettävyyttä ja uhkaa käyttäjän hyvinvointia. Havaitsemattomassa hyökkäyksessä käyttäjä ei huomaa mitään haittaa tai vaaraa normaalissa käytössä.
- Toiminnan säilyttävä vs. toiminnan vaarantava vs. toiminnan eliminoiva
  - Esimerkki toiminnan säilyttävästä hyökkäyksestä on radiotaajuuspäästöjen kasvattaminen (pois lukien akkukeston heikentyminen)
  - Esimerkkiskenaario toiminnan vaarantavasta hyökkäyksestä: Internetyhteys tai kameran/gallerian käyttö on pakotettu pois päältä, mutta muut tärkeät toiminnallisuudet, kuten puheluiden soittaminen säilyvät.
  - Toiminnan eliminoiva hyökkäys estää älypuhelimen käytön kokonaan tai laite on tuhottu.

Rauhalan (2022) mukaan, hyökkääjä hyödyntää hyökkäysvektoreita älypuhelimeen suunnatuissa hyökkäyksissä. Hyökkäysvektoreita ovat esimerkiksi:

- Istutettu sovellus
  - Haittaohjelma tai muu sovellus, joka on suunniteltu toteuttamaan tarkasti tiettyjä toimintoja upotetun hyötykuorman (engl. embedded payload) kautta.
- Vapaaehtoisesti ladattu sovellus
  - Sovellus, jonka käyttäjä on tarkoituksellisesti ladannut internetistä.
- Laiteohjelmistoon upotettu haittasovellus
  - Laiteohjelmisto, johon on valmiiksi asennettu haittaohjelma jo laitteen tuotantovaiheessa.
- Päivitys saastuneella laiteohjelmistolla
  - Esiintyy silloin, kun käyttäjä päivittää laitteensa laiteohjelmistolla, johon on upotettu haittaohjelma. Käyttäjä

on saanut laiteohjelmiston haitalliselta verkkosivulta tai muualta.

- ”Rogue”- tai huijausmatkapuhelintukiasemat
    - Kyseiset tukiasemat matkivat, eli ”spoofaavat” aitoja tukiasemia. Tämä hyökkäysvektori mahdollistaa kommunikoinnin seuraamisen tukiasemaan kytkettyjen laitteiden välillä ja spooffattujen tekstiviestien lähettämisen. Täten on mahdollista suorittaa SMS-pohjaisia hakkerointeja valetukiasemasta uhrin laitteeseen.
- Väärennetyn älypuhelimen käyttö
    - Käyttäessään väärennettyä puhelinta, käyttäjä käyttää luvatonta kopiota virallisesta puhelinmerkistä ja mallista. Tällöin älypuhelimen tuottajalla ei ole oikeuksia laitteen tuottamiseen, eikä tuottajaa välttämättä tiedetä ja sen toiminta ei ole valvottua.

3.2 Fyysinen kerros

Kuten aiemmin on kuvattu, fyysinen kerros pitää sisällään itse älypuhelimen sekä kaikki laitteen sisältämät komponentit. Koska kyseessä on mukana kannettava mobiililaite, voidaan yhtenä suurimmista fyysisen kerroksen uhkista olettaa olevan laitteen katoaminen tai varastetuksi joutuminen (Muslukhov, 2012). Lisäksi laitteen vaurioituminen vaikkapa pudotessa on esimerkiksi pöytätietokonetta todennäköisempää ja älypuhelimien katoaminen tai varastetuksi joutuminen on yleisempää kuin kannettavien tietokoneiden (Muslukhov, 2012).

Tänä päivänä haittaohjelmien tarkoituksena on usein tuottaa tekijälleen hyötyä rahallisesti tai anastetun datan avulla. Tämä ei kuitenkaan sulje pois sitä, etteikö älypuhelimiin kohdistettu haittaohjelma voisi myös vaurioittaa laitetta. Älypuhelimiin voidaan kohdistaa esimerkiksi Stuxnetin kaltainen haittaohjelma, joka nostaisi laitteen lämpötilaa ja estäisi älypuhelimen lämpösensoreita havaitsemasta lämmön nousua, jonka seurauksena älypuhelimen fyysinen kerros voi vaurioitua. Vaikka kirjallisuudessa ja mediassa suurin uhka älypuhelimille on niiden tietoturva ja yksityisyydensuoja, joistakin sähköiskuista, tulipaloista ja räjähdyksistä on raportoitu (Rauhala, 2022). Älypuhelimen hukkaaminen, varastetuksi joutuminen tai hajoaminen on lähes kokonaan ja näkyvimmin sidoksissa käyttäjän omaan toimintaan. Tästä syystä fyysisessä kerroksessa olevat haavoittuvuudet ja niihin kohdistuvat uhkat ovat hyvin vahvasti peräisin kognitiivisen kerroksen tapahtumista.

Muslukhov (2012) tuo tutkimuksessaan esille väitteen, jonka mukaan älypuhelimen jouduttua anastetuksi, voi hyökkääjä esimerkiksi vaihtaa älypuhelimessa olevia puhelinnumeroita tai istuttaa laitteeseen haittaohjelman, joka aiheuttaa käyttäjälle vahinkoa joko uudessa laitteessa, tai vanhan laitteen palauduttua omistajalleen. Tällä tavoin myös hyökkääjä voi saada rahallista

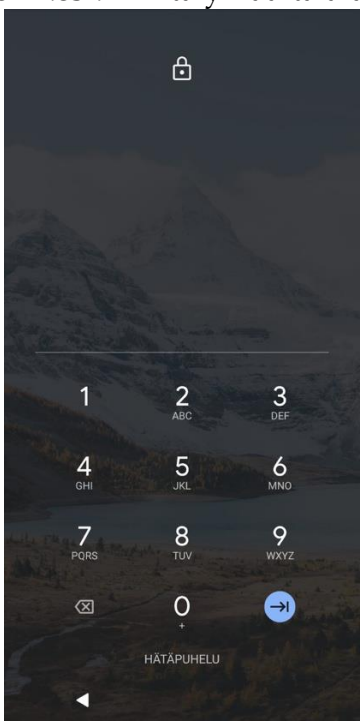
hyötyä tai haltuunsa arvokasta tai arkaluontoista dataa. Älypuhelimiin kohdistettuja niin sanotusti perinteisiäkin haittaohjelmia on olemassa, jotka leviävät esimerkiksi internetistä ladattavien tiedostojen mukana. Tällöin hyökkääjä käyttää hyväkseen jotakin hyökkäysvektoreista. Esimerkiksi akkuun kohdistuva hyökkäys on uhka laitteen fyysiselle kerrokselle ja pahimmillaan myös käyttäjälle itselleen, vaikka hyökkäys tapahtuukin todennäköisimmin syntaktisen kerroksen tai palvelukerroksen kautta. Akkuun vaikuttava hyökkäys voi aiheuttaa akun kuumenemisen, turpoamisen, syttymisen palamaan tai jopa räjähtämisen (Rauhala, 2022).

Fyysisen kerroksen akkuun kohdistuneella hyökkäyksellä voi olla hyvin tuhoisat vaikutukset. Moderneissa älypuhelimissa on erittäin tehokkaat akut. Älypuhelin sisältää Li-Ion-akun, jonka hyötysuhde on jopa 90 prosenttia. Älypuhelimen akku sisältää noin 5Wh energiaa, joka vastaa 18 000- 20 000 joulea. Purkautuessaan energiamäärä vastaa noin viittä grammaa TNT:tä. Energian purkautuessa, akku saattaa aiheuttaa tulipalon tai räjähdyksen ja sen seurauksena vahinkoa laitteen käyttäjälle (Rauhala, 2022). Tulevaisuuden älypuhelimet, jotka voidaan tuhota etälaukaisimella, tuovat mukanaan uusia riskejä älypuhelimien käyttäjille. Toiminnon tarkoituksena on, että jos puhelin katoaa tai se anastetaan, arkaluontoinen data ei joudu vääriin käsiin. Samalla kuitenkin toiminto mahdollistaa sen, että hyökkääjä voi aktivoida itsetuho-ominaisuuden, jolloin laitteesta tulee käyttökelvoton. Tämän lisäksi käyttäjä saattaa menettää arvokasta dataa ja pahimmassa tapauksessa hyökkäys aiheuttaa vaaraa käyttäjän hengelle ja terveydelle. Lähtökohtaisesti itsetuho-ominaisuus on suunniteltu niin, ettei energia purkaudu laitteen ulkopuolelle. Virhe ominaisuuden toiminnossa tai laitteen tuotantoprosessissa voi kuitenkin aiheuttaa suunniteltua suuremman räjähdyksen laitteen sisällä (Rauhala, 2022).

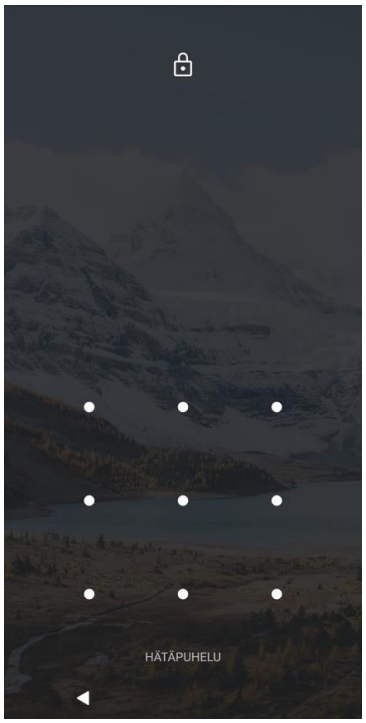
Suurempi riski itsetuhotoiminnon käytössä on kuitenkin väärennetyt älypuhelimet ja väärennetyt laitteiden varaosat. Väärennettyjä laitteita ja varaosia tuotetaan huomattavasti halvemmalla kuin alkuperäisiä, koska niiden tuottamista ei ole säädelty eikä valvottu. Tämän takia esimerkiksi alkuperäisessä laitteessa oleva väärennetty akku, näyttö tai kotelo saattaa aiheuttaa sen, että itsetuho-ominaisuutta käytettäessä energia purkautuu myös laitteen ulkopuolelle (Rauhala, 2022).

Tutkimuksen mukaan 90-prosenttia ihmisistä käyttää älypuhelimissa joko PIN-koodia (KUVIO 3) tai kuviolukitusta (KUVIO 4), jotka ovat Muslukhovin mukaan helposti murrettavissa (Muslukhov, 2012). Vaikka tutkimus on tänä päivänä jo vanha, trendin voi olettaa olevan lähes sama, sillä älypuhelimien käyttöjärjestelmät eivät tarjoa lähtökohtaisesti muita yhtä nopeasti käytettäviä lukitusmenetelmiä. Muslukhovin (2012) mukaan, ihmiset käyttävät puhelimen lukituksessa PIN-koodia ja kuviolukitusta juuri siitä syystä, että pitkän salasanan tai muiden varmempien lukitusmenetelmien käyttö on puhelimen käyttöasteeseen nähden hidasta. Toisen tutkimuksen mukaan, älypuhelimen käyttäjän olan yli katseleva (shoulder surfing) henkilö muistaa kuviolukituksen 67 prosentin varmuudella. Todennäköisyys muistaa oikea kuvio nousee 80 prosenttiin, mikäli katseleva henkilö näkee lukituksen useamman kerran. Tämän

lisäksi älypuhelinkäyttäjät suosivat yksinkertaisia lukituksia luodessaan joko PIN-koodeja tai kuvioita. Yksi yleinen PIN-koodi on 2580, jossa numerot luovat kuvion keskiriviltä ylhäältä alas (Aviv, Davin, Wolf & Kuber (2017).



KUVIO 3 Älypuhelimen PIN-koodi



KUVIO 4 Älypuhelimen kuviolukitus

3.3 Syntaktinen kerros

Tässä tutkielmassa syntaktisella kerroksella tarkoitetaan älypuhelimien laiteohjelmistoa, käyttöjärjestelmää sekä komponentteja, joilla älypuhelin liittyy osaksi verkkoa. Älypuhelimen laiteohjelmisto on hieman erilainen kuin tietokoneissa. Tietokoneen laiteohjelmisto on asennettuna laitteen ROM-muistiin ja tämän avulla laitteen komponentit toimivat. Lisäksi tietokoneiden laiteohjelmisto pitää usein päivittää erikseen. Älypuhelimissa laiteohjelmisto toimii enemmänkin siltana käyttöjärjestelmän ja komponenttien välillä ja tavallisesti laiteohjelmiston päivitys tapahtuu käyttöjärjestelmäpäivityksen yhteydessä. (Reidt, 2022.)

Tutkimuksen mukaan, halpatuotettuihin puhelimiin ja ennen kaikkea kehittyvissä maissa tuotettuihin puhelimiin haittaohjelmien kehittäjät ovat maksaneet laitteita tuottaville yrityksille siitä, että älypuhelimiin esiasennetaan haittaohjelmia. Näissä tapauksissa haittaohjelmia levitetään älypuhelimissa joko esiasentamalla laitteisiin haitallisia sovelluksia, tai asentamalla haittaohjelma suoraa laiteohjelmistotasolle. Laiteohjelmistotasolta haittaohjelman levittäminen on tehokasta, sillä haittaohjelma saa korkeammat käyttöoikeudet. (Zheng, Sun & Lui, 2014.)

Yksi suurimmista uhkista mitä käyttäjä voi syntaktiselle kerrokselle omalla toiminnallaan aiheuttaa, on älypuhelimen roottaus (Android) tai jailbreakaus (iOS). Älypuhelimen roottauksella ja jailbreakauksella tarkoitetaan älypuhelimen käyttöjärjestelmärajoitusten purkamista. Tämä tarkoittaa sitä, että käyttäjä asentaa laitteeseensa sovelluksen, jolla voidaan kiertää laitevalmistajan asettamia rajoituksia ja samalla käyttäjälle annetaan Root- tai SuperUser-tason oikeudet hallita älypuhelinta. Root- tai SuperUser-tason oikeudet ovat korkeimmat mahdolliset oikeudet, jotka käyttäjä voi saada. Tämän avulla älypuhelimen käyttöjärjestelmärajoitusten purkaminen antaa käyttäjälle mahdollisuuden muokata laitettaan vapaasti kaikilla tasoilla. (Nguyen-Vu, Chau, Kang, & Jung, 2017.) Jo sovellus itsessään, jolla älypuhelimen käyttöjärjestelmärajoitukset puretaan saattaa sisältää suuremmalla todennäköisyydellä haittaohjelman, sillä näitä ei saa ladattua Androidin eikä Applen virallisista sovelluskaupoista. Älypuhelimen käyttöjärjestelmärajoitusten purkaminen mahdollistaa myös allekirjoittamattomien sovellusten asentamisen sekä käytön niin Andoideissa, kuin iOS-käyttöjärjestelmissä. Tämä tarkoittaa sitä, että sovelluksen kehittäjä tai jakelija pystyy lisäämään sovellukseen haittaohjelman ilman, että se jää kiinni Android- tai iOs-käyttöjärjestelmän virusturvaan. Ainoa keino pitää älypuhelin, jonka käyttöjärjestelmärajoitukset on purettu edes jokseenkin turvallisena, on asentaa kolmannen osapuolen virusturva laitteeseen, joka tarkistaa sovellusten asennuspaketit ennen sovellusten asentamista älypuhelimeen (Nguyen-Vu, 2017).

Käsiteltäessä älypuhelimia, tietokoneita tai mitä tahansa älylaitteita hyvänä käytäntönä voidaan pitää, että kaikki asennukset ja muutokset järjestelmään

tulisi tehdä mahdollisimman alhaisilla oikeuksilla, jotta laitteen turvallisuus säilyy. Älypuhelin, jonka käyttöjärjestelmärajoitukset ovat puretut toimii kuitenkin lähtökohtaisesti aina root-oikeuksilla. Kuten tutkielmassa on aiemmin mainittu, Android- ja iOS-käyttöjärjestelmällä toimivat älypuhelimet perustuvat hiekkalaatikkomalliin, joka lähtökohtaisesti suojaa haittaohjelmien leviämisen sovelluksesta toiseen (Shabtai, ym., 2010). Älypuhelimen käyttöjärjestelmärajoitusten purkaminen kuitenkin heikentää, tai jopa poistaa hiekkalaatikkomallin tarjoaman suojauksen, sillä jatkuvasti käytössä olevat pääkäyttäjäoikeudet mahdollistavat myös haittaohjelmien leviämisen hiekkalaatikon rajapintojen yli (Sun, Cuadros & Beznosov, 2015).

Kuten aiemmin on mainittu, WikiLeaks on paljastanut, että eri tiedustelupalveluilla on kyvykkyys luoda takaportteja ainakin Android- ja iOs-käyttöjärjestelmää käyttäviin älypuhelimiin jo laitteen tuotantoketjun aikana. Tämän avulla valtiollinen hyökkääjä pystyy hyödyntämään takaporttia ja näin ollen ottamaan täyden kontrollin käyttäjän laitteesta. Esimerkiksi älytelevisioihin kohdistuvaa hakkerointia on kehitetty yhdessä useamman kansallisen tiedustelupalvelun yhteistyössä (Rauhala, 2022).

Rauhalan (2022) mukaan, joidenkin maiden hallinnot ovat varmasti kyvykkäitä luomaan takaovia jälkimarkkinoitaviin laitteisiin. Tämä mahdollistaa tarpeeksi voimakkaille pahantekijöille sen, että he voivat luoda ”tappokytkimen” älypuhelimeen tai älypuhelimen lisälaitteeseen, jonka voi kohdistaa jopa henkilökohtaisesti. Tappokytkimellä voidaan poistaa puhelin käytöstä tai tulevaisuuden älypuhelimissa tuhota laite räjäyttämällä se tai sytyttämällä älypuhelin tuleen.

Kaikissa älypuhelimissa on oletetusti sisään rakennettu lähetinvastaanotin, jonka avulla laite liittyy osaksi verkkoa. Lähetinvastaanotinta voidaan käyttää yhtenä hyökkäysrajapintana, esimerkiksi valeradiomaston avulla. Tällaisessa tapauksessa laite yhdistyy valeradiomastoon osaksi haitallista verkkoa, vaikka se luulee olevansa yhdistettynä operaattorin ylläpitämään ja valvomaan verkkoon (Rauhala, 2022). Tämän seurauksena hyökkääjä pystyy saastuttamaan laitteen esimerkiksi SMS-viestin avulla, joka saattaa aktivoitua jo viestin vastaanottovaiheessa (Rauhala, 2022).

Hyökkääjä voi käyttää valetukiasemana niin kutsuttua StingRay-laitetta, joka on tarkoitettu mobiilitietoliikenteen häiritsemiseen ja puhelimien käyttäjien seuraamiseen. Laite teeskentelee olevansa aito tukiasema ja samalla se ottaa puhelimien tunnistekoodeja, seuraa laitteiden sijainteja ja kaappaa tekstiviestejä sekä puheluita. Älypuhelimen lähetinvastaanotin voi olla myös hyökkäyksen kohteena. Tässä tapauksessa hyökkäys nostaa lähetinvastaanottimen aiheuttaman säteilyn määrää ja lähetinvastaanotin aiheuttaa epänormaalia säteilyä. Tämän seurauksena lähetinvastaanotin aiheuttaa ylimääräistä elektromagneettista säteilyä, akun nopeaa kulumista ja se voi aiheuttaa käyttäjässä ylimääräistä stressiä, mikäli käyttäjä osaa yhdistää tapahtumat säteilytason nousuun (Rauhala, 2022).

3.4 Semanttinen kerros

Semanttinen kerros sisältää kaiken käyttäjän itsensä hallinnassa olevan informaation ja datan (Norri-Sederholm, ym., 2019). Tällaista dataa ovat esimerkiksi laitteesta löytyvät valokuvat, videot, äänitiedostot, eri palveluissa lähetetyt viestit ja laitteeseen tallennetut dokumentit, kuten pdf- ja tekstitiedostot sekä vastaavat dokumentit (Norri-Sederholm, ym., 2019). Android- ja iOs-älypuhelinta käyttöönottaessa, laitteet pyytävät nykyisin käyttäjää kirjautumaan joko Google- tai Apple-tilille, laitteen mukaan. Tilille kirjautuessa käyttäjä liittää laitteensa myös tilillä olevaan pilvipalveluun, minne käyttäjä voi tallentaa niin älypuhelimesta, kuin myös muista laitteista kuten tietokoneista ja tableteista, tiedostoja (Android Ohjeet 2022a; Apple Support, 2022a). Tämä tarkoittaa sitä, että myös pilvipalveluun tallennettuja tiedostoja voidaan pitää semanttisen kerroksen osina ja hyökkäys voidaan kohdistaa muidenkin laitteiden semanttisiin kerroksiin.

Tarkasteltaessa kybermaailman hierarkkista rakennemallia ajatuksena on, että hyökätessä semanttiseen kerrokseen kohteena on aina informaatio. Sama ajatus pätee myös älypuhelimien kontekstissa (Lehto, ym., 2019). Älypuhelimen käyttöjärjestelmärajoitusten purkaminen on yhtä lailla vaarantava tekijä informaation vaarantumiselle kuin myös semanttisessa kerroksessa.

Yksinkertaisimmillaan älypuhelimesta löytyvää tietoa voi ulkopuolinen henkilö nähdä tai varastaa katselemalla olan yli (eng. shoulder surfing). Nähdessään arkaluontoista tietoa, katselija ei välttämättä tee sitä edes tarkoituksella. Asiasta kiinnostuneempi ja harjaantuneempi hyökkääjä voi kuitenkin ottaa näkemästään informaatiosta muistiinpanoja tai ottaa ylös kirjautumistunnuksia, joilla hyökkääjä voi myöhemmin hankkia hyötyä itselleen ja aiheuttaa haittaa uhrille (Lashkari, Farmand, Zakaria, Bin & Saleh, 2009).

Informaatiota varastettaessa, tehokas keino hyökätä on käyttää kalastelua. Kalastelulla tarkoitetaan sitä, että hyökkäyksen kohteena oleva henkilö pyritään saada paljastamaan arkaluontoista tietoa hyökkääjälle, esimerkiksi tilin kirjautumistiedot. Kalasteluhyökkäys voidaan toteuttaa monella tapaa, esimerkiksi soittamalla uhrille ja esiintymällä kirjautumistietoja tarvitsevan yrityksen edustajana, kalastelemalla tietoja sähköpostitse tai luomalla verkkosivut, jotka jäljittelevät mahdollisimman todenmukaisesti aitoja verkkosivuja ja jakamalla tätä sivua massoittain, esimerkiksi sähköpostitse tai tekstiviestitse (Basit, Zafar, Liu, Javed, Jalil & Kifayat, 2021).

Älypuhelimista puhuttaessa, hyökkääjän kalasteltua kirjautumistiedot Google- tai Apple-tilille, hyökkääjä pääsee käsiksi kaikkeen tietoon, minkä uhri on tilin pilveen tallentanut. Uusimmissa älypuhelimissa on kuitenkin mahdollisuus ottaa käyttöön kaksivaiheinen tunnistautuminen ja sitä myös suositellaan käyttäjille. Tämä tarkoittaa sitä, että uudelle laitteelle kirjauduttaessa palvelun tarjoaja pyytää käyttäjää syöttämään vahvistuskoodin, joka lähetetään käyttäjän määrittämälle luotetulle laitteelle. (Android Ohjeet 2022b; Apple Support, 2022b).

Tämän avulla hyökkääjä ei pysty kirjautumaan palveluun ainoastaan käyttäjätunnuksella ja salasanalla. Teoriassa kaksivaiheisen tunnistautumisen pystyisi kuitenkin ohittamaan. Koska älypuhelimien käyttäjät ovat ihmisiä, tapahtuu heille myös virheitä. Luotettavaksi määritelty laite saattaa kadota, hajota tai se voidaan varastaa. Tilanteessa jossa toista luotettavaa laitetta ei ole määritelty, käyttäjä pystyy ohittamaan kaksivaiheisen tunnistautumisen teknisen tuen avulla (Apple Community, 2021). Todellinen käyttäjä vahvistetaan usein turvakysymyksin, kuten sosiaaliturvatunnuksella ja asuinpaikan tiedoilla. Näiden tietojen kalastelu uhrilta on mahdollista, mutta se vaatii hyökkääjältä huomattavan paljon taitoa ja vaivaa, joten riskiä voidaan pitää marginaalisena.

3.5 Palvelukerros

Lehto ym. (2019) mukaan kybertoimintaympäristön hierarkkisessa rakennemallissa palvelukerros sisältää muun muassa julkiset ja kaupalliset verkkopalvelut, sosiaalisen median palvelut ja tietoliikennepalvelut. Älypuhelimista puhuttaessa, palvelukerrokseen voidaan olettaa kuuluvan laitteeseen ladatut ja laitteessa toimivat sovellukset. Tällaisia ovat esimerkiksi viihdekäyttöön tarkoitetut sovellukset kuten pelit ja suoratoistopalvelut, viestintäsovellukset kuten WhatsApp, Signal, Teams ym. ja sosiaalisen median applikaatiot kuten Twitter, LinkedIn ja Facebook.

Kun hyökkäys kohdistetaan palvelukerrokseen, hyökkääjän tarkoituksena on hidastaa tai lamauttaa koko palvelun käyttöä. Tämä onnistuu esimerkiksi DoS- eli palvelunestohyökkäyksellä (Denial of Service) (Lehto, ym., 2019).

Yksinkertaisimmillaan palvelunestohyökkäys toteutetaan avaamalla palvelimelle samanaikaisesti huomattava määrä yhteyksiä, jolloin palveluntarjoaja ei kykene enää vastaamaan käyttäjien kyselyihin koska palvelin ylikuormittuu. Tämä tarkoittaa käytännössä sitä, että palvelukerrokselle suunnatut hyökkäykset eivät ole koskaan kohdistettuina yksittäisiin henkilöihin, vaan kaikkiin palvelun käyttäjiin. Hyökkäysten kohdistuessa yksittäiseen internetyhteyttä vaativaan peliin tai viihteelliseen suoratoistopalveluun voivat toki harmistuttaa käyttäjää, mutta lopulta niiden seuraukset eivät ole kovinkaan vakavia. Hypoteettisessa tilanteessa, jossa yrityksen X työntekijät käyttävät älypuhelimella Teamsia pikaviestintään ja etäpalaverien pitämiseen, voi Teamsiin suunnattu palvelunestohyökkäys lamauttaa käyttäjien viestinnän ja samalla yrityksen toiminnan. Tästä syystä yrityksillä on hyvä olla käytössä varaviestintäkanava. Tässä tapauksessa esimerkiksi Signal, jolloin käyttäjät voivat jatkaa laitteiden käyttöä lähes normaalisti. Vaikka palvelun toimivuus on palveluntarjoajan vastuulla ja varaviestintäkanavan käyttö on yrityksen vastuulla, päätös varaviestintäkanavan käytöstä tapahtuu kognitiivisessa kerroksessa. Tilanteessa, jossa yritys X on ilmoittanut työntekijöilleen käyttävänsä varaviestintäkanavaa, tässä tapauksessa Signal, saattavat useat työntekijät nähdä sovelluksen käyttöönoton tarpeettomana, koska

varaviestintäkanavaa ei käytetä normaalissa arjessa. Tämä johtaa siihen, että käyttöönotto aloitetaan vasta, kun pääviestintäkanavan käyttö on estynyt.

Älypuhelimen käyttöjärjestelmärajoitusten purkaminen ja myöhemmin sovelluskaupan ulkopuolelta ladatut sovellukset saattavat myös aiheuttaa uhkia palvelukerrokseen, sillä epävirallisten sovellusten toimivuus voi olla huomattavasti epävakaampaa, kuin virallisten (Nguyen-Vu, ym., 2017). Rauhalan (2022) mukaan Android- ja iOs-käyttöjärjestelmää käyttävät älypuhelimet ovat olleet suosionsa johdosta kasvavissa määrin yksityisten hakkerien kohteena. Tätä varten laitteille onkin kehitetty sovelluksia, joiden avulla kolmannen osapuolen on mahdollista saada täysi hallinta älypuhelimesta.

3.6 Kognitiivinen kerros

Kognitiivisella kerroksella tarkoitetaan tässä tutkielmassa älypuhelimen käyttäjää. Aiemmissa alaluvuissa on pohdittu, miten älypuhelimen käyttäjän toiminta vaikuttaa eri kerroksissa ilmeneviin haavoittuvuuksiin. Tässä alaluvussa käydään läpi, miten eri kerroksissa ilmenevät haavoittuvuudet vaikuttavat itse älypuhelimen käyttäjään.

Suoraan fyysiseen kerrokseen kohdistuva hyökkäys tai onnettomuus johtaa lähes poikkeuksetta laitteen hajoamiseen, varastamiseen tai katoamiseen. Tässä tutkielmassa hajoamisella tarkoitetaan sitä, että laite on onnettomuuden jälkeen käyttökelvoton ja vaatii huoltoa. Seurauksena uhkan toteutumiselle laitteen käyttäjä siis menettää laitteen, mutta kaikki älypuhelimen sisältävä data ja informaatio on suojassa. Tämä ei kuitenkaan poissulje sitä, etteikö hyökkääjä pystyisi varastamaan tai muuttamaan kadonneen tai anastetun laitteen informaatiota tai dataa tai esimerkiksi lataamaan laitteeseen haittaohjelmaa, mutta tällöin hyökkäys kohdistuu muihin kerroksiin. Mikäli hyökkäyksen seurauksena älypuhelimen akku syttyy palamaan tai se räjähtää, voi hyökkäys aiheuttaa käyttäjälle myös fyysistä tai psyykkistä haittaa. Käyttäjä voi kärsiä palovammoista tai psykologisesta shokista. Psyykkisiä seurauksia voivat olla ahdistus, levottomuus tai emotionaalinen shokki (Rauhala, 2022). Ensisijaisten vaikutusten lisäksi hyökkäyksellä voi olla merkittäviä toissijaisia vaikutuksia. Esimerkkinä matkustajalento, jolla lähes jokaisella matkustajalla on mukanaan akkukäyttöinen laite. Mikäli matkustajan laitteen akku syttyy palamaan tai akku räjähtää lennon aikana, voi lento häiriintyä. Lisäksi sosiaaliset vaikutteet voivat alentaa käyttäjien luottamusta älypuhelinteknologiaa kohtaan ja täten aiheuttaa tahdottomuutta käyttää älypuhelimia (Rauhala, 2022)

Kuten aiemmin on mainittu, syntaktisen kerroksen haavoittuvuusriskiä kasvattaa esimerkiksi älypuhelimen käyttöjärjestelmärajoitusten purkaminen ja halpatuotetun älypuhelimen käyttö. Jos hyökkäys tapahtuu syntaktisessa kerroksessa, on kaikki mitä älypuhelin sisältää vaarantuneena. Syntaktisen kerroksen hyökkäyksessä hyökkääjän tarkoituksena on saada haltuunsa SuperUser- tai Root-käyttöoikeudet. Näiden käyttöoikeuksien avulla hyökkääjä pystyy liikkumaan hiekkalaatikkomallin rajapintojen yli. Tämä tarkoittaa sitä,

että hyökkääjä pystyy muokkaamaan tai anastamaan laitteessa olevaa dataa, informaatiota ja esimerkiksi sovelluksia. Tämän avulla hyökkääjällä on myös pääsy älypuhelimella kirjauduttuihin pilvipalveluihin. Useat pankki- ja terveyspalvelut vaativat uudelleenkirjautumisen aina, kun palvelu avataan. Mutta koska hyökkääjällä on jo tässä vaiheessa vapaa pääsy käyttäjän laitteelle, voi hyökkääjä asentaa älypuhelimeen esimerkiksi KeyLogger -haittaohjelman, joka tallentaa kaikki käyttäjän tekemät painallukset (Hussain, Al-Haiqi, Zaidan, Kiah, Anuar & Abdulnabi, 2016). Tämän jälkeen hyökkääjä pystyy kirjautumaan esimerkiksi käyttäjän mobiilipankkisovellukseen, sillä erillistä, fyysistä avainlukulistaa ei tarvita.

Semanttisessa kerroksessa hyökkäyksen kohteena on älypuhelimeen tallennettu informaatio. Kun hyökkäys kohdistuu semanttiseen kerrokseen, voidaan esimerkiksi käyttäjän älypuhelimeen tallennettuja dokumentteja kopioida, varastaa tai manipuloida. Jos dokumentti sisältää käyttäjän tai jonkun muun henkilön henkilötietoja, voi dokumentin anastus johtaa identiteettivarkauteen. Myös työpuhelimeen kohdistuessa hyökkäyksen seuraukset voivat olla vakavat.

Palvelukerrokseen suuntautuva hyökkäys on lähtökohtaisesti laajamittainen ja sen seuraukset kohdistuvat useampaan käyttäjään samanaikaisesti, sillä hyökkäys suuntautuu palveluntarjoajaan. Esimerkiksi WhatsApp -viestintäpalveluun kohdistuva palvelunestohyökkäys voi estää sovelluksen käytön pidemmäksikin aikaa. Mikäli käyttäjällä ei ole käytössään muita viestintäkanavia ja käyttäjän liittymä ei sisällä puheluita eikä tekstiviestejä, on yhteydenpito käyttäjän osalta puhelimitse täysin estynyt.

4 EMPIIRINEN TUTKIMUS

Tässä luvussa käsitellään tarkemmin tutkielman tutkimusmenetelmät, tutkimusongelmat, tutkimuskysymykset ja tutkimuksen lähtökohdat. Tutkimuksen empiirinen osa suoritettiin kvalitatiivisena sisällönanalyysinä, jonka tarkoitus on olla kuvaileva. Kuvailevan tutkimuksen tarkoituksena on ”Esittää tarkkoja kuvauksia henkilöistä, tapahtumista tai tilanteista” (Hirsjärvi, Remes & Sajavaara, 2007). Aineiston keruu suoritettiin haastattelemalla työssä käyviä älypuhelimien käyttäjiä, joilla on käytössään työpuhelin. Tutkimuksen perusjoukko rajattiin edellä mainitulla tavalla, jotta tutkimustuloksista voidaan tarkastella anonyymisti mahdollisia poikkeavuuksia eri organisaatioiden mobiililaitteisiin kohdistuvien tietoturvakäytänteiden välillä. Lisäksi tutkimustuloksista pyrittiin myös selvittämään, vaikuttaako haastateltavan työpaikan turvallisuuskäytänteet henkilökohtaisen älypuhelimen käyttämiseen.

4.1 Tutkimuskysymykset

Tämän tutkielman päätutkimuskysymys on:

- Minkä tasoinen on älypuhelinkäyttäjien tietoturvatuntemus?

Lisäksi tutkimuksessa käytetään kahta apututkimuskysymystä, jotka täydentävät päätutkimuskysymystä:

- Millä osa-alueilla älypuhelinkäyttäjien toimet aiheuttavat eniten uhkia?
- Millä osa-alueilla älypuhelinkäyttäjien toimet aiheuttavat vähiten uhkia?

Tässä tutkielmassa laitteen ja itsensä suojaamista älypuhelimiin kohdistuvien uhkien varalta tarkoittaa tietoturvasovellusten käyttöä, esimerkiksi VPN-yhteyksiä, virus- ja haittaohjelmaturvaa, identiteettisuojaa, nettisuojaa ja salasanaholveja. Lisäksi tällä tarkoitetaan käyttäjän niin kutsuttuja perustoimintamalleja älypuhelimen kanssa. Tällaisia malleja ovat esimerkiksi turvallisen näyttölukituskoodin käyttö älypuhelimessa, puhelimen automaattilukituksen käyttö, salasanojen ja maksutietojen säilyttäminen turvallisesti älypuhelimessa. Kolmantena suojaavana tekijänä voidaan pitää käyttäjän omaa huolellisuutta älypuhelinta käytettäessä. Esimerkiksi julkisilla paikoilla älypuhelinta käytettäessä salasanojen, näyttölukituskoodien ja arkaluontoisen tiedon käyttö niin, ettei ympärillä olevat ihmiset pääse niitä katsomaan (engl. shoulder surfing) (Bošnjak & Brumen, 2019) ja sitä, että älypuhelimen käyttäjä säilyttää laitetta niin, että sen varastetuksi tulemisen mahdollisuus on mahdollisimman pieni. Lisäksi käyttäjän huolellisuutta mittaavaksi tekijäksi voidaan laskea piittaamattomuus älypuhelimien kohdalla hyväksymättömiä tai laittomia käytänteitä kohtaan. Tällaisia ovat esimerkiksi väärennetyt älypuhelimet, älypuhelimien varaosat tai lisälaitteet, juuritason oikeuksien hankkiminen käyttäjälle roottaamalla tai jailbreakaamalla älypuhelin tai hankkimalla sovelluksia tuntemattomista lähteistä sovelluskappojen ulkopuolelta. Koska tutkimuksen kohteena on kannettava mobiililaite, on myös relevanttia kysyä, miten käyttäjät suojaavat älypuhelimiaan fyysisiltä vaurioilta. Fyysisiltä vaurioilta älypuhelinta voi suojata erilaisilla suojakuorilla tai näyttösuojalla. Lisäksi huolellisuus älypuhelinta käytettäessä otettiin tutkimuksessa huomioon.

4.2 Aineiston kerääminen

Tutkimus toteutettiin kvalitatiivisena, eli laadullisena, sisällönanalyysitutkimuksena. Koska kyseessä on laadullinen tutkimus, tutkimuksen lähtökohtana ja tarkoituksena on kuvata todellista elämää mahdollisimman tarkasti (Hirsjärvi, ym., 2007). Laadullinen tutkimus keskittyy yleisesti yksittäisiin tapauksiin ja ihmisten näkemyksiin. Juuti ja Puusa (2020) korostavat, että tässä tutkimusmenetelmässä käytetään usein ihmisiä tiedonkeruun välineinä luonnollisissa tilanteissa, joka mahdollistaa osallistujien näkemysten ja ajatusten esiintuomisen. Yleisimmät aineistonkeruumenetelmät laadullista tutkimusta tehdessä ovat kysely, haastattelu, erilaisista dokumenteista koottu tieto ja havainnointi. (Sarajärvi & Tuomi, 2017; Juuti & Puusa, 2020).

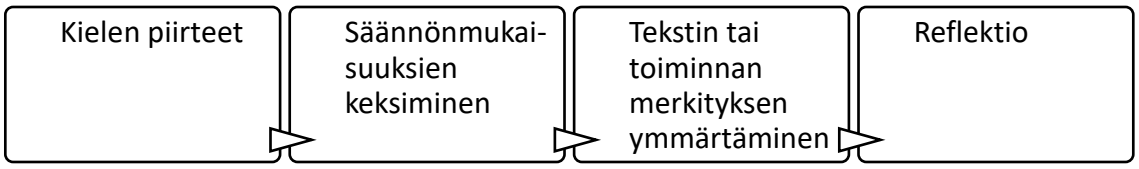
Tässä tutkimuksessa tiedonkeruumenetelmänä käytettiin puolistrukturoitua yksilöhaastattelua. Puolistrukturoitu ja strukturoitu haastattelu eroavat toisistaan siinä, että strukturoidun haastattelun tulee seurata kysymysluetteloa tarkasti, kun taas puolistrukturoidussa haastattelussa on käytössä ennalta laadittu kysymysrunko, johon haastateltava antaa avoimia vastauksia (Hirsjärvi, ym., 2007). Tutkimuksessa käytetty kysymysrunko sisälsi

41 kysymystä. Suuri osa kysymyksistä olisi sopinut myös strukturoituun haastatteluun, sillä niihin oli mahdollista vastata kyllä tai ei, vastausvaihtoehdot oli annettu likertin asteikon mukaan tai kysymyksen vastaukset sisälsivät haastateltavien kesken lopulta sellaisia yhtäläisyyksiä, että ne olisi voitu luokitella omiksi vastausvaihtoehdoikseen avoimen kysymyksen sijaan. Kysymysrunko on nähtävillä ensimmäisessä liitteessä (liite 1.)

Laadullisen tutkimuksen aineiston määrä vaihtelee tutkimuksen tarkoituksesta ja tavoitteista riippuen. Juuti ja Puusa (2020) huomauttavat, että esimerkiksi haastateltavien määrä määräytyy tutkimuksen tarpeiden perusteella. Laadullinen tutkimus ei pyri tilastollisiin yleistyksiin, vaan sen tavoitteena on tapahtumien ja ilmiöiden kuvaaminen, teoreettisesti mielekkään tulkinnan antaminen tai toiminnan ymmärtäminen (Sarajärvi & Tuomi, 2017).

Haastattelu on joustava tutkimusmenetelmä, joka soveltuu erilaisiin tutkimustarkoituksiin. Hirsjärvi ja Hurme (2000) selittävät, että haastattelut mahdollistavat vuorovaikutuksen tutkittavan kanssa ja antavat tutkijalle mahdollisuuden suunnata tiedonkeruuta tilanteen mukaan. Haastattelu voi olla hyödyllinen erityisesti silloin, kun tutkimuskohde on vähän tunnettu, ennakoimattomia vastauksia odotetaan tai tutkimuksen aihe on monimutkainen ja moniulotteinen (Hirsjärvi & Hurme, 2000). Puolistrukturoiduissa haastatteluissa on myös huonot puolensa. Menetelmänä puolistrukturoiduissa haastatteluissa saattaa kertyä huomattavasti tutkimuksen kannalta epäolennaista materiaalia (Hirsjärvi & Hurme, 2000). Tämä seikka oli huomattavissa myös tässä tutkimuksessa.

Hirsjärvi, ym. (2007) viittaavat kirjassaan Teschiin (1992), jonka mukaan kvalitatiivisen tutkimuksen lähestymistavat voidaan jakaa neljään osaan (kuvio 5).



KUVIO 5 Kvalitatiivisen tutkimuksen intressit

Tyypittely on esitelty luettelon sijaan ulottuvuutena, jossa tutkimustyyppi on vasemmassa laidassa strukturoidumpi ja se muuttuu oikealle siirryttäessä kokonaisvaltaisemmaksi ja vähemmän strukturoiduksi (Hirsjärvi, ym., 2007). Nämä neljä tutkimustyyppien päätyyppiä voidaan jaotella perinteisesti vielä 26 eri kvalitatiivisen tutkimuksen lajiin. Näiden lisäksi jokainen tutkija tekee tutkimuksensa omalla tavallaan, jolloin metodien määrä vain kasvaa (Hirsjärvi, ym., 2007). Tutkimustyyppinä sisällönanalyysissä ollaan tässä tutkimuksessa kiinnostuneita haastattelun sisällöstä kommunikaationa, joka tarkoittaa sitä, että tutkimuksessa ollaan kiinnostuneita kielen piirteistä (Hirsjärvi, ym., 2007). Kuten kuviossa 5 todetaan, kielen piirteitä tutkiessa haastattelun rakenne on hyvin strukturoitu. Mutta kuten monissa muissakin tutkimuksissa, ei tämäkään

tutkimus ole täysin yksiselitteinen, sillä haastattelut sisältävät myös keskustelua ja puolistrukturoituja kysymyksiä.

4.3 Haastatteluiden toteuttaminen

Tutkimuksen aineisto kerättiin yksilöhaastatteluina, joita toteutettiin kaiken kaikkiaan 21 kappaletta. Kolme ensimmäistä haastattelua toimivat koehaastatteluina, joiden tarkoituksena oli kerätä palautetta haastateltavilta ja mitata haastatteluun käytettyä aikaa. Koehaastatteluiden keskipituus oli noin 24 minuutta. Haastattelun kysymyksiä muotoiltiin uudelleen ensimmäisen koehaastattelun jälkeen ja toisen koehaastattelun jälkeen kysymyksiä järjesteltiin uudelleen. Kolmannen koehaastattelun jälkeen tutkija ei saanut palautetta haastateltavalta, eikä huomannut itsekään mitään suurempaa kehitettävää. Koehaastattelut suoritettiin 25.-27.8.2023, jonka jälkeen kysymysrunko todettiin valmiiksi varsinaisia haastatteluja varten. Varsinaisia haastatteluja toteutettiin 18 kappaletta aikana 28.8.-7.9.2023. Haastattelut kestivät keskimäärin noin 21 minuuttia. Lyhin haastattelu oli pituudeltaan noin 16 minuuttia ja pisin haastattelu oli pituudeltaan noin 32 minuuttia. Koehaastatteluista saatujen tulosten perusteella, haastattelut olivat hieman arvioitua lyhyempiä.

Maantieteellisten rajoitteitten takia, varsinaisista haastatteluista yhteensä 12 kappaletta suoritettiin etänä Microsoft Teamsin välityksellä. Heti haastatteluvaiheen alussa selvisi, ettei kaikilla haastateltavilla ole mahdollisuutta käyttää kameraa haastattelun aikana, joten kaikki etähaastattelut päätettiin suorittaa pelkän äänen välityksellä. Hirsjärvi & Hurme (2000) mainitsevat, että puhelinhaastattelut toimivat hyvin melko strukturoiduissa haastatteluissa ja sillä on mahdollista saada laaja otanta lyhyessäkin ajassa. Otantojen määrä oli ajoittain suurta tässäkin tutkimuksessa, sillä haastatteluita oli parhaimmillaan neljä yhden päivän aikana. Puhelinhaastattelussa on kuitenkin myös huonot puolensa, sillä puhelinhaastattelun aikana tutkija ei pysty saamaan niitä näkyviä vihjeitä, joita normaalisti kasvotusten saisi. Tämä voi johtaa esimerkiksi siihen, ettei haastattelija voi olla täysin varma ymmärsikö haastateltava kysymyksen oikein (Hirsjärvi & Hurme, 2000).

Puhelinhaastattelua tehdessä on myös tärkeää lähestyä haastateltavia erityisen asiallisesti ja antaa aikaa haastattelun toteuttamiselle. Tämä antaa haastateltavalle mahdollisuuden varmistua haastattelijan luotettavuudesta ja aikaa perehtyä haastattelun aiheeseen (Hirsjärvi & Hurme, 2000). Tämän tutkimuksen tutkija oli jo ennalta tuttu haastatteluihin osallistuville, joten luottamuksen kanssa ei ollut erityistä ongelmaa. Sovittaessa haastatteluita, haastateltaville annettiin mahdollisuus varata haastatteluaika yli kymmenen päivän päähän, mutta suurin osa haastateltavista halusi haastattelun samana päivänä tai viimeistään kolmen päivän päästä ensimmäisestä kontaktista. Haastatteluista kuusi kappaletta suoritettiin kasvotusten, joko haastattelijan tai haastateltavan asunnolla tilassa, johon muilla ei ollut pääsyä eikä mahdollisuutta kuulla haastattelua. Jotta asetelma kaikkiin haastatteluihin pysyisi

mahdollisimman samanlaisena, kasvokkain tehdyissä haastatteluissa pyrittiin mahdollisuuksien mukaan jättämään haastateltavien ilmeet ja eleet huomiotta. Haastattelutilanteet etenivät seuraavasti:

1. Tutkija esittäytyy ja kertoo tutkimuksen aiheen sekä painottaa, että kyseessä on Pro Gradu -tutkielma. Tutkija tarkastaa haastateltavan ennalta lähettämän esitietolomakkeen (liite 2.) ja varmistaa, että kaikki esitietolomakkeessa esitetyt kysymykset on ymmärretty oikein. Tutkija ilmoittaa tutkimuksen olevan täysin anonyymi ja kertoo että esitietolomakkeen (liite 2.) tietoja käytetään ainoastaan tutkimustarkoitukseen. Tutkija ilmoittaa, että tutkimushaastattelu on täysin vapaaehtoinen, eikä haastatteluun osallistumisesta ole tarjolla palkkiota. Mikäli haastateltava ei ollut täyttänyt esitietolomaketta (liite 2.), lomake täytetään yhdessä ennen nauhoituksen aloittamista. Haastateltavalle kerrotaan, että vastausten tulee olla mahdollisimman rehellisiä, eikä oikeita tai vääriä vastauksia ole. Haastateltavalta kysytään lupaa haastattelun nauhoitukseen ja automaattilitterointiin. Luvan saatua haastateltavalle ilmoitetaan, että nauhoitukset tuhotaan heti, kun litteroinnit on oikoluettu ja litteroinnit tuhotaan, kun tutkimus on saatu valmiiksi.
2. Tutkija käy läpi tutkimuksen lähtökohdat ja esittelee kybertoimintaympäristön hierarkkisen rakennemallin eri kerrokset haastateltavalle. Haastateltavalle tarkennetaan, että haastateltavan ei tarvitse olla tietoinen kybertoimintaympäristön hierarkkisesta rakennemallista ja että esittely tehtiin vain siksi, että haastateltavalle annetaan mahdollisuus ymmärtää tutkimuksen lähtökohdat mahdollisimman hyvin. Tutkija varmistaa vielä haastateltavalta, että hänellä on käytössään työpuhelin, joka määritellään älypuhelimeksi. Haastateltavaksi hyväksytään myös henkilöt, joilla on siviili- ja työpuhelin yhdistettynä samaan laitteeseen.
3. Haastattelun kysymykset on jaettu valmiiksi omiin teemoihinsa kybertoimintaympäristön hierarkkisen rakennemallin kerrosten mukaan. Kysymykset on jaoteltu lähtökohtaisesti niin, että kysymys, joka liittyy tiettyyn kerrokseen, liittyy myös uhkaan tai haavoittuvuuteen, joka on reitti kyseisen kerroksen kautta älypuhelimeen. Haastattelun teemat etenevät järjestyksessä kognitiivinen kerros, palvelukerros, semanttinen kerros, syntaktinen kerros ja fyysinen kerros. Teemasta toiseen siirryttäessä haastateltavalle esitellään, mitä kukin kerros pitää sisällään. Kybertoimintaympäristön hierarkkinen rakennemalli älypuhelinkontekstissa on esiteltynä tarkemmin luvussa 2.2. Kysymysten edetessä, mikäli vastauksesta on selkeästi huomattavissa, että haastateltava ei ymmärtänyt kysymystä, tutkija esittää tarkentavia kysymyksiä.

4. Lopuksi tutkija kysyy, tuleeko haastateltavalle mieleen mitään lisättävää ja onko haastattelusta noussut esille kysymyksiä. Lisäksi haastateltavalta pyydetään suullinen palaute haastattelun jälkeen. Tämän jälkeen haastattelija lopettaa nauhoituksen, automaattilitteroinnin ja kiittää haastateltavaa osallistumisesta haastatteluun.

Ennen etähaastatteluita, tutkija lähetti haastateltaville sähköpostitse kutsun Teams -kokoukseen, jonka ajankohta oli sovittu jo ensimmäisen yhteydenoton aikana. Haastattelut tallennettiin hyödyntäen Microsoft Teamsin ”Nauhoita ja litteroi” työkalua. Samoin kasvotusten toteutetut haastattelut sovittiin ensimmäisen yhteydenoton aikana. Myös kasvotusten toteutetut haastattelut nauhoitettiin Teamsin avulla, jolloin kannettava tietokone asetettiin haastattelijan ja haastateltavan väliin, sopivalle etäisyydelle.

Aineisto rajattiin ja tutkittavat valittiin niin, että otanta erilaisista älypuhelinkäyttäjistä olisi mahdollisimman laaja. Tutkittavat valittiin käyttäen harkinnanvaraista otantaa (Patton, 1990). Jotta tutkimuksesta saadaan mahdollisimman monipuolinen kuva, tulee tutkittavien koostua mahdollisimman erilaisista lähteistä (Myers & Newman, 2007). Kutsu haastatteluun lähetettiin tutkijan jo tuntemille ihmisille, jonka avulla tutkimukseen saatiin helpommin eri ikäisiä ja eri aloilla työskenteleviä henkilöitä, jonka tarkoituksena oli saada mahdollisimman monipuolinen kuva otannasta. Jotta harkinnanvarainen otanta toimisi mahdollisimman tehokkaasti, tulee tutkittavien tapausten, tässä tapauksessa haastateltavien, sisältää mahdollisimman paljon tietoa ja tapausten tulee tuoda lisäarvoa tutkimukselle (Patton, 1990). Jokaisen osallistujan tiedettiin olevan työssäkäyvä älypuhelimen käyttäjä, jolla oli käytössään älypuhelin myös työpuhelimenaan. Monipuolisuutta vastauksiin saatiin esimerkiksi vastaajien ammatin ja iän perusteella. Näiden lisäksi tutkijalla oli hieman ennakkotietoa joidenkin haastateltavien lähtökohdista älypuhelimen käyttäjänä. Tällä tarkoitetaan sitä, että käyttääkö haastateltava älypuhelintaan vain välttämättömien asioiden ja kommunikaation hoitamiseen, onko haastateltavalla useampiakin työtä tai vapaa-aikaa helpottavia sovelluksia tai toimintoja käytössään älypuhelimessa vai onko haastateltavalla syvempääkin kokemusta älypuhelimen toiminnoista, kuten sovelluskehityksestä tai vaikkapa root-tason oikeuksien hallinnasta. Näitä asioita ei kuitenkaan itse haastattelussa tai esitietolomakkeessa kysytty.

Tutkimukseen osallistuminen oli täysin vapaaehtoista. Tutkija oli yhteydessä 21 henkilöön, joista 18 suostui vapaaehtoiseksi haastatteluun. Kaikki haastatteluun suostuneet haastateltiin ja kaikkien haastateltavien vastaukset olivat valideja, joten jokainen vastaus otettiin huomioon tutkimusta tehdessä. Haastateltavien ikäjakauma oli haastattelua tehdessä 26–64 vuotta. Haastateltavien keski-ikä oli 40,3 vuotta, mediaani 32 vuotta ja moodi 31 vuotta. Haastateltavien sukupuolta ei kysytty, sillä tätä ei pidetty tutkimuksen kannalta merkittävänä tietona. Haastateltavista kukaan ei ollut mobiililaiteasiantuntija ja haastateltavista kaksi oli joko kyberturva- tai tietoturva-asiantuntijoita. Tavoitteena oli toteuttaa vähintään 12 haastattelua, joka täyttyi huomattavasti.

Haastatteluita oli tarkoitus kerätä niin pitkään, kunnes informaatiota on kerätty tarpeeksi ja kysymysten vastauksissa rupeaa esiintymään selkeitä samankaltaisuuksia. Vastauksissa oli havaittavissa samankaltaisuuksia kymmenennen haastattelun valmistuttua, jonka jälkeen uusia haastatteluaikoja ei enää varattu. Ensimmäiseen taulukkoon (taulukko 1) on listattu haastateltavien itsearviot omasta tietoturvatuntemuksesta sekä teknisestä osaamisesta älypuhelimen käyttöön liittyen. Toiseen taulukkoon (taulukko 2) on listattu tietoja haastateltavien älypuhelimista ja älypuhelimien käyttöhistoriasta.

TAULUKKO 1 Haastateltavien itsearviot

Tunniste	Tietoturvatuntemus	Älypuhelimien tekninen tuntemus
H1	Kiitettävä	Kiitettävä
H2	Kiitettävä	Kiitettävä
H3	Hyvä	Erinomainen
H4	Tyydyttävä	Hyvä
H5	Kiitettävä	Kiitettävä
H6	Hyvä	Hyvä
H7	Hyvä	Hyvä
H8	Hyvä	Tyydyttävä
H9	Hyvä	Kiitettävä
H10	Hyvä	Hyvä
H11	Hyvä	Hyvä
H12	Kiitettävä	Kiitettävä
H13	Tyydyttävä	Tyydyttävä
H14	Tyydyttävä	Hyvä
H15	Tyydyttävä	Hyvä
H16	Tyydyttävä	Tyydyttävä
H17	Hyvä	Kiitettävä
H18	Hyvä	Hyvä

TAULUKKO 2 Haastateltavien älypuhelimien käyttöhistoria

Tunniste	Henkilökohtainen älypuhelin	Työpuhelin	Ensimmäinen älypuhelin	Älypuhelimien määrä
H1	iOs, iPhone	Android, Samsung	2011	6
H2	Android, Samsung	Android, Samsung	2016	5
H3	iOs, iPhone	Android, Samsung	2010	20
H4	Android, Samsung	Android, Samsung	2013	5
H5	Android, Samsung	Android, Samsung	2010	9
H6	Android, Samsung	iOs, iPhone	2011	7
H7	iOs, iPhone	iOs, iPhone	2001	20
H8	iOs,iPhone	Android, Samsung	2014	5
H9	Android, Samsung	iOs, iPhone	2011	9
H10	iOs, iPhone	iOs, iPhone	2006	9
H11	iOs, iPhone	Android, Samsung	2008	8
H12	Android, Samsung	iOs, iPhone	2008	6
H13	iOs, iPhone	iOs, iPhone	2014	3
H14	iOs, iPhone	Android, Samsung	2001	30
H15	iOs, iPhone	Android, Nokia	2008	6
H16	Android, Nokia	Android, Samsung	2012	5
H17	iOs, iPhone	iOs, iPhone	2011	8
H18	Android, OnePlus	Android, OnePlus	2007	17

Haastateltavista seitsemällä oli käytössä työsuhdepuhelin, joka tarkoittaa sitä, että samassa puhelimessa on työpuhelin sekä henkilökohtainen puhelin. Tutkimuksessa älypuhelin on määritelty laitteeksi, jota voidaan kantaa mukana ja siinä on normaalien puhelinominaisuuksien lisäksi internetselain ja siihen on mahdollista ladata erillisiä sovelluksia. Haastateltavilta, jotka ilmoittivat hankkineensa ensimmäisen älypuhelimensa vuonna 2001, varmistettiin erikseen, että kyseessä todella on älypuhelin. Molemmissa tapauksissa oli kyseessä Nokia

9210 Communicator Symbian OS käyttöjärjestelmällä, joka täyttää vaadittavat kriteerit.

4.4 Aineiston purkaminen

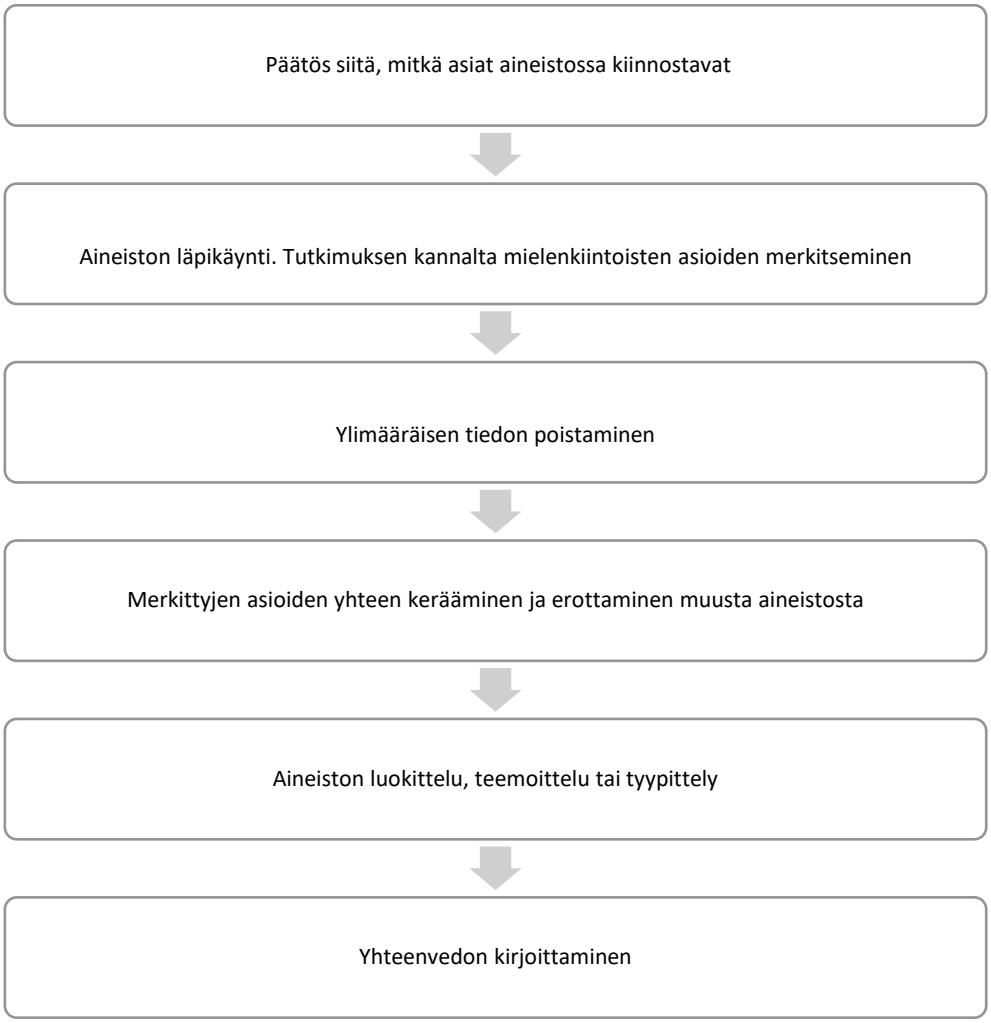
Kerätyn aineiston purkaminen aloitettiin välittömästi ensimmäisen haastattelun jälkeen. Aineistoa purkaessa, ensimmäisenä kirjoitettiin puhtaaksi Microsoft Teamsin luoma automaattilitterointi kuuntelemalla tallenteet läpi ja vertaamalla automaattilitteroinnin tuottamaa transkriptiota keskenään. Automaattinen litterointi toi huomattavan hyödyn aineiston käsittelyyn ja säästi merkittävästi aikaa, vaikkakin suomen kielellä toteutetuissa haastatteluissa esiintyi myös huomattavia virheitä. Erityisesti haastatteluissa esiintyvät pitkät puheenvuorot ja runsas täytesanojen käyttö (niin niin, tota tota tota, yms.) saattoi vaatia sen, että koko vastaus piti kirjoittaa uudelleen. Haastattelun kysymykset oli laadittu niin, että vain neljä kysymystä muotoutui sen mukaan, miten edelliseen kysymykseen oli vastattu. Näissäkin tapauksissa kysymys joko esitettiin tai jätettiin välistä. Tästä syystä litteroidessa tutkijan esittämät kysymykset merkattiin aina samalla tavalla, vaikka sanajärjestys saattoi hieman vaihdella. Ennen kysymyksen puhtaaksi kirjoittamista kuitenkin arvioitiin tarkasti, olisiko sanajärjestyksen muuttuminen voinut vaikuttaa kysymyksen ymmärrettävyyteen. Kysymyksen esittämisen ja siihen saadun vastauksen perusteella, näin ei kuitenkaan yhdessäkään tapauksessa ollut. Mikäli kysymyksiä oli tarpeen tarkentaa tai kysymys suuntautui keskusteluksi, litterointi suoritettiin mahdollisimman sanatarkasti.

Haastateltavien vastaukset litteroitiin aina mahdollisimman tarkkaan. Tietyt täytesanat jätettiin litteroinnissa huomioitta ja mikäli haastateltava kertoi tutkimuksen kannalta epärelevantin ja pitkän selostuksen, litteroitiin sen tilalle ainoastaan selite, mistä asiasta keskustelua käytiin. Selite merkattiin sulkuihin esimerkiksi näin: (kertoo tarinaa hyvästä salasanasta, joka on joskus ollut käytössä). Hirsjärvi & Hurmeen (2000) mukaan litterointi kannattaa tehdä mahdollisimman pian haastattelun jälkeen, sillä haastattelussa ilmenneet tapahtumat ja siitä tehtävät johtopäätökset ovat vielä haastattelijan tuoreessa muistissa. Vaikka haastattelut olivatkin puolistrukturoituja ja esimerkiksi haastateltavien äänenpainoon, taukoihin ja eleisiin ei juurikaan otettu kantaa, tätä neuvoa pyrittiin noudattamaan koko haastattelukierroksen ajan. Haastattelut litteroitiin aina joko samana tai viimeistään seuraavana päivänä. Tapauksissa, joissa haastatteluja oli kertynyt yli kaksi kappaletta yhden päivän ajalle, vähintään yksi puhtaaksi kirjoitus jouduttiin tekemään seuraavan päivän aikana. Haastattelijan esittämät kysymykset ja muut puheenvuorot merkattiin litterointiin laittamalla tunnus K: (kysymys) puheenvuoron eteen ja haastattelijan puheenvuorot merkattiin tunnuksella V: (vastaus). Litteroinnista kertyi aineistoa yhteensä noin 200 sivua ja jokainen litterointi tallennettiin omana dokumenttinaan.

4.5 Sisällönanalyysi

Tuomin ja Saarijärven (2018) mukaan sisällönanalyysillä tarkoitetaan perusanalyysimenetelmää, jota voidaan käyttää kaikissa laadullisen tutkimuksen perinteissä. Sisällönanalyysi voidaan tulkita kahdella eri tapaa. Sisällönanalyysi voi olla joko oma yksittäinen metodinsa, tai sitä voidaan pitää erilaisiin analyysikokonaisuuksiin liitettävänä teoreettisena kehyksenä (Tuomi & Saarijärvi, 2018). Tuomi ja Saarijärvi (2018) mainitsevat, että useimmat laadullisen tutkimuksen analyysimenetelmät pohjautuvat jollakin tavalla sisällönanalyysiin, jos kyseessä on nähtyjen, kuultujen tai kirjoitettujen sisältöjen analyysi teoreettisena kehyksenä. Näin tarkastellen, sisällönanalyysi ei ole ainoastaan laadullisessa tutkimuksessa käytettävä analyysimenetelmä (Tuomi & Saarijärvi, 2018). Tätä näkemystä vahvistaa myös Hirsjärvi, ym. (2007) maininta siitä, että sisällönanalyysissä tutkimushaastattelun kysymykset ovat laadullisen menetelmän metodeista strukturoiduimpia, jota voidaan taas pitää karkeasti lähimpänä määrällistä tutkimusta.

Ennen analyysivaihetta, haastattelija pyrkii karsimaan ylimääräisen tiedon pois litteroidusta aineistosta ja korostaa tutkimuksen kannalta relevantin aineiston, toisin sanoen haastattelija tulkitsee aineistoa selventämällä ja rakentamalla (Hirsjärvi & Hurme, 2000). Tuomi ja Saarijärvi (2018) mainitsevat tutkija Timo Laineen laatiman rungon, joka kuvaa laadullisen tutkimuksen analyysin etenemistä (KUVIO 6).



KUVIO 6 Laadullisen tutkimuksen analyysin eteneminen (Tuomi & Saarijärvi, 2018).

Tässä tutkimuksessa aineistossa, eli litteroiduissa haastatteluissa, esiintyvien mielenkiintoisten asioiden päättäminen tapahtui verrattain helposti, sillä tarkoituksena oli selvittää, millaiset haastateltavien toimintatavat aiheuttavat uhkia älypuhelimen turvallisuudelle ja millaiset toimintatavat taas parantavat laitteen turvallisuutta. Haastattelun kysymykset oli aseteltu niin, että tutkimuksen kannalta relevantti tieto oli helposti tunnistettavissa, jolloin aineistoa läpikäydessä epäoleellinen aineisto pystyttiin karsimaan pois. Samalla merkitty tieto luokiteltiin omiin alaluokkiinsa, jonka jälkeen vastaukset luokiteltiin yläluokkiin, eli onko vaikutus älypuhelimen turvallisuuteen positiivinen, neutraali vai negatiivinen. Analyysissä käytettiin siis yhdistelyä, jossa litteroidusta aineistosta etsittiin tiettyjä yhdenmukaisuuksia sekä poikkeavuuksia (Hirsjärvi & Hurme, 2000). Tuomi ja Saarijärvi (2018) mainitsevat, että luokittelu on aineiston järjestämisen muodoista yksinkertaisin ja että sitä pidetään määrällisen tutkimuksen analyysina sisällön teemoin. Tutkimuksen aineiston järjestäminen olisi ollut mahdollista myös käyttämällä teemoittelua. Teemoittelu voi olla samankaltaista kuin luokittelu, sillä eroavaisuudella että teemoittelussa painotetaan kussakin teemassa sanottua

asiaa (Tuomi & Saarijärvi, 2018). Haastattelut sisälsivät kuitenkin kysymyksiä, joihin oli mahdollista vastata kyllä tai ei, sekä kysymyksiä, joihin vastattiin arvio yhden ja viiden väliltä, jolloin teemoittelu ei olisi ollut mielekästä. Vastaukset, jotka sisälsivät selityksen haastateltavan toiminnalle ja jotka olivat tutkimuksen kannalta mielekkäitä, merkattiin erikseen ylös ja niihin paneudutaan erikseen luvussa 5.

Jo haastatteluvaiheessa kysymykset oli jaoteltu eri kategorioihin. Kategoriat olivat samat kuin kybertoimintaympäristön hierarkkisessa rakennemallissa, eli kognitiivinen kerros, palvelukerros, semanttinen kerros, syntaktinen kerros ja fyysinen kerros (Lehto, ym., 2019). Jaottelun tarkoituksena oli kohdentaa kysymys kerrokseen, johon haastateltavan toiminta vaikuttaa suorimmin. Toisin sanoen aiheuttaako toiminta haavoittuvuuksia tai parantaako se kerroksen turvallisuutta, tarkkaillessa uhkan toteutumisen mahdollisuutta niin, että reitti älypuhelimeen on kyseinen kerros. Osa haastattelussa esitetyistä kysymyksistä olisi voinut kohdistua useampaankin kerrokseen, mutta kysymykset pyrittiin kategorisoimaan sitä parhaiten kuvaamalla tavalla.

5 TULOKSET

Tässä luvussa käsitellään tutkimuksessa tehtyjen haastatteluiden tulokset. Tutkimuksessa käytettiin viitekehyksenä viisikerroksista kybertoimintaympäristön hierarkkista rakennemallia. Tulokset on jaoteltu kybertoimintaympäristön hierarkkisen rakennemallin kerrosten mukaan, eli alaluvut on nimetty kunkin kerroksen perusteella. Kybertoimintaympäristön hierarkkisen rakennemallin kerrokset ovat kognitiivinen kerros, palvelukerros, semanttinen kerros, syntaktinen kerros ja fyysinen kerros (Lehto, ym., 2019). Tulokset on luokiteltu sen mukaan, vaikuttaako älypuhelimen käyttäjän toiminta kerroksen turvallisuuteen positiivisesti, neutraalisti vai negatiivisesti. Vaikutuksella kerroksen turvallisuuteen tarkoitetaan tässä tapauksessa mahdollisen uhkan suoraa kohdistumista kyseiseen kerrokseen, eli tilannetta, jolloin esitelty kerros on hyökkääjän käyttämä reitti älypuhelimeen.

5.1 Kognitiivinen kerros

Kognitiivisella kerroksella tarkoitetaan älypuhelimen käyttäjää. Tulosten sisällyttäminen kognitiivisen kerroksen alle oli hankalaa, sillä tutkimuksen luonteen mukaan hierarkkisen rakennemallin jokaisen kerroksen haavoittuvuudet tai suojaavat tekijät ovat kytköksissä itse käyttäjän toimintoihin, tavalla tai toisella.

5.1.1 Älypuhelimiin kohdistuvat tietoturvaloukkaukset

Haastateltavilta kysyttiin, ovatko he ikinä joutuneet älypuhelimeen kohdistuvan tietoturvaloukkauksen uhriksi. Kysymyksessä tarkennettiin, että loukkaus tulisi pystyä yhdistämään juuri älypuhelimen käyttöön. Tämän jälkeen haastateltaville esitettiin neljä erilaista tietoturvaloukkausta ja heiltä kysyttiin, miten he reagoisivat, jos tällainen tilanne sattuisi omalle kohdalle. 18 haastateltavasta 15 sanoi, ettei ole joutunut älypuhelimeen kohdistuvan tietoturvaloukkauksen uhriksi. Haastateltavista kaksi oli avannut sosiaalisessa mediassa haitallisen

linkin, jonka seurauksena käyttäjän oma profiili alkoi levittämään samaa linkkiä haastateltavan kontakteille. Reaktiona tapahtuneelle, kumpikin haastateltava poisti saastuneen profiilin ja loi uuden profiilin sosiaalisen median palveluun. Tapaukset olisivat kuitenkin olleet mahdollisia myös muilla laitteilla kuin älypuhelimella. Yksi haastateltavista kertoi, että hänen salasanansa oli vuotanut kolmannelle osapuolelle:

> H7: Tuleehan mulle jatkuvasti, että mun yks tunnussana, että yksi käyttämäni tunnussana on joutunut vääriin käsiin, joo. Eli korjaan, se tulee muistutuksena. Mä käytän sitä tunnussanaa edelleen. Ohitan sen huomautuksen, että kannattais vaihtaa, koska se on niin hyvä salasana, että en viitsi vaihtaa sitä.

Kaikissa tietovuototapauksissa, etenkin salasanadumpeissa, tulisi vaihtaa vähintäänkin käyttäjätunnukseen liitetty salasana. Reagoimattomuus tilanteeseen viestii tiedonpuutteesta tai tietynlaisesta välinpitämättömyydestä. Reagointi tietovuotoihin on myös yleisempää alle 54-vuotiailla ikäluokilla (Mayer, Zou, Schaub, & Aviv, 2021).

Tietoturvaloukkauksiin ja niihin liittyviin reagointitapoihin liittyvissä kysymyksissä oli havaittavissa huomattavia samankaltaisuuksia. Jokaisessa skenaariossa vähintään kolmasosa haastateltavista poistaisi sekä käyttäjätilin että koko sovelluksen. Tilanteissa, joissa sovellus on sisältänyt vakavia, jo hyödynnettyjä haavoittuvuuksia tai laitteeseen asennettu sovellus olisi tarkoituksella haitallinen, yli puolet haastateltavista poistaisi sovelluksen ja palauttaisi laitteen tehdasasetuksille. Näissä tilanteissa yli kolmasosa haastateltavista vaihtaisi tilanteen mukaan myös muiden palveluiden salasanoja. Haastateltavilla oli hyvä käsitys omista teknisistä taidoistaan. Poislukien tilanteen, jossa tuottaja on laiminlyönyt tuotteen tietoturvaa, kaikissa skenaarioissa haastateltavat etsisivät lisätietoa verkosta, konsultoisivat asiantuntijaa tai viranomaista taikka antaisivat oman työpaikan teknisen tuen hoitaa tilanteen. Tilanteessa, jossa tuottaja olisi laiminlyönyt tuotteen tietoturvaa kolmelle haastateltavista tilanne ei aiheuttaisi toimenpiteitä, kun taas viisi haastateltavaa lopettaisi palveluntarjoajan kaikkien tuotteiden käytön kaikilla laitteilla ja alustoilla. Usean haastateltavan kohdalla haastateltava myös painotti, että reaktio riippuu tarkemmin tilanteesta:

> H3: Niin no, kyllähän siinä jää semmonen epäluottamus sitten koko toimittajaan tai softan valmistajaan. Rupeaa miettimään, että onko muut kyseisen firman sovellukset luotettavia. Vähän riippuu firmasta, että jos on joku tunnettu, niin ehkä en olis niin huolissaan. Jos olis joku vähemmän tunnettu, niin saattaisin lopettaa kaikkien kyseisen firman tuotteiden tai softien käyttämisen.

> H9: Siinä kohtaa varmaan vähän riippuen myös, että mitä tietoja on sinne syöttänyt, että jos on sellainen sovellus mihin on itse syöttänyt ihan niin kun esimerkiksi pankkikortin tiedot, niin siinä kohtaa pitäisi ottaa vakavammin se syyniin ja lähteä noita samoja reittejä selvittämään, että mitä voi tehdä. Ja toki sitten nää jo mainitut salasanan vaihdot ja muut, mutta tuota jos on

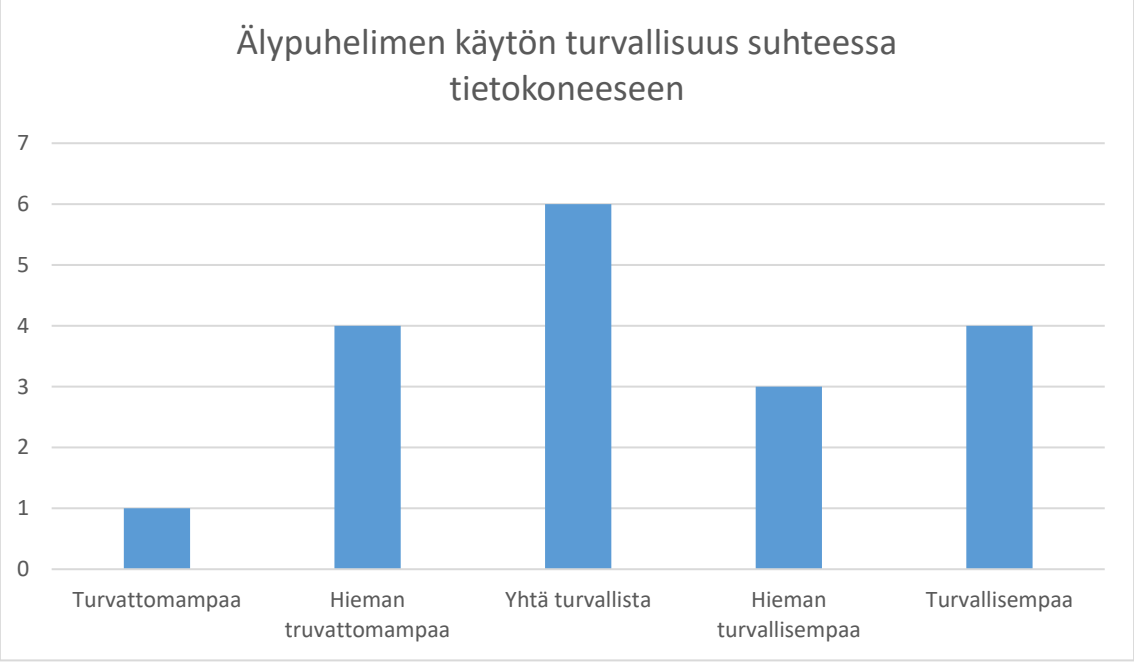
joku tällainen höpöhöpösovellus missä ei tavallaan ole mitään, en ole antanut mitään erityisempiä tietoja, niin ehkä saattaisin… Tavallaan jättäisi sen oman arvonsa sen ilmoituksen sitten. Se pitäisi tapauskohtaisesti katsoa kyllä.

H11: Varmaan ensimmäisinä poistaisin tunnukset siitä ja sen sovelluksen ja sitten varmaan en tiedä mitä sen jälkeen tekisin. Riippuu vähän, että minkälaista tietoa ja minkälainen sovellus ja minkälaista tietoa, jos siellä on jotain maksutietoja ja muita niin sitten ehkä… sitten niitten mukaan toimisin. Mahdollisia sulkuja ja muita, mutta jos pelkkää henkilötietoa niin varmaan tunnuksen poisto ja sovelluksen poisto. En tiedä olisiko siinä muuta tehtävissä

Useimmille haastateltavista tilanteet aiheuttaisivat jonkinlaista huolta, paniikkia tai pelkoa. Haastateltavista kolme pyrkisi turvaamaan omat oikeutensa ja suojaamaan henkilötietonsa. Neljä haastateltavaa toi esille pankkikorttien kuolettamisen tai pankkitileillä tapahtuvan rahaliikenteen seurannan.

5.1.2 Älypuhelimen käytön turvallisuus

Tutkimushaastattelussa kysyttiin osallistujilta heidän mielipidettään älypuhelimen käytön turvallisuuteen. Seuraavassa kuviossa (KUVIO 7) on esitelty vastaukset kysymykseen: *Miten koet älypuhelimen käytön turvallisuuden kannalta suhteessa tietokoneeseen? Turvallisempaa, hieman turvallisempaa, yhtä turvallista, hieman turvattomampaa vai turvattomampaa.*



KUVIO 7 Älypuhelimen käytön turvallisuus suhteessa tietokoneeseen

Jos vastaukset numeroidaan yhdestä viiteen niin, että yksi on turvattomampaa ja viisi on turvallisempaa, keskiarvoksi tulee noin 3,27, eli hieman yli yhtä turvallista. Leavitt (2011) on tutkimuksissaan yli kymmenen vuotta sitten todennut, että käyttäjät luottavat etenkin kalasteluyrityksissä ja sosiaalista mediaa käyttäessään enemmän mobiililaitteisiin, kuin tietokoneeseen. Älypuhelimien huomattavan yleistymisen ja käyttäjien tietoisuuden kasvamisen myötä, älypuhelinkäyttäjien varautuminen laitteisiin kohdistuvien uhkien osalta on voinut nousta. On kuitenkin huomioitava, että otanta koostuu täysin suomalaisista työikäisistä älypuhelimien käyttäjistä, joiden tietoisuus ja koulutustaso keskiarvolta muita kansalaisuuksia ja ikäluokkia korkeampi.

Tutkimuksessa haastateltavilta kysyttiin, onko heidän suhtautumisensa älypuhelimien tietoturvaan muuttunut siitä lähtien, kun he hankkivat ensimmäisen älypuhelimensa. Osallistujista 14 vastasi suhtautumisen muuttuneen kriittisemmäksi, varovaisemmaksi tai epäileväisemmäksi ja samalla näistä 14:sta kolme mainitsi myös luottamuksen puhelimen valmistajaan ja oman yksityisyydensuojan säilymiseen madaltuneen. Osallistujista kolme mainitsi luottamuksen puhelimen tietoturvaan kasvaneen ja epäilyksien vähentyneen. Yksi vastaajista sanoi, että suhtautuminen ei ole muuttunut. Tämä tulos vahvistaa johtopäätöstä siitä, että älypuhelimien käyttäjien liiallinen luottamus älypuhelimen turvallisuuteen on tasoittunut siitä, kun Leavitt (2011) on oman tutkimuksensa tehnyt.

5.1.3 Älypuhelimen käyttö julkisilla paikoilla

Älypuhelimen käytöstä julkisilla paikoilla keskusteltaessa oli huomattavissa, että kyberympäristön kognitiivisella tasolla älypuhelimien käyttäjät noudattavat erityistä varovaisuutta. Tällä tarkoitetaan sitä, että tieto mitä digitaalisen ympäristön ulkopuolella on saatavilla, varjellaan tarkasti. Digitaalisen ympäristön ulkopuolinen tieto on sitä, joka esiintyy älypuhelimen näytöllä tai mitä puhelimeen puhuessa tulee ilmi. Haastateltavista jopa 15 mainitsi tekevänsä erilaisia toimenpiteitä näytön suojaamiseksi olan yli vilkuilijoilta (eng. shoulder surfing). Tällaisia toimenpiteitä ovat näytön suojaaminen, kääntäminen pois ja esimerkiksi kirkkauden säätäminen alemmas.

> H17: Tosi usein julkisissa, esimerkiksi julkisilla liikennevälineillä kun menee, matkustaa ja on ihmisiä paljon ympärillä, niin että mä havaitsen, että joku voi nähdä niin käännän tota näytön kirkkautta pienemmälle. Ja sitten aina, jos mä laitan tunnukset, mitkä tahansa, niin kun että mä koitan niin kun mennä sisään jonnekin, eli olisi sitten pankki tai mikä tahansa, niin peitän kädellä monesti sitä näyttöä, että sitten sitä ei tavallaan pystyisi kukaan näkemään.

Näistä 15:sta neljä ei käsittele sensitiivistä tietoa, kuten pankki tai terveystietoja ollenkaan julkisilla paikoilla. Haastateltavista kolme mainitsi käyttävänsä älypuhelinta muuten samalla tavalla kuin esimerkiksi kotonaan, paitsi pitäen laitteen äänet pienellä tai pois päältä ja varmistaen että älypuhelimessa toistettava sisältö on sosiaalisesti hyväksyttävää.

Älypuhelimen varastaminen ei lähtökohtaisesti aiheuttanut haastatteluun osallistuneissa aktiivista huolta, mutta haastateltavat olivat pääosin hyvin huolellisia laitteen säilyttämisen osalta, ettei sitä varasteta. Haastateltavista 16 säilyttää puhelinta aina joko etutaskussa, käsilaukussa, älypuhelimelle tarkoitetussa kantopussissa tai kantaa sitä kädessä, jolloin laite ei ikinä ole esimerkiksi takataskussa tai repun sivutaskussa, josta se voitaisiin varastaa.

> H5: Otan sen vakavasti ja haluan pitää puhelimen aina lähellä tai mukana silleen, että sen varastaminen ei ole mahdollista.

> H11: Kyllä ja varsinkin kun olen reissannut semmoisissa maissa, joissa ryöstetyksi tulemisen riski tai taskuvarkausriski on korkeampi, niin se tulee lähinnä siitä, että mä tiedostan tarkemmin, että kännykkä on taskussa ja enemmänkin että tuntuu kummalliselta, jos se ei olisi. Ja jos on epäilyttävä tilanne, niin pidän kättä vielä taskun päällä.

Haastateltavista yksi miettii aktiivisesti, miten varkausriskiä voisi pienentää, mutta oman hajamielisyyden takia laite saattaa unohtua julkisille paikoille. Yksi haastateltavista säilyttää laitetta muuten huolellisesti, mutta esimerkiksi tutussa lounasravintolassa älypuhelin voi jäädä hetkeksi vartioimatta.

5.2 Palvelukerros

Älypuhelimien kontekstissa, palvelukerroksella tarkoitetaan laitteeseen asennettuja sovelluksia ja ohjelmia. Tässä alaluvussa pyritään selvittämään haastateltavien toimintoja, jotka parantavat tai heikentävät palvelukerroksen turvallisuutta.

5.2.1 Älypuhelinsovellukset

Haastateltavista yhdeksän kertoi ladanneensa sovelluksia virallisen sovelluskaupan ulkopuolelta. Virallisen sovelluskaupan ulkopuolelta ladanneista käyttäjistä kolme oli ladannut sovelluksia vain ns. luotettavista lähteistä. Tällaisiksi voidaan luokitella työssä käytettävät APK-tiedostot, ulkomaalaiset suoratoistopalvelut, joita suomen App Storessa tai Play-kaupassa ei ole tarjolla, uhkapelisovellukset, jotka on kielletty Play-kaupassa tai muut tunnettujen toimittajien sovellukset heidän omilta sivuiltaan.

> H12: Kyllä olen, esimerkiksi jotain semmoisia mitä suomen Play Storesta ei saa. Eli jos on pitänyt jollain VPN:llä tai jollain jostain ulkomailta ladata, niin semmoisia. Esimerkiksi vaikka striimaukseen tarkoitettuja tai sitten jostain laillisista syistä kuten esimerkiksi pokeri ja mitähän muuta. No sitten jotain omia kehityksiä, mutta niitä nyt ei ole ladattu mistään muualta kuin omalta koneelta tuohon puhelimeen. Ehkä ne noihin menee, että jotain tämmöisiä ulkomaan sovelluksia, mitä ei suomen Play kaupasta saa niin sitten APK ladattu sitten ihan selaimen kautta palveluntarjoajan sivuilta.

Haastateltavista kuusi sanoi ladanneensa sovelluksia ei täysin luotettavista lähteistä, kuten forumeilta saatujen linkkien kautta tai GitHubista. Vaikka GitHubin avoin lähdekoodi antaa tietynlaista luotettavuutta sovellukselle, ei se estä haitallisten sovellusten lisäämistä.

> H5: Olen ladannut rahapelisovelluksia näiden yritysten omilta sivuilta. Ja joskus tota S-nelosen (Samsung) aikaan emulaattorin ja siihen pelejä epäilyttäviltä sivuilta.
>
> H9: Kyllä olen esimerkiksi sellaisia sovelluksia mitä on julkaistu muualla kuin suomessa ennemmin kuin... tai niin kun muualla maailmalla aiemmin kuin Suomessa ja tullut Suomessa vasta myöhemmin saataville, niin olen saattanut, tai pari kertaa olen ladannut APK tiedoston, josta sitten päässyt asentamaan sovelluksen puhelimelle, vaikka se ei vielä suomessa ole Play kauppaan julkaistu. Ja ne sivustot… en ole varma, että miltä sivustolta, en muista, mutta sellaisilta mistä olen lukenut, että monet muutkin ovat ladanneet.

Epäluotettavista lähteistä sovelluksia ladanneista haastateltavista, enää kahdella käyttäjällä on kyseisiä sovelluksia älypuhelimessaan. Poissulkien työhön liittyvät APK-tiedostot, kaikki sovelluskauppojen ulkopuolelta ladatut sovellukset oli ladattu ainoastaan henkilökohtaiseen puhelimeen. Kysyttäessä millaisia sovelluksia käyttäjät olivat ladanneet puhelimiinsa, suosituimpia olivat:

- Verkkopankkisovellukset (18 haastateltavalla),
- Pikaviestisovellukset, kuten Whatsapp ja Signal (18 haastateltavalla),
- Sosiaalisen median sovellukset (17 haastateltavalla),
- Media- ja suoratoistopalvelut, kuten musiikki video ja äänikirjapalvelut (13 haastateltavalla),
- Verkkokauppasovellukset (7 haastateltavalla),
- Auton etähallintasovellukset ja parkkisovellukset (7 haastateltavalla),
- Pelit (7 haastateltavalla).

Haastateltavien eniten käyttämät sovellukset olivat pikaviestipalvelut, sosiaalinen media, selain ja sähköposti. Haastateltavista yksi oli ladannut puhelimeensa vain viisi sovellusta, joka oli otannan pienin määrä. Otannan suurin määrä oli 140 sovellusta. Keskimäärin erilaisia sovelluksia haastateltavat olivat itse ladanneet omaan älypuhelimeensa noin 58 kappaletta.

Haastattelun aikana haastateltavat pitivät älypuhelinta lähellään, jotta tiedot voitiin tarkistaa. Sovellusten keskimäärä oli haastateltavien keskuudessa huomattava ja ladattujen sovellusten suuri luku tuli monelle yllätyksenä ja monista sovelluksista haastateltavilla ei ollut edes muistikuvaa niiden lataamisesta. Di Sorbo & Panichella (2021) testasivat tutkimuksessaan noin tuhatta eri Google Play -kaupan sovellusta. Tutkimuksessa lähes jokaisesta sovelluksesta löytyi jokin haavoittuvuustekijä. Puolueettomien haittaohjelmatestausten mukaan, Google Playn Protect -toiminto ei pystynyt

tunnistamaan edes yleisimpiä haittaohjelmia (Davis & Samani, 2018). Di Sorbo & Panichella (2021) ottavat myös kantaa siihen, että useimmat sovellukset vaativat käyttöoikeuksia esimerkiksi yhteystietoihin tai kuvagalleriaan toimiakseen, joka vaarantaa älypuhelinkäyttäjän yksityisyydensuojaa. Mikäli käyttäjällä ei ole edes muistikuvaa asennetusta sovelluksesta, ei käyttäjä välttämättä edes tiedä tulleensa tietoturvaloukkauksen uhriksi. Käyttäjän unohtamat sovellukset voivat myös olla niin sanotusti ”kuolleita”. Tämä tarkoittaa sitä, että sovelluskehittäjä on poistanut sovelluksen sovelluskaupasta ja lopettanut sovelluksen päivittämisen ilmoittamatta tästä sovelluskaupan ylläpitäjälle (Davis & Samani, 2018).

Lähtökohtaisesti sovelluskaupasta asennetun sovelluksen turvallisuutta kuitenkin parantaa se, että sovellukset päivitetään säännöllisesti. Haastateltavista 11 vastasi päivittävänsä sovellukset säännöllisesti. Palvelukerrokseen liittyvien kysymysten lopuksi käyttäjiä pyydettiin tarkistamaan puhelimen sovelluskaupasta, montako sovellusta haastatteluhetkellä käyttäjällä on päivittämättä:

- Nolla: 4 haastateltavaa,
- 1–10: 7 haastateltavaa,
- 11–20: 2 haastateltavaa,
- 21–30: 0 haastateltavaa,
- 31–40: 2 haastateltavaa,
- 41–50: 2 haastateltavaa,
- 51–60: 1 haastateltava.

Yli puolilla haastateltavista oli alle kymmenen päivittämätöntä sovellusta, joista osaan on saatettu julkaista päivitys hieman ennen haastattelutilannetta. Sovellusmäärän keskiarvon ollessa noin 58, voidaan tätä lukemaa pitää verrattain hyvänä.

5.2.2 Suhtautuminen sovellusten turvallisuuteen

Haastateltavista viidellä oli asennettuna puhelimeensa erillisiä laitteen turvallisuutta ja käyttäjän yksityisyyttä parantavia sovelluksia. Kaikilla näistä oli henkilökohtainen- ja työpuhelin samassa laitteessa, josta voidaan päätellä työpaikan turvallisuuskäytäntöjen mahdollisesti vaativan niitä. Vaikka asiasta ei erikseen kysytty, haastateltavista, joilla erillistä turvallisuussovellusta ei ollut asennettuna, neljä mainitsi omistaneen turvallisuutta parantavan sovelluksen aiemmin, muttei nähnyt sellaista enää tarpeelliseksi. Haastateltavilta kysyttiin, pitävätkö he sovelluskaupasta ladattuja sovelluksia luotettavina, asteikolla yhdestä viiteen, jossa yksi on erittäin epäluotettava ja viisi on erittäin luotettava. Sama kysymys kysyttiin myös sovelluskaupan ulkopuolelta ladattavista sovelluksista. Mikäli työpuhelimesta puhuttaessa yrityksellä oli käytössä oma sovelluskeskus, se laskettiin viralliseksi sovelluskaupaksi. Kysymysten tulokset ovat esitettyinä seuraavassa taulukossa (taulukko 3).

TAULUKKO 3 Luottamus sovelluskaupan ja sovelluskaupan ulkopuolisiin sovelluksiin

Luottamus	Sovelluskaupan sovellukset	Sovelluskaupan ulkopuoliset sovellukset
5	9 haastateltavaa	
4	6 haastateltavaa	1 haastateltava
3	2 haastateltavaa	1 haastateltava
2	1 haastateltava	9 haastateltavaa
1		7 haastateltavaa

Tulosten mukaan haastateltavat lähtökohtaisesti pitävät sovelluskaupasta ladattavia sovelluksia luotettavina ja sovelluskaupan ulkopuolisia sovelluksia epäluotettavina. Neljä käyttäjää, joilla oli henkilökohtaisena älypuhelimenaan Apple iOs, mainitsi pitävänsä Googlen Play -kauppaa hieman epäluotettavampana. Aiempien tutkimusten perusteella, etenkin Google Play -kaupasta sovelluksia ladatessa, kannattaa käyttää myös omaa harkintaa. Etenkin sovellusoikeuksia myöntäessä ja syöttäessä sovellukseen omia henkilökohtaisia- tai pankkitietoja (Di Sorbo & Panichella, 2021; Davis & Samani, 2018). Osa haastateltavista mainitsi sovelluskaupan ulkopuolelta ladattavista sovelluksista, että luottamus perustuu myös käyttäjän kokemukseen.

H3: Niin no no, siinä pitää vähän itse tietää mitä tekee ja mistä lataa.

Vaikka sovelluskauppoihin onkin kohdistettu niiden olemassaolon ajan erilaisia haittaohjelmakampanjoita, haitallisten sovellusten poistamisen ja estämisen eteen tehdään sovelluskauppojen ylläpidossa töitä. Sovelluskauppojen ulkopuolisia sovelluksia ei kuitenkaan lähtökohtaisesti analysoida haittaohjelmien varalta, joten luottamus sovelluskauppojen ulkopuolisiin sovelluksiin on syystäkin alhainen. Etenkin haastateltavat, jotka pitivät omaa älypuhelimiin suuntautuvaa teknistä osaamistaan keskiarvoa alhaisempana, pitivät myös sovelluskauppojen ulkopuolisten sovellusten luotettavuutta alhaisena.

5.3 Semanttinen kerros

Semanttisella kerroksella tarkoitetaan älypuhelimeen tallennettua tietoa, informaatiota ja dataa. Laitteeseen tallennetun tiedon, informaation tai datan kautta hyökkääminen älypuhelimeen olisi ilman edeltäviä välivaiheita hankalaa,

ellei kyseessä olisi haittaohjelma, joka on upotettu esimerkiksi pdf-tiedostoon. Mutta tämäkään ei täysin vastaisi tutkielman kuvausta. Siksi tässä alaluvussa kiinnitetään huomiota suorimpiin reitteihin semanttiseen kerrokseen.

5.3.1 Älypuhelimen tietoturvallinen käyttö

Haastateltavilta kysyttäessä, millaisia lukituksia he käyttävät henkilökohtaisissa sekä työpuhelimissaan, oli henkilökohtaisessa puhelimessa ns. kovana tunnuksena selkeästi suosituin pin-koodi, jota käyttivät 11 kappaletta haastateltavista. Kuviolukitus ja salasana olivat yhtä suosittuja, joista molempia käytti kolme haastateltavaa ja yhdellä haastateltavista ei ollut käytössä lukitusta lainkaan. Muslukhov (2012) on kritisoinut pin-koodin ja kuviolukituksen käyttöä niiden helpon murtamisen takia. Pin-koodin ja kuviolukituksen taustalla olevat salausmenetelmät ovat vuosien aikana kehittyneet ja niitä kehitetään jatkuvasti. Tämä tarkoittaa sitä, että näytön lukitus ei ole hakkeroitavissa niin helposti kuin aiemmin (Ibrahim, Alarood, Chiroma, Al-garadi, Rana, Muhammad & Gabralla, 2019). Pin-koodia tai näyttölukitusta murtaessa, sen arvaaminen on kuitenkin suhteellisen helppoa. Erityisesti älypuhelimen näyttöön jääneet sormenjäljet rajaavat lukituskoodien vaihtoehdot niin pieniksi, että koodi on joissakin tapauksissa murrettavissa, ennen kuin laite disabloituu vääristä yrityksistä. Myös pahantekijä, joka on nähnyt älypuhelimen käyttäjän avanneen näyttölukon kuviolla, todennäköisesti muistaa kuvion. Tämän jälkeen pahantekijällä on esimerkiksi laitteen varastamisen jälkeen pääsy laitteeseen (Aviv, Davin, Wolf & Kuber (2017).

Myös älypuhelimien helppokäyttölukitukset olivat suosittuja henkilökohtaisissa puhelimissa. Vain kolmella haastateltavalla, joilla oli näyttölukitus käytössä, ei ollut helppokäyttölukitusta käyttöön. Tässä tutkimuksessa käsiteltävät helppokäyttölukitukset ovat kasvojentunnistus sormenjäljen tunnistus. Sekä kasvojentunnistuksesta, että sormenjäljen tunnistuksesta ja niiden luotettavuudesta on ollut paljon keskustelua puolin ja toisin. Kasvojentunnistuksesta ollaan blogikirjoitusten ja foorumien mukaan tehty testejä, joissa esimerkiksi älypuhelimen kaksoissisarus on saanut puhelimen avattua tai tarpeeksi tarkka digitaalinen mallinnus on toiminut avaimena. Sormenjäljen osalta myös blogiteksteissä ja foorumeilla puhutaan, että esimerkiksi 3D-tuloste sormesta ja siihen liitetty sormenjälki, joka on otettu puhelimen pinnasta, on onnistunut avaamaan älypuhelimen. Tällaiset toimet vaativat kuitenkin huomattavia resursseja, eikä varsinaista tieteellistä lähdettä väitteille löytynyt. Näiden keskusteluiden vaikutukset käyttäjiin oli kuitenkin huomattavissa myös haastateltavien osalta, sillä osa haastateltavista mainitsi, ettei luota joko sormenjäljen tunnistukseen tai sitten kasvojentunnistukseen.

Työpuhelimista puhuttaessa, osalla haastateltavista työpaikan turvallisuuskäytännöt vaikuttivat lukituksen valitsemiseen. Kaikilla haastateltavilla, joilla oli henkilökohtaisessa puhelimessa lukituskoodina salasana, oli työpuhelin ja henkilökohtainen puhelin yhdistettynä samaan laitteeseen. Yhteensä salasanoja oli työpuhelimissa käytössä neljällä käyttäjällä. Suurin vaikutus oli helppokäyttölukituksiin, sillä kahdeksalla käyttäjällä ei ollut

käytössä helppokäyttölukitusta työpuhelimessa. Tämä johtui joko siitä, että työnantaja oli kieltänyt helppokäyttölukituksen asettamisen tai helppokäyttölukitusta ei ollut käytössä henkilökohtaisessakaan puhelimessa. Yhdellä haastateltavista ei ollut näyttölukitusta käytössä työpuhelimessaan.

Haastateltavista, jotka käyttivät lukitusta puhelimessaan, yhdeksän ei vaihda näyttölukituksen pin-koodia, salasanaa tai kuviota koskaan. Yksi vaihtaa viiden vuoden välein, kolme puhelinta vaihdettaessa, jonka keskiarvo on ensimmäisen puhelimen hankinnan ja älypuhelimien määrän perusteella noin neljä vuotta, yksi vaihtaa kolmen vuoden välein ja kaksi kerran tai useammin vuodessa. Yksi haastateltavista ei halunnut vastata kysymykseen.

Haastateltavista 13 työpaikalla noudatetaan joitakin älypuhelimen käyttöön liittyviä tietoturvakäytänteitä joko ohjeellisesti tai työpuhelimeen oli asetettuna tiettyjä rajoitteita. Kahdella työpaikalla älypuhelimen tietoturvakäytänteitä ei ollut käytössä ja kolme haastateltavaa ei osannut vastata kysymykseen. Kysyttäessä, onko työpaikalla käytössä olevat tietoturvakäytänteet vaikuttaneet jotenkin oman puhelimen käyttöön, 14 vastasi saaneensa joitakin vaikutteita näistä käytännöistä. Haastateltavista viisi tarkensi kysymyksen vastausta. Kolmella haastateltavista tietoisuus tietoturvariskeistä ja sen myötä varovaisuus oli kasvanut. Yhdellä haastateltavista, jolla molemmat puhelimet ovat samassa laitteessa, luottamus omaan yksityisyydensuojaan oli madaltunut. Tämä johtui siitä, että haastateltava ei luottanut siihen, etteikö työnantaja seuraisi älypuhelimen käyttöä. Yhdellä haastateltavista, jolla myös molemmat puhelimet olivat samassa laitteessa, reaktio on ollut hyvin päinvastainen. Haastateltavan työnantaja on estänyt useiden sovellusten ja verkkosivujen käytön älypuhelimella, kuten uhkapelit, joten haastateltava pyrki käyttämään estettyjä palveluita sulkemalla VPN-yhteyden ja näin ollen pysyen pois yrityksen sisäverkosta.

Julkisten USB-latausporttien yleistymisen ja niistä laitteisiin suuntautuvien vaarojen takia haastateltavilta kysyttiin myös, ovatko he ladanneet älypuhelintaan julkisissa USB-latauspistokkeissa ja mikäli lataavat, käyttävätkö he ladatessaan niin kutsuttua data blockeria, joka lähtökohtaisesti estää datan liikkumisen latauskaapelissa estäen haittaohjelmien tarttumisen saastuneesta latauspistokkeesta. Vaikka tänä päivänä on myös löydetty älypuhelimiin suuntautuvia haittaohjelmia, jotka pääsevät läpi data blockereista, on suojan käyttö erittäin suositeltavaa (Jiang, Ji, Wang, Yan, Mitev, Sadeghi & Xu (2022). Haastateltavista viisi kertoi ladanneensa älypuhelintaan julkisessa latauspistokkeessa ja yksi mainitsi, että lataisi jos olisi pakko. Kukaan haastateltavista ei ole käyttänyt eikä käyttäisi data blockeria. Haastatteluissa oli selkeästi huomattavissa, että haastateltavat eivät lähtökohtaisesti luota julkisiin USB-portteihin ja niitä käyttävien lukumäärä oli suhteellisen alhainen porttien yleisyyteen verrattuna.

5.3.2 Älypuhelimeen tallennettu tieto

Tutkimuksessa oletuksena oli, että jokaisen haastateltavan henkilökohtaiseen älypuhelimeen on tallennettuna joko itselle tai muille arkaluontoista dataa tai

informaatiota, esimerkiksi ihan kuvien tai viestien muodossa. Oletus piti hyvin paikkaansa, sillä vain yksi haastateltavista koki, ettei hänen henkilökohtaiseen älypuhelimeensa ole tallennettuna mitään sellaista, jonka paljastuminen voisi vahingoittaa itseä tai muita. Haastateltavista kahdeksan kertoi, että heidän työpuhelimiinsa on tallennettuna yrityksen tai yrityksen asiakkaan kannalta arkaluontoista, salaista tai turvaluokiteltua dataa tai informaatiota. Vastauksissa pitää myös huomioida vastaajien oma tietämys arkaluontoisen, salaisen ja turvaluokitellun materiaalin määrittelystä. Haastateltavista vain kaksi ei ollut yhdistänyt työpuhelintaan työsähköpostiin ja voidaan pitää mahdollisena, että useampien haastateltavien työsähköposteista olisi löytynyt vähintäänkin arkaluontoista materiaalia. Kukaan haastateltavista, joilla oli erikseen työ- ja henkilökohtainen älypuhelin, ei ollut tallentanut omaan työhönsä liittyviä tietoja henkilökohtaiseen älypuhelimeensa.

Haastatteluihin osallistuneet älypuhelimine käyttäjät suojaavat laitteisiin tallennetun tiedon lähtökohtaisesti hyvin tai melko hyvin. Lähes kaikki käyttäjät käyttävät edes jonkinlaista näyttölukitusta laitteissaan. Kuten kaikkien salasanojen kohdalla, myös näyttölukitusta olisi hyvä vaihtaa säännöllisin määräajoin. Haastateltavat kuitenkin vaihtoivat näyttölukitustaan pääosin hyvin harvoin tai ei koskaan.

5.4 Syntaktinen kerros

Syntaktinen kerros pitää sisällään älypuhelimen laiteohjelmiston, käyttöjärjestelmän ja kaikki laitteen verkkoon liittävät komponentit. Älypuhelin, jonka käyttöjärjestelmää ei ole päivitetty tai laite, jolle ei ole saatavilla enää käyttöjärjestelmäpäivityksiä, kasvattaa huomattavasti syntaktisen kerroksen haavoittuvuutta. Haastateltavista 14 päivittää älypuhelimen käyttöjärjestelmän välittömästi, kun huomaa uuden päivityksen ilmestyneen. Vastaajista kolme päivittää käyttöjärjestelmänsä muutaman viikon sisällä uuden päivityksen ilmestyttyä ja yksi päivittää vasta, kun laite ilmoittaa käyttöjärjestelmäpäivityksestä liian usein ja ilmoitukset hankaloittavat laitteen käyttöä.

> H16: En päivitä, muuta kuin sitten automaattisesti se tulee, että nyt pitää päivittää. Enkä päivitä vielä ekasta, nytkin tää on täällä kolmatta kertaa. Yleensä kysyn *henkilöltä X* tai *henkilöltä Y*, että onko tää nyt luvallinen päivitys.

Kaikkien haastateltavien henkilökohtaisiin- sekä työpuhelimiin oli vielä saatavilla käyttöjärjestelmäpäivityksiä.

Antamalla juuritason oikeudet älypuhelimen käyttäjälle, käyttäjä altistaa laitteen laajasti vakaville uhkille. Niin kutsuttu jailbreak tai roottaus antaa käyttäjälle mahdollisuuden hallita älypuhelinta vapaammin. Samalla kuitenkin älypuhelimien yksi suurimmista suojaavista tekijöistä, hiekkalaatikkomalli,

murtuu. (Nguyen-Vu, ym., 2017). Tämä mahdollistaa esimerkiksi erilaisten haittaohjelmien liikkumisen vapaammin eri sovellusten ja kerrosten välillä. Haastateltavista kuusi oli joskus asettanut juuritason oikeudet älypuhelimeensa, mutta kukaan heistä ei ollut tehnyt tätä nykyiselle älypuhelimelleen. Kukaan haastateltavista ei kuitenkaan ole yrittänyt antaa juuritason oikeuksia työpuhelimelleen.

Liityttäessä julkiseen, avoimeen langattomaan verkkoon, on hyökkääjällä mahdollisuus tarkkailla käyttäjän toimintaa verkossa. Hyökkääjä voi myös asettaa oman tukiasemansa näyttämään luotettavalta julkiselta avoimelta verkolta, johon liittyminen aiheuttaa uhkan esimerkiksi väliintulohyökkäykselle (engl. man in the middle). Haastateltavista 16 kertoi käyttävänsä joskus avoimia langattomia verkkoja, erityisesti ulkomailla tai julkisissa kulkuneuvoissa. Avoimia julkisia langattomia verkkoja käyttävistä kolme mainitsi käyttävänsä aina samalla myös VPN-yhteyttä, joka estää pakettiliikenteen tarkkailun kolmannelta osapuolelta.

Suurimmalta osalta syntaktiseen kerrokseen kohdistuvista uhkista haastateltavat minimoivat riskejä hyvin. Älypuhelimien käyttöjärjestelmäpäivityksiä ladataan ja asennetaan aktiivisesti. Lisäksi lisääntyneen tietoisuuden myötä, kukaan haastateltavista ei enää halua altistaa älypuhelintaan ylimääräisille uhkille asettamalla siihen juuritason oikeuksia. Yli puolet haastateltavista oli tietoisia siitä, että avoimien langattomien verkkojen käyttö voi olla riskialtista. Haastateltavat eivät kuitenkaan välttämättä tienneet tarkkaan, mitä nämä riskit ovat. Suuri osa älypuhelimien sovelluksista vaatii toimiakseen internetyhteyttä. Mikäli mobiiliverkkoa tai suojattua langatonta verkkoa ei ole saatavilla, houkutus liittyä suojaamattomaan verkkoon on suuri.

5.5 Fyysinen kerros

Fyysisellä kerroksella tarkoitetaan itse älypuhelinta fyysisenä laitteena sekä kaikkia älypuhelimen sisältäviä fyysisiä komponentteja. Fyysiseen kerrokseen voidaan myös laskea mukaan erilaiset älypuhelimessa käytettävät lisälaitteet, joita tässä tutkimuksessa käsitellään hyvin pintapuolisesti. Fyysisen kerroksen haavoittuvuudet asettuvat usein päällekkäin muidenkin kerrosten kanssa.

5.5.1 Älypuhelimen suojaaminen katoamisilta ja fyysisiltä vaurioilta

Haastateltavista suurin osa ei ollut koskaan kadottanut älypuhelintaan kotinsa tai muun luotettavan alueen ulkopuolella. Haastateltavista kolme kertoi kadottaneensa älypuhelimensa hetkellisesti, mutta laite on aina lopulta löytynyt. Suurimmassa osassa tapauksista haastateltava on itse löytänyt laitteen. Joissakin tapauksissa ulkopuolinen henkilö on kuitenkin palauttanut laitteen haastateltavalle.

> H16: Olen monta kertaa ja tota noin niin. Jos aatellaan nyt näitäkin kertoja, että se on sitten niinku ollut jossain auton katolla ja tippunut, niinku että se on ollut niin, joka kerta se puhelin on löytynyt. Mutta joko sitten rikkinäisenä ja se on palautettu tai jotain muuta. Sitten on muutaman kerran suljettu ne pankkiyhteydet ja muut, korttiyhteydet ja muut.

Kaikki haastateltavat, jotka olivat joskus kadottaneet älypuhelimensa, olivat kadottaneet laitteen useamman kerran. Vastauksista ei voida tehdä suoria johtopäätöksiä, onko kyseessä välinpitämättömyys älypuhelinta ja sitä kautta omaa tieto- ja yksityisyydensuojaa kohtaan, vai johtuuko tapaukset haastateltavien yleisestä hajamielisyydestä.

Hypoteettisessa tilanteessa, jossa haastateltava kadottaisi älypuhelimensa eikä löytäisi sitä, seitsemän käyttäisi ensimmäisenä laitteen etädisablointia ja lukitusta, jonka jälkeen älypuhelimeen tallennettuihin tietoihin ei pääse enää käsiksi. Neljä haastateltavaa käyttäisi käyttöjärjestelmän tarjoamaa laitteenlöytämispalvelua, jolla pystyy GPS:n avulla paikantamaan laitteen ja tarvittaessa kytkemään älypuhelimesta hälytyksen päälle, joka helpottaa laitteen löytymistä. Sekä Android että Apple muistuttavat nykyisin laitteenetsintäpalvelussaan myös laitteen etädisabloinnista ja lukituksesta, jota voidaan käyttää, mikäli ominaisuus on kytketty laitteessa päälle. Haastateltavista kuusi mainitsi ilmoittavansa työpuhelimen katoamisesta työpaikan IT-tukeen, josta saisi todennäköisesti apua ongelmaan. Muutamat haastateltavat kertoivat myös kuolettavansa pankkikorttinsa, ilmoittavansa poliisille tai vaihtavansa laitteeseen liitettyjä salasanoja. Kaksi haastateltavaa ei tietäisi mitä tekisi. Samaan aiheeseen liittyen haastateltavilta kysyttiin, onko heillä käytössä laitteen etädisablointi ja lukitus, ja tiesivätkö he kyseisestä ominaisuudesta. Haastateltavista kahdeksan sanoi tietävänsä ja käyttävänsä ominaisuutta, viisi sanoi tietävänsä ominaisuudesta, mutta ei käytä sitä ja viisi sanoi, ettei tiennyt kyseisestä ominaisuudesta. Poissulkien kaksi haastateltavaa, jotka eivät tietäisi mitä tehdä laitteen kadotessa, kaikki haastateltavat osaisivat tehdä nopeita toimenpiteitä omien henkilökohtaisten tietojen suojaamiseksi. Kuusi haastateltavaa mainitsi erikseen, että tärkeintä olisi suojata kaikki laitteeseen tallennettu tieto, informaatio tai data, jonka jälkeen mahdollinen fyysisen laitteen takaisin saaminen olisi toisarvoista.

Laitteelle aiheutuvat fyysiset vauriot voidaan luokitella myös tietoturvariskiksi, sillä älypuhelimen varmuuskopiointi ei kaikissa tilanteissa ole jatkuvaa ja osa siihen tallennetuista tiedoista voidaan menettää, mikäli laite tai sen tallennustila vaurioituu korjauskelvottomaksi. Erityisesti suojakuorien käyttö oli haastateltavien keskuudessa suosittua. Henkilökohtaisissa älypuhelimissa haastateltavista 11 käytti kannetonta suojakuorta ja kolme kannellista suojakuorta. Haastateltavista viisi käytti henkilökohtaisessa älypuhelimessaan panssarilasia ja kaksi suojakalvoa. Haastateltavista neljä ei käyttänyt ollenkaan erillistä fyysistä suojausta. Työpuhelimien osalta yritysten käytänteet ohjailivat pitkälti haastateltavien toimintaa. Työpuhelimen fyysiseen suojaukseen ei tarvitse kuitenkaan tarkemmin paneutua, sillä työpuhelimen fyysisestä suojauksesta päätti haastateltavien työnantajat, eikä itse älypuhelimen

käyttäjä, eli haastateltava. Huomioitavaa kuitenkin oli, että haastateltavien henkilökohtaiset älypuhelimet olivat työpuhelimia paremmin suojattu fyysisiltä vaurioilta, joten vaikutteita fyysiseen suojaukseen ei ole tullut työpaikan käytännöistä. Haastateltavista 14 oli joskus hajottanut älypuhelimensa niin, että se on ollut ilman huoltoa käyttökelvoton. Tämä voi myös olla osittain syy sille, miksi haastateltavat suojasivat nykyisiä laitteitaan tarkemmin.

5.5.2 Väärennetyt älypuhelimet, komponentit ja lisälaitteet

Rauhalan (2022) mukaan väärennetty elektroniikkatuotanto on arvoltaan noin 100 miljardia dollaria, joka kattaa 10 prosenttia koko maailman elektroniikkatuotannosta. Väärennettyjen älypuhelimien markkina-arvo on noin 48 miljardia dollaria. Väärennetyt älypuhelimet, älypuhelinkomponentit ja älypuhelimissa käytettävät lisälaitteet ovat vakava turvallisuusriski, niin tietoturvan, kuin fyysisenkin turvallisuuden kannalta.

Haastateltavista kaksi oli tietoisesti ostanut aiemmin omistamaansa älypuhelimeen väärennetyn varaosan. Yksi vastaajista oli melko varma, että puhelimen huollon tehnyt liike ei käyttänyt virallisia, sertifioituja varaosia puhelinta huoltaessa. Haastateltavista kolme oli käyttänyt älypuhelimessaan väärennettyä lisälaitetta. Kysyttäessä väärennetyistä varaosista, haastateltavalle tarkennettiin, että esimerkiksi erimerkkisen laturin, mitä älypuhelin on, käyttäminen ei ole väärennetyn lisälaitteen käyttämistä. Väärennetyn lisälaitteen käyttäjät olivat käyttäneet juuri latureita, jotka oli joko tilattu Kiinasta tai ostettu ulkomailta muutaman euron hintaisina. Väärennetty laturi voi sisältää esimerkiksi komponentteja, joiden tarkoituksena on saastuttaa laturiin kiinnitettävä laite. Halpatuotettu laturi ei myöskään usein noudata niille asetettuja standardeja, jolloin vaarana on laitteen vaurioituminen tai tulipaloriski. Kukaan haastateltavista ei ollut koskaan ostanut täysin väärennettyä älypuhelinta.

Rauhalan (2022) esittämiin lukuihin verrattuna, haastateltavien käyttämien väärennettyjen älypuhelimien, älypuhelimien lisälaitteiden ja älypuhelinkomponenttien määrät olivat hyvin maltilliset. Tässä tuloksessa on huomioitava se, että tutkimuksen otanta oli melko pieni. Lisäksi kaikki haastateltavat henkilöt olivat suomalaisia. Elektroniikan myyntiä ja tuotantoa valvotaan Suomessa ja Euroopassa huomattavasti tarkemmin kuin esimerkiksi tietyissä osissa Aasia. Tästä voidaan päätellä, että väärennetyn elektroniikan hankkiminen Suomessa on huomattavasti hankalampaa.

6 YHTEENVETO JA POHDINTA

Tässä tutkielmassa käsiteltiin älypuhelimen määritelmä sekä kybertoimintaympäristön hierarkkinen rakennemalli ja muokattiin siitä älypuhelimille sopiva. Kybertoimintaympäristön hierarkkista rakennemallia käytettiin tutkielman viitekehyksenä, jonka tarkoituksena oli vastata seuraaviin tutkimuskysymyksiin:

- Millaiset älypuhelinkäyttäjien toimet parantavat älypuhelimien tietoturvaa?
- Millaiset älypuhelinkäyttäjien toimet heikentävät älypuhelimien tietoturvaa?

Tutkielman teoriaosassa käsiteltiin laajalti kybertoimintaympäristön hierarkkista rakennemallia erilaisissa ympäristöissä. Kun kybertoimintaympäristön hierarkkiseen rakennemalliin liittyvää aineistoa oli käsitelty tarvittava määrä, siitä pystyttiin muokkaamaan älypuhelimille sopiva, joka oli tarpeellinen tässä tutkielmassa. Älypuhelimiin kohdistuvia uhkia tarkasteltiin tutkielman teoriaosassa käyttäen kybertoimintaympäristön hierarkkista rakennemallia ja tarkastellen eri kerroksissa toimivia uhkia. Tutkielmassa kävi ilmi, että älypuhelimien maailmanlaajuisen yleistymisen myötä, myös älypuhelimiin kohdistetut erilaiset hyökkäykset ovat yleistyneet. Hyökkäysvektoreiden määrä ja laatu on jo verrattavissa tietokoneisiin suunnattuihin hyökkäysvektoreihin. Myös valtiolliset toimijat voivat kohdistaa hyökkäyksensä älypuhelimiin, jopa yksityistä hyökkääjää helpommin. Tämä tapahtuu asentamalla älypuhelimeen sen käyttöä seuraavia sovelluksia jo laitteen valmistusvaiheessa.

Tutkielman empiirisessä osassa viitekehyksen avulla tarkkailtiin älypuhelimiin suuntautuvien uhkien reittejä laitteisiin. Tällä tarkoitetaan sitä, että uhka voi suuntautua lopulta esimerkiksi semanttiseen kerrokseen, vaikka hyökkäys olisi päässyt läpi palvelukerroksesta. Hyökkäyksen lopullisen kohteen tutkiminen empiirisessä osiossa olisi vaatinut lisää resursseja. Tämän tutkiminen olisi kuitenkin kannattavaa jatkotutkimuksissa, joissa tutkittaisiin tarkemmin älypuhelimiin suuntautuvien uhkien riskiä. Tutkielman tutkimusmenetelmänä

käytettiin laadullista sisällönanalyysiä ja haastattelukysymykset olivat puolistrukturoituja.

Haastatteluiden kognitiivista kerrosta tarkastellessa oli huomioitavissa, että reagoiminen erilaisiin skenaarioihin ja haastateltavien suhtautuminen älypuhelimien tietoturvaan oli peruskäyttäjätasolla vähintäänkin hyvää. Mikäli haastateltavan omat tiedot ja taidot eivät riittäneet, olisi hän lähtökohtaisesti pyytänyt apua muualta. Näiden lisäksi esiintyi myös välinpitämättömyyttä älypuhelimen tietoturvaa kohtaan, mutta se oli hyvinkin marginaalista.

Tutkimushaastattelusta saatujen tulosten perusteella voidaan todeta, että palvelukerrokseen suuntautuvien uhkien määrä on suurin. Vaikka vain harvalla haastateltavista olikin asennettuna nykyisessä älypuhelimessaan epäluotettavasta lähteestä ladattava sovellus, oli silti luottamus sovelluskauppojen sovelluksiin ja sovelluskaupoista ladattujen sovellusten määrä suuri. Aiempien tutkimusten perusteella, myös sovelluskaupasta ladattavien sovellusten kohdalla tulisi harkita tarkkaan sovelluksen lataamisen tarpeellisuutta ja miettiä sovelluksen luotettavuutta. Suurin osa haastateltavista kuitenkin päivitti sovelluksiaan säännöllisesti ja yleisimmin käytetyt sovellukset olivat laajalti tunnetuilta kehittäjiltä. Tämän perusteella tutkija voi todeta, että palvelukerroksen osalta haastateltavien tietoturvakäyttäytyminen oli vähintäänkin tyydyttävää.

Semanttisen kerroksen osalta haastateltavien tietoturvatuntemus oli hyvää. Ainoita esille nousseita tietoturvauhkia olivat laitteiden lukituskoodien vaihtovälit sekä julkisten USB-latausporttien käyttö. Lukituskoodin hyödyntäminen vaatii kuitenkin jo saastunutta puhelinta tai pahantekijän pidempiaikaista älypuhelinkäyttäjän seurantaa. Lukituskoodien kompleksisuuden tietäminen olisi tuonut tutkimukselle huomattavaa lisäarvoa, mutta tämän kysymistä pidettiin epäsopivana. USB-latausportteja käyttävät haastateltavat mainitsivat, että käyttävät kyseisiä portteja hyvin harvoin.

Syntaktisen kerroksen osalta haastateltavien toiminta oli tutkijan mielestä kiitettävää. Suurin osa haastateltavista suorittaa järjestelmäpäivitykset aina mahdollisimman pian. Kukaan haastateltavista ei myöskään ole enää asettanut juuritason oikeuksia älypuhelimelleen.

Suojautuminen fyysisen kerroksen uhkilta oli tutkijan mielestä hyvää. Suurin osa haastateltavista suojaa laitettaan fyysisiltä vaurioilta ja pyrkii toimillaan estämään laitteen vaurioitumisen tai katoamisen. Suurin osa haastateltavista oli hajottanut joko nykyisen tai aiemman älypuhelimensa niin, että se vaatii huoltoa. Kyseessä on kuitenkin kannettava laite, jolloin inhimillinen tekijä nostaa laitteen hajoamisen riskiä. Hajonneen laitteen kohdalla käytännössä ainut uhka kuitenkin on, että laitteeseen tallennettua tietoa katoaa. Väärennettyjen laitteiden, komponenttien ja lisälaitteiden käyttö oli hyvin alhaista, vaikka näitäkin esiintyi. Yleisesti voidaan todeta, että haastateltavien tietoturvatuntemus älypuhelimien peruskäyttäjinä on hyvä.

Tämän tutkimuksen perusteella, jatkotutkimusta kannattaisi paneutua tarkemmin palvelukerroksesta löytyviin ongelmakohtiin. Tutkimus, joka sisältäisi uhkaraportin tekemisen tutkimukseen osallistuvien älypuhelimiin

asennetuista sovelluksista antaisi tarkempaa kuvaa sovellusten luomista uhkista ja riskeistä. Lisäksi Rauhalan (2022) mainitsemien lukujen perusteella, kasvattamalla otantaa olisi löydettävissä myös väärennettyjen älypuhelimien käyttäjiä. Väärennetty älypuhelin on itsessään uhkana erittäin suuri. Tästä syystä olisi mielekästä tutkia, miksi ihmiset käyttävät väärennettyjä älypuhelimia ja ovatko väärennettyjen älypuhelimien omistajat täysin tietoisia niiden aiheuttamista tietoturvauhkista. Tässä tutkielmassa luotiin valmis viitekehys kybertoimintaympäristön hierarkkisesta rakennemallista älypuhelinkontekstissa, jonka käyttö tulevissa tutkimuksissa on suotavaa.

LÄHTEET

Android Ohjeet (2022a), *Uuden Android-puhelimen käytön aloittaminen,* Haettu 23.7.2022 osoitteesta https://support.google.com/android/answer/10904410?hl=fi

Android Ohjeet (2022b), *Kaksivaiheisen vahvistuksen laittaminen päälle,* Haettu 5.9.2022 osoitteesta https://support.google.com/accounts/answer/185839?hl=fi&co=GENIE.Platform%3DAndroid

Apple Community (2021) *Lost phone & no other device,* Haettu 5.9.2022 osoitteesta https://discussions.apple.com/thread/252835991

Apple Support (2022a), *iPhonen, iPadin ja iPod touchin käyttöönotto,* Haettu 23.7.2022 osoitteesta https://support.apple.com/fi-fi/HT202033

Apple Support (2022b), *Apple ID:si kaksiosaisen todennuksen hallitseminen iPhonella,* Haettu 5.9.2022 osoitteesta https://support.apple.com/fi-fi/guide/iphone/iphd709a3c46/ios

Aviv, A. J., Davin, J. T., Wolf, F., & Kuber, R. (2017). Towards baselines for shoulder surfing on mobile authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (pp. 486-498).

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). *A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76(1), 139-154.*

Bošnjak, L., & Brumen, B. (2019). *Shoulder surfing: From an experimental study to a comparative framework. International Journal of Human-Computer Studies, 130, 1-20.*

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In Security and Privacy (SP), 2011 IEEE Symposium on (pp. 96-111). IEEE

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security*.

Davis, G., Samani, R. (2018). McAfee Mobile Threat Report Q1, 2018

Di Sorbo, A., & Panichella, S. (2021). Exposed! a case study on the vulnerability-proneness of google play apps. *Empirical Software Engineering*, *26*(4), 78.

Faraj, S. & Sambamurthy, V. (2006). Leadership of Information Systems Development Projects. *IEEE Transactions on Engineering Management, 53(2),* 238–249.

Gaw, D. C. (2016). *U.S. Patent No. 9,401,977*. Washington, DC: U.S. Patent and Trademark Office.

Guri, M. (2021). GAIROSCOPE: Leaking Data from Air-Gapped Computers to Nearby Smartphones using Speakers-to-Gyro Communication. In *2021 18th International Conference on Privacy, Security and Trust (PST)* (pp. 1-10). IEEE.

Hirsjärvi, S., & Hurme, H. (2000). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2007). Tutki ja kirjoita. (13.-14. Osin uudistettu painos). Helsinki: Tammi.

Hussain, M., Al-Haiqi, A., Zaidan, A. A., Zaidan, B. B., Kiah, M. M., Anuar, N. B., & Abdulnabi, M. (2016). The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks. *Pervasive and Mobile Computing*, *25*, 1-25.

Ibrahim, T. M., Alarood, A. A., Chiroma, H., Al-garadi, M. A., Rana, N., Muhammad, A. N., ... & Gabralla, L. A. (2019). Recent advances in mobile touch screen security authentication methods: A systematic literature review. *Computers & Security*, *85*, 1-24.

Islam, N., & Want, R. (2014). Smartphones: Past, present, and future. IEEE Pervasive Computing, 13(4), 89-92.

Jiang, Y., Ji, X., Wang, K., Yan, C., Mitev, R., Sadeghi, A. R., & Xu, W. (2022). WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 984-1001). IEEE

Jiang, X., & Zhou, Y. (2012). Dissecting android malware: Characterization and evolution. In *2012 IEEE Symposium on Security and Privacy* (pp. 95-109). IEEE.

Juuti, P. & Puusa, A. (2020). Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus.

Kielitoimiston sanakirja (2020). *Älypuhelin.* Haettu 5.12.2020 osoitteesta https://www.kielitoimistonsanakirja.fi/#/%C3%A4lypuhelin?source=suggestion&searchMode=all

Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951*.

Leavitt, N. (2011). Mobile security: finally a serious problem?. Computer, 44(6), 11-14.

Lehto, M. (2018). The modern strategies in the cyber warfare. In *Cyber Security: Power and Technology* (pp. 3-20). Springer, Cham.

Lehto, M., Neittaanmäki, P., Pöyhönen, J., & Hummelholm, A. (2022). Cyber Security in Healthcare Systems. In *Cyber Security* (pp. 183-215). Springer, Cham.

Lehto, M., Pöyhönen, J., & Lehto, M. (2019). *Kyberturvallisuus sosiaali-ja terveydenhuollossa.*

Keusch, F., Struminskaya, B., Antoun, C., Couper, M. P., & Kreuter, F. (2019). *Willingness to participate in passive mobile data collection. Public opinion quarterly, 83(S1), 210-235.*

Li, Y., Li, D., Cui, W., & Zhang, R. (2011). Research based on OSI model. In *2011 IEEE 3rd International Conference on Communication Software and Networks* (pp. 554-557). IEEE.

Libicki, M. (2007). *Conquest in Cyberspace, National Security and Information Warfare.*

Mayer, P., Zou, Y., Schaub, F., & Aviv, A. J. (2021). " Now I'm a bit {angry:}" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 393-410).

Maslennikov, D. (2011). *Mobile malware evolution: An overview, part 4. Disponibile*

Muslukhov, I. (2012). Survey: Data protection in smartphones against physical threats. *Term Project Papers on Mobile Security. University of British Columbia*.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. Information and Organization, 17(1), 2-26.

National Vulnerability Database (2022a). *CVE-2021-1905.* Haettu 18.3.2022 osoitteesta https://nvd.nist.gov/vuln/detail/CVE-2021-1905

National Vulnerability Database (2022b). *CVE-2021-1905.* Haettu 18.3.2022 osoitteesta https://nvd.nist.gov/vuln/detail/CVE-2021-1906

Norri-Sederholm, T., Laitinen, T., Lehto, M., & Kari, M. (2019). Health care and cyber threats. *Finnish Journal of eHealth and eWelfare*, *11*(1-2).

Nguyen-Vu, L., Chau, N. T., Kang, S., & Jung, S. (2017). Android rooting: An arms race between evasion and detection. *Security and Communication Networks*, *2017*.

Patton, M. Q. (1990). Qualitative evaluation and research methods. Thousand Oaks, California, US: Sage Publications, Inc.

Peda (2020). *Älypuhelimen määritelmä*. Haettu osoitteesta 5.12.2020 https://peda.net/kouvola/kk/tietotekniikka/p/asiakirjan-muokkaus/o

Peng, S., Yu, S., & Yang, A. (2014). *Smartphone malware and its propagation modeling: A survey*. IEEE Communications Surveys & Tutorials, 16(2), 925-941.

Rastogi, V., Chen, Y., & Jiang, X. (2014). *Catch Me If You Can: Evaluating Android Anti-Malware Against Transformation Attacks*. *IEEE Trans. Information Forensics and Security*, *9*(1), 99-108.

Rauhala, J. (2022). Physical Weaponization of a Smartphone by a Third Party. In *Cyber Security: Critical Infrastructure Protection* (pp. 445-460). Cham: Springer International Publishing.

Reidt, T. *What is Firmware? Emteria.* Haettu 31.5.2022 osoitteesta https://emteria.com/learn/firmware

Sarajärvi, A., & Tuomi, J. (2017). *Laadullinen tutkimus ja sisällönanalyysi: Uudistettu laitos*. Tammi.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010). *Google android: A comprehensive security assessment. IEEE Security & Privacy,* (2), 35-44.

Statista (2019) Number of smartphone users worldwide from 2016 to 2021. Haettu 2.12.2020 osoitteesta https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Sun, S. T., Cuadros, A., & Beznosov, K. (2015). Android rooting: Methods, detection, and evasion. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices* (pp. 3-14).

Tilastokeskus (2018). *Internetiä käytetään yhä yleisemmin matkapuhelimella – myös ostosten tekemiseen.* Haettu 2.12.2020 osoitteesta http://tilastokeskus.fi/til/sutivi/2018/sutivi_2018_2018-12-04_tie_001_fi.html?ad=notify

Wright, J., Dawson, M. E., & Omar, M. (2012). *Cyber security and mobile threats: The need for antivirus applications for smart phones. Journal of Information Systems Technology and Planning*, 5(14), 40-60.

Yang, S. J., Choi, J. H., Kim, K. B., & Chang, T. (2015). New acquisition method based on firmware update protocols for Android smartphones. *Digital Investigation*, *14*, S68-S76

LIITE 1 KYSYMYSRUNKO

Kognitiivinen kerros

- Oletko koskaan huomannut joutuneesi tietoturvaloukkauksen uhriksi älypuhelimen käytön takia, jos olet niin millaisen?

- Miten toimisit konkreettisesti tilanteeseen, jossa saisit kuulla älypuhelimeesi asennetun sovelluksen:

1) joutuneen kolmannen osapuolen tietomurron uhriksi,
2) sisältävän vakavia haavoittuvuuksia, joita on ehditty laajalti hyödyntää,
3) tuottajan laiminlyöneen tuotteen tietoturvaa tai
4) olleen tarkoituksella haitallinen?

- Miten koet älypuhelimen käytön turvallisuuden kannalta suhteessa tietokoneeseen? (Turvallisempaa, hieman turvallisempaa, yhtä turvallista, hieman turvattomampaa, turvattomampaa)

- Onko suhtautumisesi älypuhelimien tietoturvaan muuttunut siitä lähtien, kun hankit ensimmäisen älypuhelimesi? Jos on, niin miten?

- Käytätkö älypuhelinta eri tavalla julkisilla paikoilla, kuin yksin ollessa? Jos kyllä, niin miten?

- Mietitkö älypuhelinta kuljettaessasi sen varastamisen mahdollisuutta? Millä tavalla?

Palvelukerros

- Oletko ikinä ladannut sovelluksia virallisen sovelluskaupan ulkopuolelta? Jos olet niin millaisia ja mistä?

- Onko älypuhelimeesi hankittu erikseen laitteen turvallisuutta tai käyttäjän yksityisyyttä parantavia sovelluksia?

- Millaisia sovelluksia puhelimeesi on asennettu?

- Millaisia sovelluksia pääsääntöisesti käytät älypuhelimellasi? (Sosiaalinen media, pikaviestipalvelut, suoratoistopalvelut, pelit, hyötysovellukset yms.)

- Kuinka monta applikaatiota suunnilleen olet itse siihen asentanut?

- Asteikolla 1-5, kuinka luotettavana pidät virallisesta sovelluskaupasta asennettuja sovelluksia?

- Asteikolla 1-5, kuinka luotettavana pidät virallisen sovelluskaupan ulkopuolelta asennettuja sovelluksia?

- Päivitätkö älypuhelimeesi ladatut sovellukset säännöllisesti?

- Ota henkilökohtainen puhelimesi esiin, montako sovellusta on tällä hetkellä sovelluskaupassa päivittämättä?

Semanttinen kerros

- Millaista lukitusta käytät älypuhelimessasi? (Vahva lukitus sekä helppokäyttölukitus)

- Kuinka usein vaihdat puhelimesi lukituskoodia?

- Noudatetaanko työpaikallasi joitakin älypuhelimen käyttöön liittyviä tietoturvakäytäntöjä? (esimerkiksi millaisia sovelluksia puhelimeen saa asentaa, missä ympäristöissä puhelinta saa käyttää, kuinka usein lukituskoodit yms. salasanat pitää vaihtaa)

- Ovatko yrityksessäsi käytettävät käytännöt vaikuttaneet henkilökohtaisen älypuhelimesi käyttöön?

- Onko älypuhelimeesi tallennettuna sinulle tai muille arkaluontoista dataa tai informaatiota?

- Onko älypuhelimeesi tallennettu yrityksesi tai yrityksen asiakkaan kannalta arkaluontoista, salaista tai turvaluokiteltua dataa tai informaatiota?

- Lataatko älypuhelintasi julkisissa latauspistokkeissa, joissa on tarjolla ainoastaan USB-A tai USB-C portti?

- Käytätkö julkisia latauspistokkeita käyttäessäsi datablockeria?

Syntaktinen kerros

- Päivitätkö puhelimesi käyttöjärjestelmän säännöllisesti ja kuinka usein?

- Onko älypuhelimeesi saatavilla vielä päivityksiä?

- Oletko koskaan rootannut/jailbreakannut älypuhelintasi? (nykyistä tai aiempaa? myös työpuhelin)

- Liitätkö älypuhelintasi usein avoimeen julkiseen wifi-verkkoon? (junassa, lentokentällä, ravintoloissa)

Fyysinen kerros

- Oletko koskaan kadottanut älypuhelintasi? Jos olet, miten reagoit tilanteeseen?

- Jos edellinen ei: Miten toimisit, jos kadottaisit?

- Onko puhelimessasi käytössä älypuhelimen etädisablointi ja lukitus? Tiesitkö kyseisestä ominaisuudesta?

- Suojaatko älypuhelintasi fyysisiltä vaurioilta? jos kyllä, niin miten?

- Oletko koskaan hajottanut älypuhelintasi tahattomasti niin, että siitä on tullut käyttökelvoton?

- Oletko koskaan ostanut älypuhelimeesi väärennettyä varaosaa? Esimerkiksi akku, näyttö tai kamera?

- Oletko koskaan ostanut väärennettyä älypuhelinta?

- Oletko käyttänyt älypuhelimessasi väärennettyjä, ei standardoituja lisälaitteita? Esimerkiksi kuulokkeet tai laturi.

LIITE 2 ESITIETOLOMAKE

Esitietolomake

Nimi:

Ikä:

Ammattinimike/työtehtävä:

Toimitko tietoturva-/kyberturva-asiantuntijana? kyllä / en

Toimitko mobiililaiteasiantuntijana? kyllä / en

Millainen on mielestäsi tietoturvatuntemuksesi: erinomainen kiitettävä hyvä tyydyttävä välttävä

Teknologinen osaamisesi älypuhelimien osalta on: erinomainen kiitettävä hyvä tyydyttävä välttävä

Minkä merkkistä ja mallista älypuhelinta käytät? (Henkilökohtainen puhelin ja työpuhelin)

Milloin olet hankkinut ensimmäisen älypuhelimesi?

Monta eri älypuhelinta sinulla on ollut käytössä?

Onko älypuhelimissasi ollut eri käyttöjärjestelmiä? (esim. Android, iOs)