Patrik Elfvengren

OPEN BANKING API-RAJAPINTOJEN TIETOTURVARISKIT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Elfvengren, Patrik
Open banking api-rajapintojen tietoturvariskit
Jyväskylä: Jyväskylän yliopisto, 2022
Tietojärjestelmätiede, Kandidaattitutkielma
Ohjaaja: Pekkala, Kaisa

Avoimen tiedon saatavuudesta on tullut tavoiteltava arvo kaikilla aloilla. Tämä pätee myös rahoitusalaan, jossa EU on ennakoinut tämän suhteen ja asettanut rajat toiminnalle toisen maksupalveludirektiivin muodossa (PSD2). Tämä direktiivi edellyttää pankkeja avaamaan heidän API-rajapintansa kolmansien osapuolien maksupalveluiden tarjoajille, jotka voivat tämän avulla tuoda parannettuja palveluita markkinoille käyttäen pankin asiakkaiden pankkitietoja heidän luvallansa. Tämä direktiivi lisää läpinäkyvyyttä ja kilpailua pankkisektorilla. API (Application programming interface) on teknologia, jonka avulla kaksi eri ohjelmaa voi keskustella keskenään ja lähettää tietoa käyttäen yhteistä kieltä. Tämä rajapinta on direktiivissä mainittu suositeltavana teknologiana. API-rajapintojen yleisempiä tietoturvariskejä on tutkittu laajasti ja ne kuvataan myös tässä tutkielmassa. Toisen maksupalveludirektiivin myötä on myös syntynyt Open banking -käsite (OB), joka kuvaa tätä PSD2 mukaista toimintamallia universaalimpana käsitteenä. Tämä toimintamalli herättää luontaisesti huolta käyttäjien kallisarvoisten pankkitietojen turvallisuudesta, kun kolmansille osapuolille annetaan mahdollisuus käyttää asiakkaiden tilitietoja palveluiden tuottamisessa. Tässä tutkielmassa tunnistettiin kirjallisuuskatsauksen muodossa näitä mahdollisia riskejä API-rajapinnan teknisellä ja organisatorisella käyttöönottoon liittyvällä tasolla keräämällä tietoa olemassa olevasta tutkimustiedosta aiheesta. Aihetta ei ole entuudestaan tutkittu vielä riittävästi, johtuen koko ilmiön tuoreudesta. Tämä tutkielma auttaa tunnistamaan olemassa olevia riskejä OB API-rajapintojen kehittämiseen ja ylläpitoon liittyen.

Asiasanat: Open banking, PSD2, API, tietoturva

ABSTRACT

Elfvengren, Patrik
Open banking's API information security threats
Jyväskylä: University of Jyväskylä, 2022.
Information systems, Bachelor's thesis
Supervisor: Pekkala, Kaisa

Open access to information has become value to be pursued in every industry. This also applies to financial industry, where EU has anticipated this by setting the boundaries for operating in the form of a second payment directive (PSD2). This directive requires banks to open their APIs to third-party payment service providers, who can then offer enhanced products to marketplace by using the customers' account information with their consent. This directive increases transparency and competition in the banking sector. API (Application programming interface) is a technology, that allows two programs to communicate with each other and transfer data by using a common language. This interface technology is being recommended in the directive. APIs most common information security risks has been studied broadly and they are also discussed in this study. With the concept of PSD2 there has also arisen the concept of Open banking (OB), which represents the PSD2 way of working in a much universal concept. This model naturally raises worries for the security of the valuable customers banking information, when the third parties are given the chance to use customers account information in providing services. In this study these possible risks were recognized on the technical level and on the organizational implementation related level by gathering information from already existing research data in the form of a literature review. This subject has not been yet studied enough, due to the novelty of this phenomenon. This study helps to recognize existing risks in OB API development and management.

Open banking: API, PSD2, information security

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Teknologinen muutos on kiihtymässä rahoitusalalla samaan aikaan kun pankkipalveluiden lisääntyvä käyttö jatkaa nousuaan (Boot ym., 2021). Tiedon helpommasta saatavuudesta on tullut myös tärkeä aihe kaikilla aloilla, mukaan lukien rahoitusalalla. Esimerkiksi, G20 korruption vastainen työryhmä on määritellyt avoimen tiedon olevan prioriteettina julkisen sektorin läpinäkyvyyden ja rehellisyyden kehittämisessä. Kaupallisesta näkökulmasta katsottuna, tieto voi toimia katalyyttinä uusille tuotteille ja liiketoimintamalleille. EU on ennakoinut tällä rintamalla asettamalla säännöt toiminnalle toisen maksupalveludirektiivin (PSD2) muodossa (Brodsky & Oakes, 2017). Tästä on seurannut Open banking (OB) käsitteen synty. OB kuvaa aivan omanlaista finanssiekosysteemiä. Ekosysteemi tarjoaa kolmansien osapuolien finanssipalveluiden tarjoajille vapaan pääsyn kuluttajapankki-, pankkitapahtuma- ja muihin pankkitietoihin pankeista ja pankkien ulkopuolisista rahoituslaitoksista käyttäen avoimia sovellusten ohjelmoitavia rajapintoja (API) (Laplante & Kshetri, 2021). OB-malli edistää siis avointa kilpailua ja läpinäkyvyyttä pankkisektorilla.

Muutos tuo kuitenkin tullessaan riskejä. Digitaaliset innovaatiot ja teknologiaan perustuvat liiketoimintamallit voivat luoda uusia liiketoiminta mahdollisuuksia yrityksille, tai ne voivat sekoittaa rahoitusalan rakenteita hämärtämällä sen rajoja (Navaretti ym., 2018). Avoimet API-rajapinnat (application programming interface) herättävätkin huolta arvokkaiden pankkitietojen turvallisuudesta. D. Kelezzin ym. (2019) mukaan pankkitietojen paljastaminen kolmansien osapuolien palveluntarjoajille API-rajapintoja käyttäen nostaa esiin useita kyberturvallisuus ongelmia.

API (Application programming interface) on yksinkertaistettuna teknologia, joka mahdollistaa kahden ohjelman välisen kommunikaation ja tiedonsiirron käyttäen kieltä, jotka molemmat osapuolet ymmärtävät. Rajapinnat jaetaan yleisesti kahteen eri luokkaan; julkisiin ja yksityisiin. Julkinen rajapinta on kaikkien saatavilla, kun taas yksityinen on vain esimerkiksi saatavilla jonkin organisaation sisällä. (Jacobson ym. 2011)

Yleisimmistä API-rajapintojen tietoturvariskeistä on tehty paljon omia tutkimuksiaan, mutta OB API näkökulmasta vastaavanlaisia tutkimuksia

hyvin vähän. Koska aihe on uusi, on siitä tällä hetkellä vielä melko vähän tutkimustietoa, joka käsittelisi laajasti eri riskejä OB-ratkaisujen käyttöönottoon ja hallintaan liittyen. Kuten Kellezzi ym. (2019) mainitsi, vaarannettuna on pankin asiakkaiden pankkitiedot ja tämän vuoksi aiheen tutkiminen on tärkeää.

Tässä kirjallisuuskatsauksena toteutetussa tutkielmassa tarkastellaan OB tyyppisten ratkaisujen turvallisuutta ja siihen liittyviä riskejä erityisesti rajapintatasolla. Tavoitteena on olemassa olevan kirjallisuuden avulla koostaa OB API tietoturvariskejä ja myös soveltaa argumentoiden yleisiä API tietoturvariskejä OB kontekstiin, sillä suoraan OB kontekstissa näitä riskejä ei ole vielä tieteellisessä kirjallisuudessa käsitelty riittävästi. Tätä kautta tutkimus pyrkii auttamaan rahoitusalan toimijoita ja sen sidosryhmiä kehittämään ja kontrolloimaan OB API-rajapintoja valistamalla tähän liittyvistä mahdollisista riskeistä. Tutkimuksessa etsitään seuraaviin tutkimuskysymyksiin vastauksia:

- Mikä on Open banking ja mikä on käsitteen taustat?
- Mitä riskejä on otettava huomioon Open banking API-rajapintojen käyttöönotossa ja hallinnassa?
- Miksi Open banking API-rajapintojen riskien tunnistaminen on tärkeää?

Tutkielmassa käytetty kirjallisuus on pääsääntöisesti tieteellisiä artikkeleja tai muita tieteellisiä julkaisuja. Tavoitteena on käyttää mahdollisimman paljon vertaisarvoitua materiaalia, mutta koska tutkielman aihepiiri on niin tuore, on lähteiden hankinnassa jouduttu soveltamaan paljon. Tiedon hankintaa on pääsääntöisesti tehty käyttäen IEEE Xplore ja Google Scholar -hakutietokantoja. Lisäksi tutkielmassa on käytetty paljon alan yritysten dokumentteja.

Tutkielmassa ensiksi määritellään keskeiset käsitteet aiheeseen liittyen ja avataan aiheen taustaa näiden käsitteiden avulla tutkielman kannalta olennaiselta osin. Tämän jälkeen tutkielman kolmannessa luvussa keskitytään tunnistamaan olemassa olevia OB API tietoturvariskejä käyttäen lähdekirjallisuutta ja soveltamalla aiemmin tutkielmassa läpikäytyjä taustatietoja ja käsitteitä.

Tutkielmassa löydettiin muutama mainittava riski OB API teknisellä tasolla, sekä organisatorisiin käyttöönottoon ja hallintaan liittyvällä tasolla. Riskit jaettiin näihin kahteen eri osioon. Organisatorisiin riskeihin lukeutui riskit liittyen muutokseen, jonka keskellä pankkisektori on. Riskit liittyivät enimmäkseen pankkien ja heidän kanssansa yhteistyötä tekevien FinTech yritysten toiminnan eroavaisuuksiin, josta voi seurata ongelmia (Zachariadiksen & Ozcanin 2017). FinTech (financial technology) tarkoittaa yritystä, joka tarjoaa moderneja teknologiaratkaisuja rahoitusalalla (Saksonova & Kuzmina-Merlino, 2017). Lisäksi riskiksi osoittautui julkisten API-rajapintojen julkaisu ja niiden kontrollointi (Leaden ym., 2017, Tang ym., 2015).

Teknisellä tasolla löytyi riskejä pitkään yleisesti käytetyn TLS protokollan käyttöön, johon OB API perustuu. TLS (Transport Layer Security) koostuu monista kryptografisista protokollista, jotka on suunniteltu tarjoamaan turvallinen kommunikaatio verkon yli. (Soldatos ym., 2020) Tutkielmassa myös mainittiin OB API riskeiksi OWASP API Security Top 10 – 2019 -listassa mainitut riskit,

sillä nämä riskit pätevät kaikkien API-rajapintojen kehittämiseen ja käyttöön (OWASP, 2019).

2 TAUSTA

Tässä luvussa tutustutaan Open bankingiin käsitteenä, käsitteen taustaan sekä muihin tärkeimpiin käsitteisiin, jotka liittyvät tutkielman aiheeseen. Tämä luku toimii johdatuksena tutkielman aihepiiriin ja luo perustaa tutkielman loppupuoliskon OB:in API-rajapintojen tietoturvariskien tunnistamiseen ja ymmärtämiseen. Tämä kuku mahdollistaa sen, että seuraavassa luvussa lukija ymmärtää välttämättömät käsitteet ja ilmiöt niiden taustalla näiden riskien tunnistamiseen ja niiden ymmärtämiseen liittyen.

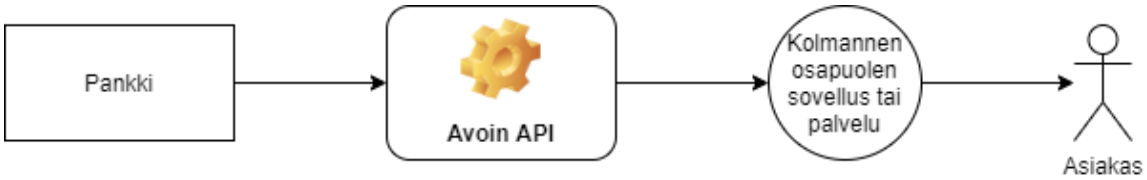
2.1 Open banking

Euroopan Unioni julkaisi vuonna 2015 toisen maksupalveludirektiivin (PSD2), jonka myötä pankkitunnuksien omistaminen siirtyi yksittäisille henkilöille itselleen, sen sijaan, että pankki omistaisi ne. Tämän seurauksen syntyi Open banking -käsite (OB), joka tarkoittaa pankkien API-rajapintojen avaamista kolmansien osapuolien palveluntarjoajille (Kellezi ym., 2019). Käsite tuli ensimmäisen kerran suuremmin esille sen jälkeen, kun Yhdistynyt kuningaskunta julkaisi heidän vastineen EU:n toiselle maksupalveludirektiiville. Tarjotakseen standardin API-rajapinnan asiakkaiden tietojen jakoon useampien pankkien välillä, Yhdistynyt kuningaskunta julkaisi Open banking standardin (Almehrej ym., 2020).

OB voidaan kuitenkin nähdä paljon laajempanakin kuin vain direktiivinä ja standardina. OB-käsite voidaan määritellä yhteistyömallina, jossa pankkitietoja jaetaan API-rajapintoja käyttäen kahden tai useamman riippumattoman osapuolen välillä parannettujen ominaisuuksien tarjoamiseksi markkinoille (Brodsky & Oakes, 2017). Käsite kuvaa siis uudenlaista toimintamallia pankkisektorilla kuluttajien tietojen käsittelyssä ja jakamisessa, joka tarjoaa aivan uudenlaisia mahdollisuuksia.

Seuraava Kuvio 1 havainnollistaa näitä molempia määritelmiä hyvin. Kuvio 1 perustuu monen eri OB API-rajapintoja tarjoavan yrityksen ja monen eri

pankkisektorin blogin havainnollistukseen, kuinka OB yksinkertaistettuna toimii ja mitä se tarkoittaa.



KUVIO 1, Open banking (*Open Banking - WSO2 Open Banking Accelerator Documentation*, ei pvm., *How to Use Open Banking API for Your Fintech App?*, ei pvm., ”How Open Banking Is Revolutionizing the Banking Industry”, 2019)

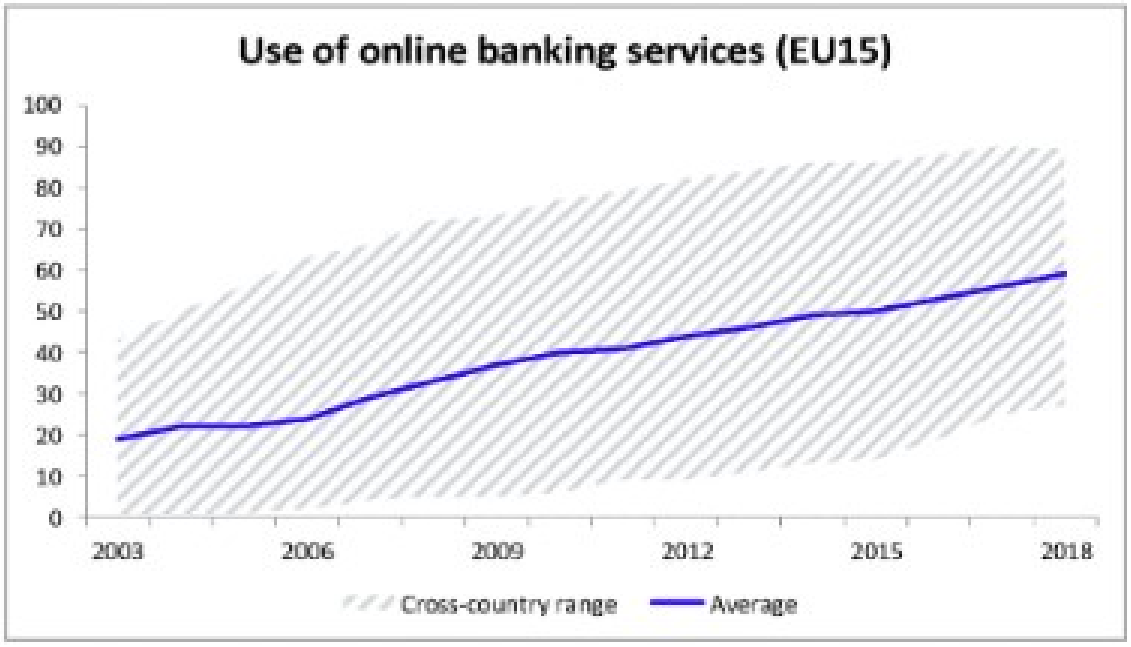
Kuvio 1 havainnollistaa siis sitä, kuinka pankki jakaa avoimen API-rajapinnan avulla asiakkaan pankkitietoja kolmansien osapuolien palvelun tarjoajille, jotka taas käyttävä näitä tietoja uusien tuotteiden tarjoamiseen kuvion oikean laidan asiakkaalle.

Seuraavissa alakappaleissa avataan tarkemmin jo tässä kappaleessa mainittuja tärkeimpiä käsitteitä liittyen OB:iin.

2.2 PSD2

OB-käsite ja sen mukainen toiminta malli ei syntynyt itsestään suoraan tarpeesta luoda läpinäkyvyyttä ja kilpailua pankkisektorille, vaan se syntyi seurauksena EU:n sääntelystä. Vuonna 2007, ensimmäinen Euroopan parlamentin maksupalveludirektiivi (PSD) tuli voimaan. Sen tavoitteena oli luoda yleiset vaatimukset sähköisille maksutavoille kuten esimerkiksi luottokorteille ja verkkopankki maksuille ja tätä kautta luoda tehokkaat markkinat maksu palveluille (Romanova ym., 2018). Tämä oli siis ensimmäinen maksupalveluita koskeva direktiivi, jolla ei ollut vielä suoraa vaikutusta OB-käsitteelle.

Vajaa kymmenen vuotta myöhemmin seurasi tässä tutkielmassa tarkemmin tarkastelussa oleva toinen maksupalveludirektiivi (PSD2). Ensimmäisen direktiivin tapaan, vuonna 2016 julkaistu PSD2 on sääntelevä viitekehys, jonka tarkoituksena on helpottaa rahan siirtoja laajentamalla maksupalveluntarjoajien sekä niiden käyttäjien tiedon saatavuutta, oikeuksia ja vaatimuksia (Zachariadis & Ozcan, 2017). PSD2 mahdollistaa siis sen, että käyttäjä pääsee käsiksi omiin tilitietoihinsa muidenkin palveluiden kautta, kuin vain oman pankin tarjoaman portaalin kautta edellyttämällä vahvaa tunnistautumista (*Maksupalveludirektiivi PSD2*, 2021). On myös hyvin todennäköistä, että tämän direktiivin tarpeeseen vaikuttaa verkkopankin kasvanut käyttö Euroopassa. Alla oleva kuva havainnollistaa tätä trendiä.



KUVIO 2, Verkkopankkien käyttö Euroopassa (Boot ym., 2021)

Kuten kuviosta 2 käy ilmi, verkkopankin käyttö EU:ssa oli vuonna 2003 19%, mutta se on noussut tasaisesti ja vuonna 2018 se oli jo 59% (Boot ym., 2021). Tällä trendillä voi olla myös vaikutusta maksupalvelu direktiivin päivitykselle, jotta tällä rahoitus alalla saadaan mahdollisimman hyvät olot avoimelle kilpailulle.

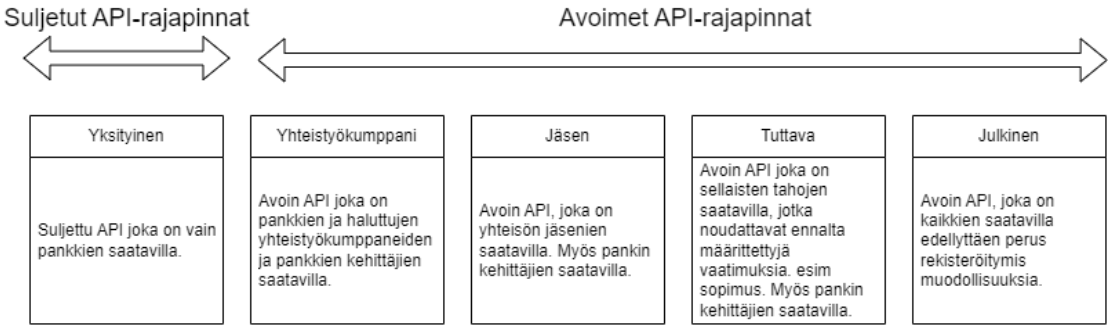
PSD2 on osa globaalia trendiä pankkisääntelyssä, joka korostaa turvallisuutta, innovointia ja markkinakilpailua. PSD2 edustaa merkittävää askelta kohti kaupallistamista EU:n pankkisektorilla edellyttämällä pankkeja tarjoamaan yhteydet muille päteville maksupalveluntarjoajille (payment service provider, PSP) asiakkaiden tilitietoihin ja maksujen suorittamiseen (Botta ym., 2018). Zachariadiksen ja Ozcanin (2017) mukaan PSD2 vaatii, että pankit avaavat API-rajapintansa kolmansien osapuolien palveluntarjoajille tavalla, joka noudattaa tarkasti asiakkaan hyväksyntää. Artikkelissa mainitaan myös, että direktiivi ei suoraan vaadi käyttämään API-teknologiaa, mutta se on yleisesti todettu kaikista luotettavamaksi ja käytetyimmäksi teknologiaksi käyttäjien tilien turvallisuuden kannalta. PSD2 on siis se direktiivi, joka vaatii Euroopassa käyttämään OB-tyyppistä toiminta mallia. Direktiivi toimi myös ikään kuin katalyyttinä OB-käsitteen synnylle.

2.3 API-rajapinta

Kuten aiemmassa kappaleessa mainittiin, PSD2 suosittelema OB-tyyppisen toimintamallin toteuttamisessa käytetty teknologia on API, ja siksi tämän käsitteen selittäminen on olennaista tämän tutkinnon osalta. Jacobson ym. (2011) määrittelee yksinkertaistettuna sovelluksen ohjelmoitavan rajapinnan eli API:n ratkaisuksi, jolla kaksi sovellusta voivat keskustella toisilleen verkon välityksellä käyttäen yleistä kieltä, jotka molemmat sovellukset ymmärtävät. API on tietynlainen paketti sääntöjä, joita noudattamalla ohjelmistot voivat kommunikoida keskenään. Se toimii siis rajapintana sovelluksien välillä, samalla tapaa kuin graafinen käyttöliittymä toimii rajapintana sovelluksen ja ihmisen välillä (Mosqueira-Rey ym., 2018).

Jacobsonin ym. (2011) mukaan API:t voidaan jakaa kahteen eri tyyppiin; yksityisiin ja julkisiin. Heidän mukaansa julkisen API:n määritelmä on se, että rajapinta on kenen tahansa saatavilla pienellä tai olemattomalla vaivannäöllä. Yksityinen API on taas sellainen, joka on käytössä vain jonkin organisaation sisällä, mutta johon tarvittaessa on myös pääsy organisaation kumppanilla ja suurimmilla asiakkailla, jos näin osapuolen kanssa sovitaan. Jacobson ym. (2011) mainitsevat kirjassaan, että jako yksityisen ja julkisen API:n välillä määrittelee pääosin organisaation liiketoiminnan järjestelyt.

Yksityiset API:t ovat Jacobsonin ym. (2011) mukaan yleisempiä, sillä yritykset, jotka tarjoavat julkisia API-rajapintoja omaavat myös suuren määrään heidän organisaationsa sisäisten järjestelmien välisiä API-rajapintoja, jotka eivät ole asiakkaiden tai kolmansien osapuolten palveluntarjoajien käytössä. He mainitsevat kirjassaan tällaisiksi esimerkkiorganisaatioksi Facebookin (nyk. Meta) ja Twitterin. Seuraavassa kuviossa kuvataan tarkemmin julkisten ja yksityisten API-rajapintojen jakoa pankki kontekstissa.



KUVIO 3, Erityyppiset API-rajapinnat (Premchand & Choudhry, 2018)

Kuviossa Premchand & Choudhry (2018) ovat kuvanneet juuri pankkien näkökulmasta tätä jakoa yksityisiin ja julkisiin API-rajapintoihin. Kuten kuviosta käy ilmi, julkisten API-rajapintojen alta löytyy hyvin monen erityyppisiä rajapintaratkaisuja, jotka on suunniteltu eri tahojen käytettäviksi. Jacobson ym. (2011) jako on siis hieman karkeampi kuin kuviossa esitetty malli, mutta siitäkin löytyy sama jako yksityisiin ja julkisiin rajapintoihin.

Tässä tutkielmassa käsitellään kuitenkin näitä pankin julkisia API-rajapintoja, jotka ovat keskeinen osa OB-toimintamallia. Tämänkin tutkielman aihepiirin osalta on tärkeä ymmärtää, että vaikka OB-käsite tarkoittaa pankin rajapintojen avaamista, se ei tarkoita sitä, että pankki avaisi kaikki sen organisaation käyttämien järjestelmien välisiä rajapintoja. Tarkoituksena on luoda rajapinta, jota kolmannen osapuolen palveluntarjoajat voivat käyttää ilman, että pankki altistuisi tietoturvariskeille.

2.4 API tietoturva riskit (OWASP API Security Top 10)

Tästä väliotsikon aiheesta voi, ja on tehtykin laajoja omia tutkimuksia. Tämän tutkielman kannalta ei ole tarkoituksen mukaista käsitellä aihetta niin mittavasti, joten tässä alakappaleessa keskitytään käsittelemään niitä tietoturva riskejä API-rajapintojen osalta, jotka mahdollisesti koskettavat tutkielman kannalta olennaisinta Open banking (OB) aihealuetta.

Osion otsikon kannalta tässä tutkielmassa on tehty rajaus käsittelemään ainoastaan yleisimpiä API tietoturvariskejä. Lähteenä näille yleisimmille tietoturvariskeille käytetään The Open Web Application Security Project (OWASP) yhteisön Top 10 listaa API tietoturva riskeistä. OWASP on avoin yhteisö, jonka tavoitteena on auttaa organisaatioita kehittämään, ostamaan ja ylläpitämään applikaatioita ja API-teknologioita, joihin voi luottaa (OWASP, 2019). Top 10 yleisimmät API tietoturvariskit on eritelty ja selitetty Taulukossa 1.

TAULUKKO 1, OWASP API Security Top 10 – 2019 (OWASP, 2019)

API1:2019 - Broken Object Level Authorization (BOLA)	Hyökkääjät voivat hyväksikäyttää API päätepisteitä, jotka ovat haavoittuvaisia BOLA:lle manipuloimalla objektin id:tä, joka lähetetään pyynnössä. Tämä voi johtaa luvattomaan pääsyyn arkaluonteisiin tietoihin.
API2:2019 - Broken User Authentication	Autentikointi menetelmät ovat usein toteutettu väärin, joka antaa hyökkääjille mahdollisuuden riskeerata API:n turvallisuuden.
API3:2019 - Excessive Data Exposure	Kehittäjillä on yleisesti tapana paljastaa kaikki objektin ominaisuudet huomioimatta niiden arkaluonteisuutta ja jättämällä vastuun asiakkaalle niiden suodattamisesta ennen käyttäjälle näyttämistä.
API4:2019 - Lack of Resources & Rate Limiting	API-rajapinnoissa ei usein ole rajoituksia resurssien siirroissa. Tämä voi johtaa suorituskyky ongelmiin ja tätä kautta autentikointi virheisiin.

API5:2019 - Broken Function Level Authorization	Monimutkaiset pääsynhallintakäytänteet johtavat yleensä autoritointi virheisiin. Näitä ongelmia hyödyntämällä hyökkääjät pääsevät käsiksi käyttäjien resursseihin ja/tai hallinnollisiin tehtäviin.
API6:2019 - Mass Assignment	Jos ominaisuuksia, jotka ovat käyttäjän syöttämiä ei suodateta, voi hyökkääjä vaikuttaa ominaisuuksiin, johon sillä ei kuuluisi olla pääsyä.
API7:2019 - Security Misconfiguration	Tietoturvan väärin konfigurointi johtuu yleensä epäturvallisesta oletus konfiguroinneista tai esimerkiksi vajaista tai tilapäisitä konfiguroinneista.
API8:2019 - Injection	Injektio virheitä ilmenee silloin, jos epäluotettavaa dataa lähetetään osana komentoa tai kyselyä. Tämä haitallinen data saattaa huijata ohjelmaa suorittamaan ei toivottuja komentoja tai antaa luvan käsitellä dataa, johon riittävää lupaa ei todellisuudessa ole.
API9:2019 - Improper Assets Management	Vanhat päivittämättömät API versiot ovat riski, sillä niiden tietoturva mekanismit eivät ole nykyaikaisia. Hyvällä dokumentaatiolla on tässä iso rooli, sillä se helpottaa haavoittuvuuksien tunnistamisen ja täten niiden korjaamisen.
API10:2019 - Insufficient Logging & Monitoring	Riittämätön monitorointi yhdessä tehottoman tapaukseen (incident) vastaamisen kanssa sallii hyökkääjille mahdollisuuden hyökätä järjestelmiin.

Artikkelin mukaan tavoitteena on näiden Top 10 tietoturvariskien avulla valistaa henkilöitä, jotka ovat mukana API kehityksessä ja ylläpidossa, kuten esimerkiksi kehittäjiä, suunnittelijoita, arkkitehtejä, johtajia tai organisaatioita. Tämän perusteella tämä pätee siis myös OB avoimien API-rajapintojen kehittämiseen.

Näiden edellä mainittujen riskien lisäksi, API-rajapintojen käyttöön liittyy paljon muitakin riskejä, jotka eivät ole pelkästään teknisellä tasolla tunnistettavissa. Tang ym., (2015) mukaan API-rajapintojen julkaiseminen organisaaton ulkopuolelle julkiseen käyttöön on koitumassa turvallisuuden ja menestyksen kannalta IT-osastoille merkittäväksi huolen aiheeksi. Tällaisessa tilanteessa siis turvallisuuden kannalta kontrollin merkitys kasvaa. Leaden ym., (2017) mukaan API turvallisuus on kuitenkin ennemmin erilaisten päällekkäisten standardien villi länsi, kuin sivistynyt ja turvallinen kaupunki. Kontrollointi on siis kuitenkin mainittava haaste rajapintojen ylläpidossa. Mosqueira-Rey ym., (2018) mukaan mitä useampi ohjelma käyttää yhtä samaa API-rajapintaa, sitä suuremmaksi riskiksi pienetkin ongelmat rajapinnassa suurentuvat. Tämä asetelma luo merkittävän riskin API turvallisuuden saralla.

Myös kontekstilla, johon API aiotaan julkaista, on merkitystä. Aiemmin mainitulla jaolla yksityisiin ja julkisiin API-rajapintoihin on merkitystä myös turvallisuuden kannalta. Tästä hyvä esimerkki on vuonna 2016 tutkijoiden

havaitsema haavoittuvuus Nissan Leaf sähköauton rajapinnassa. Auton käyttämään API-rajapintaan pääsi käsiksi kuka tahansa ilman kunnollista autentikointia. (Controlling Vehicle Features of Nissan LEAFs across the Globe via Vulnerable APIs, 2016) Tämä on hyvä esimerkki siitä, kuinka yksityisen ja julkisen APIn ominaisuudet voivat mennä sekaisin suunnitteluvaiheessa. Bhuiyan ym., (2018) mainitsevat myös, että yleisesti käytetyt julkiset API-rajapinnat eivät ole tarpeeksi turvallisia tarjotakseen turvallisuutta salassa pidettävän tiedon siirtämiseen. Heidän tutkimuksessansa valittiin satunnaisesti 60 julkista API-rajapintaa, joista 53 oli haavoittovuuksia omaava.

Nämä edellä mainitut riskit osoittautuvat tarkemman tarkastelun jälkeen ikään kuin ylemmän tason riskeiksi, joista moni Taulukon 1 riskeistä johtaa juonensa. Näiden löydöksien valossa on siis huomioitava, että API tietoturvariskejä on otettava huomioon organisaation ylemmän tason päätöksissä kuin myös aivan API kehittämisen teknisen tason päätöksissä. Näihin tietoturvariskeihin perehdytään tarkemmin OB kontekstissa tämän tutkielman seuraavassa kappaleessa, jossa esitetään edellä mainittujen riskien lisäksi uusiakin riskejä, jotka ovat olennaisia lähinnä OB:in osalta.

3 OPEN BANKING RISKIT

Tässä luvussa tunnistetaan Open bankingiin (OB) liittyviä tämänhetkisiä suurimpia riskejä. Riskejä on tunnistettu kirjallisuudesta joko artikkeleista, jotka suoraan käsittelevät OB-tyyppisiä avoimia API-rajapintoja tai artikkeleista, joissa käsitellään yleisiä API tietoturvariskejä, jotka ovat mahdollisia OB API kontekstissa. OB API tietoturvariskeistä ei ole vielä paljon tehty tutkimuksia, sillä aihe on niin tuore, mutta tässä luvussa pyritään tunnistamaan joitakin OB API riskejä yleisten API tietoturvariskien kautta, jotka täyttävät OB API yleisiä piirteitä.

Nämä eri riskit on tutkielmassa jaettu kahteen suurempaan eri luokkaan, joissa niitä käsitellään erikseen. Ensimmäinen luokka, jota käsitellään 3.1-osiossa, kattaa alleen ne OB API riskit, jotka liittyvät enemmän uuden OB toimintamallin käyttöönottoon pankkisektorilla. Toista luokkaa käsitellään osiossa 3.2, joka sisältää kirjallisuudessa tunnistettuja teknisen tason riskejä Open banking API-rajapinnoissa. Nämä riskit liittyvät siis enemmän rajapintojen teknisiin toettuuksiin, verrattuna ensimmäiseen osioon.

3.1 Organisatoriset ja käyttöönottoon liittyvät riskit

Pankkitietojen paljastaminen kolmansien osapuolien palveluntarjoajille avoimen API-rajapinnan avulla tuovat esiin useita kyberturvallisuuteen liittyviä ongelmia (Kellezi ym., 2019). Osa näistä ongelmista tai riskeistä eivät kuitenkaan liity suoraan aiemmin tässä tutkielmassa läpikäytyihin teknisen tason yleisimpiin API tietoturva riskeihin. Nämä riskit liittyvät lähinnä muutokseen, jonka keskellä pankkisektori on. Digitaaliset innovaatiot ja teknologiaan perustuvat liiketoimintamallit voivat luoda uusia liiketoiminta mahdollisuuksia yrityksille, tai ne voivat sekoittaa rahoitusalan rakenteita hämärtämällä sen rajoja (Navaretti ym., 2018). Brodsky & Oakes, (2017) mainitsevat artikkelissaan, että koska OB-mallin

tilanteessa on luontaisesti riski käyttäjän tietojen siirrossa, on tärkeää kehittää prosesseja ja hallintaa teknisen yhteyden tueksi.

Zachariadis & Ozcan, (2017) tutkimuksen mukaan FinTech yritykset, jotka tekevät yhteistyötä pankkien kanssa avoimien API-rajapintojen saralla, ovat osoittaneet huolensa pankkien toiminnan nopeudesta. FinTech (financial technology) tarkoittaa yritystä, joka tarjoaa moderneja teknologiaratkaisuja rahoitusalalla. FinTech yrityksillä on selkeä ajatus siitä, miten olemassa olevia palveluita rahoitusalalla voidaan parantaa. (Saksonova & Kuzmina-Merlino, 2017)

FinTech yrityksien osoittamat huolet kohdistuvat Zachariadiksen ja Ozcanin (2017) mukaan erityisesti pankkien hyväksynnän nopeuteen uusia tuotteita julkaistaessa markkinoille. Heidän tutkimuksensa mukaan nämä huolet eivät välttämättä johdu pelkästään perinteisestä start-up yrityksen ja vakiintuneen yrityksen välisestä ketteryyden erosta, vaan pankkien pitkään itse kantama vastuu tietoturvasta voi olla tässä ongelmassa myös vaikutuksena. Tämän tuotteen hyväksymisprosessin turvallisuuden parantaminen voi osoittautua haasteeksi FinTech-yrityksen ja pankin välisessä yhteistyössä toiminnan nopeuden osalta (Zachariadis & Ozcan, 2017).

Tällainen Zachariadis ja Ozcan (2017) mainitsema tuote voi siis olla tässä tutkielmassa tarkastelussa oleva Open banking (OB) avoin API-rajapinta. Hätiköinnin tai heikon yhteistyön tuloksena syntynyt OB API-rajapinta voi jäädä turvallisuuden konfiguroinnin osalta vajaaksi. Tämä onkin mainittu myös yhdeksi yleiseksi API-rajapinnan tietoturva riskiksi Taulukossa 1. "API7:2019 - Security Misconfiguration "- (OWASP, 2019).

Jo aiemmassa luvussa käsiteltiin yleisiä API tietoturva riskejä, jotka ovat samankaltaisia tämän ensimmäisen luokan kanssa, jossa riskit liittyvät lähinnä organisatorisiin tekijöihin ja käyttöönottoon. Yksi tällainen riski oli Tang ym., (2015) mainitsema organisaatioiden haaste API-rajapintojen julkaisemisessa julkiseen käyttöön. Tämä voi osoittautua juuri OB API-rajapintojen julkaisussa myös riskiksi, sillä pankeilla ei ole juuri kokemusta julkisten rajapintojen julkaisemisesta, varsinkaan näin laajassa mittakaavassa, missä OB API-rajapintoja julkaistaan.

Leaden ym., (2017) mainitsi myös, kuinka API-rajapintojen kontrollointi on hyvin haastavaa. Pankeilla ei ole tästäkään kokemusta tässä mittakaavassa, millaista kontrollointia julkisten API-rajapintojen kanssa tulee toteuttaa. Näihin riskeihin liittyy myös hyvin paljon aiemmassa luvussa mainittu julkisen ja yksityisen API-rajapinnan sekoittuminen suunnitteluvaiheessa. Pankit ovat tottuneet toteuttamaan pääsääntöisesti yksityisiä rajapintoja, joten nyt kun heiltä vaaditaan laajamittaisten julkisten rajapintojen julkaisua, on riski olemassa, että tärkeimmät turvallisuuteen liittyvät julkisen API-rajapinnan ominaisuudet ei oteta mahdollisesti huomioon tai unohdetaan.

Dapp, (2015) kertoo artikkelissaan tämän kaltaiseen tilanteeseen liittyen ratkaisuksi Walled garden -strategian. Walled garden -strategia tarkoittaa IT ympäristön rajaamista yhteistyökumppaneiden ja asiakkaiden kanssa paremman kontrollin saavuttamiseksi ohjelmistoihin, mobiililaitteisiin ja niiden sisältöön (Dapp, 2015). Dapp selittää artikkelissaan, kuinka FinTech yritykset ovat

käyttäneet tätä strategiaa paremman IT tietoturvan takaamiseksi. Tätä strategiaa voisi siis toteuttaa myös OB-mallin kanssa paremman tietoturvan ja sen paremman kontrollin takaamiseksi. Pankit voisivat siis luoda omaa rajattua ekosysteemiä valittujen Fintech-yritysten kanssa OB mallia ja sen API- rajapintoja kehittäessä.

Valitettavasti OB mukaisessa toiminnassa vastuuta turvallisuudesta jää myös itse pankin asiakkaalle. Haupert & Gabert, (2019) mainitsevat artikkelissaan, että tietoturva hyökkäyksen mitigoinniksi on välttämätöntä, että käyttäjä on tietoinen jonkin tiedonsiirto väylän epäluotettavuudesta. Tämä ei kuitenkaan ole ideaali asetelma, kun tarkoituksena on luoda uutta turvallisempaa maksupalvelutoimintamallia.

3.2 Open banking API tekniset riskit

Almehrej ym., (2020) mukaan tällä hetkellä OB standardisointi luottaa nykyisiin web teknologioihin, jotka voivat olla jo lähitulevaisuudessa vanhentuneita tulevaisuuden teknologia- ja turvallisuustarpeisiin. Tähän riskiin onkin löytynyt tämänhetkisestä kirjallisuudesta viitteitä teknisellä tasolla.

Kirjallisuudesta on löytynyt erityisesti mainintoja liittyen OB API Transport Layer Securityn (TLS) haavoittuvuudesta. TLS koostuu monista kryptografisista protokollista, jotka on suunniteltu tarjoamaan turvallinen kommunikaatio verkon yli (Soldatos ym., 2020). TLS on mahdollisesti eniten käytetty turvallisuus protokolla ja sitä on laajasti käytetty turvaamaan muun muassa verkkoliikennettä, sähköpostiliikennettä ja VPN yhteyksiä sen 18 vuoden olemassaolon ajan (nykyään 27 vuotta) (Bhargavan ym., 2013). Soldatos ym., (2020) mukaan TLS protokollan suosio on kannustanut hyökkääjiä etsimään siitä haavoittuvuuksia ja kehittämään hyökkäys keinoja.

TLS protokollaa käytetään yhtenä OB tietoturvan perustana ja sitä on suositeltu myös PSD2 säännöksessä (Soldatos ym., 2020). Tämä pitkien perinteiden omaava TLS-protokollan käyttö voi luoda riskin OB API-rajapinnalle, sillä niin kuin aiemmin tässä kappaleessa mainittiin, OB standardisointi nojaa vahvasti nykyisiin web teknologioihin, jotka voivat hyvinkin pian osoittautua liian vanhoiksi. TLS protokollalla on pitkä historia kehityksistä ja korjauksista, mutta myös hyökkäyksistä (Bhargavan ym., 2013).

Kellezi ym., (2019) tutkivat artikkelissaan Nordean OB API-rajapintaa sen hiekkalaatikko versiossa. Hekin nostavat esille tutkimuksessaan erityisesti TLS protokollaan liittyvän löydöksen. Heidän mukaansa applikaatio on suuressa riskissä API:n TLS protokollan vaarantavan käsittelyn vuoksi, joka johtaa jatkuviin järjestelmän kaatumisiin HTTPS protokollaa käytettäessä. Heidän mukaansa tämä johtaa riskien kasvuun järjestelmien arkkitehtuurissa ylöspäin mentäessä, joka johtaa korkeaan käyttäjän tilitietojen ja varojen riskeeraamiseen, sillä järjestelmän kaatumiset aiheuttavat pakettien lähettämisen salaamattomana.

Kellezi ym., (2019) mainitsevat kuitenkin, että täysin varmaksi tätä haavoittuvuutta järjestelmässä ei voida todeta, sillä heillä ei ole tarpeeksi tietoa Nordean OB API-rajapinnan dokumentaatiosta. TLS protokollan käyttö on kuitenkin nostettu monesti esille kirjallisuudessa OB API riskien yhteydessä ja kirjallisuudessa alleviivataankin TLS protokollan huolellista konfigurointia turvallisuuden takaamiseksi (Bhargavan ym., 2013, Soldatos ym., 2020).

Näiden yllä mainittujen riskien lisäksi, jotka on suoraan mainittu kirjallisuudessa OB API kontekstissa, on olemassa mahdollisuus myös muiden yleisten API-tietoturva riskien toteutumisesta, joita aiemmassa luvussa kohdassa 2.1.3 käsiteltiin. Nämä OWASP API Security Top 10 riskit on luotu lisäämään tietoisuutta modernien API-rajapintojen ongelmista (*OWASP API Security Project | OWASP Foundation*, ei pvm.). Tämän perusteella ne myös pätevät siis OB API-rajapintoihin. Jo aiemmassa alaluvussa mainittiin kuinka esimerkiksi "API7:2019 - Security Misconfiguration "- (OWASP, 2019) toteutuminen voi olla hyvinkin todennäköistä johtuen API kehitystyön haasteista. Kirjallisuudesta ei löydy erityisesti mainintoja OB kontekstissa näiden API tietoturvariskien toteutumisesta, mutta niin kuin kaikkien API-rajapintojen kehittämisessä ja ylläpidossa, on ne myös tässäkin kontekstissa relevantteja.

4 YHTEENVETO

Tässä kirjallisuuskatsauksena toteutetussa tutkielmassa tutkittiin Open banking (OB) API-rajapintoihin liittyviä tietoturvariskejä. Tutkielman kannalta olennainen käsitteistö liittyen OB:iin kuvattiin tutkielman kannalta tarvittavissa osin, joka sisälsi määritelmät toisen maksupalveludirektiivin (PSD2) -käsitteelle, API-rajapinnalle (Application programming interface) ja niiden ylisimmille ja tämän tutkimuksen kannalta olennaisimmille tietoturvariskeille. Näiden käsitteiden kautta tutkielmassa selitettiin sen taustat ja aihepiirin kannalta olennaisimmat ilmiöt. Tämän jälkeen tutkielmassa tunnistettiin olemassa olevan kirjallisuuden sekä tutkielmassa aiemmin läpikäytyjen käsitteiden ja ilmiöiden avulla OB API-rajapintoihin liittyviä mahdollisia tietoturvariskejä. Osa riskeistä tutkielmassa tunnistettu kirjallisuudesta suoraan ja osa niistä tunnistettiin yleisiä API-tietoturvariskejä soveltaen OB-kontekstiin kirjallisuuden avulla argumentoiden.

4.1 Aihepiiri ja tavoitteet

Teknologinen muutos on kiihtymässä rahoitusalalla (Boot ym., 2021). Tämä näkyy muun muassa tässä tutkielmassa käsitellyn uuden PSD2 EU:n sääntelyn muodossa. Direktiivi on osa globaalia trendiä pankkisääntelyssä, joka painottaa turvallisuutta, innovointia, ja vapaata markkinakilpailua (Botta ym., 2018). Helpompi tiedonsaanti on myös ollut nouseva trendi joka alalla, mukaan lukien rahoitusala, joten PSD2 tarkoitus on myös lisätä läpinäkyvyyttä tiedonsaatavuuden saralla (Brodsky & Oakes, 2017).

Vastatakseen EU:n sääntelyyn Yhdistynyt kuningaskunta julkaisi oman saman kaltaisen sääntelyn. Tarjotakseen standardin API-rajapinnan asiakkaiden tietojen jakoon useampien pankkien välillä Yhdistynyt kuningaskunta julkaisi Open Banking -standardin (Almehrej ym., 2020). OB-käsitettä on käytetty kirjallisuudessa yleisesti kuvaamaan PSD2 mukaista toimintamallia ja käsite on käytännössä seurausta EU:n ja Yhdistyneiden kuningaskuntien sääntelystä (Boot

ym., 2021, Botta ym., 2018, Kellezi ym., 2019, Laplante & Kshetri, 2021). PSD2 tavoin OB tarjoaa kolmansien osapuolien finanssipalveluiden tarjoajille vapaan pääsyn kuluttajapankki-, pankkitapahtuma- ja muihin pankkitietoihin pankeista ja pankkien ulkopuolisista rahoituslaitoksista käyttäen sovellusten API-rajapintoja (Laplante & Kshetri, 2021).

Zachariadiksen ja Ozcanin (2017) mukaan PSD2 sääntelyssä suositellaan API-teknologian käyttöä, sillä se on myös kaikista yleisimmin käytetty rajapintateknologia. Yksinkertaistettuna sovelluksen ohjelmoitavan rajapinnan eli API:n voi kuvata ratkaisuksi, jolla kaksi sovellusta voivat keskustella toisilleen verkon välityksellä käyttäen yleistä kieltä, jotka molemmat sovellukset ymmärtävät. API on tietynlainen paketti sääntöjä, joita noudattamalla ohjelmistot voivat kommunikoida keskenään. API-rajapinnat voidaan jakaa kahteen eri tyyppiin yksityisiin ja julkisiin, jossa julkinen API on sellainen, johon kuka tahansa voi päästä käsiksi ja yksityinen taas sellainen, joka on vain käytössä esimerkiksi jonkin organisaation sisällä. (Jacobson ym. 2011)

API-tietoturva on paljon tutkittu aihe, josta on tehty paljon omia tutkimuksia ja opinnäytteitä. Tässä tutkielmassa kerrottiin yleisimmistä API tietoturva riskeistä, jotka pohjautuvat pääsääntöisesti The Open Web Application Security Project (OWASP) yhteisön Top 10 listaan. Tämän artikkelin tarkoituksena on valistaa API-kehittäjiä ja -käyttäjiä yleisimmistä API tietoturvariskeistä (OWASP, 2019). Tässä artikkelissa kerrottiin tärkeimmät asiat, jotka tulee ottaa huomioon API-rajapintojen teknisessä toteutuksessa kymmenellä eri tasolla.

Näiden riskien lisäksi tunnistettiin kirjallisuuteen perustuen muita riskejä, jotka eivät olleet niin teknisellä tasolla, vaan ennemmin organisatorisella ja käyttöönottoon liittyvällä tasolla. Erityisesti julkisten rajapintojen käyttö osoittautui haasteeksi. Tang ym., (2015) mukaan API-rajapintojen julkaisu organisaation ulkopuolelle on koitumassa IT-osastoille haasteeksi. Leaden ym., (2017) mukaan API-rajapintojen kontrollointi on myös erittäin haastavaa erilaisten päällekkäisten protokollien vuoksi. Bhuiyan ym., (2018) tutkimuksessa myös huomattiin, että heidän tarkasteluunsa satunnaisesti valitsemista julkisista API-rajapinnoista noin 88% osoittautui haavoittuviksi.

Avoimien API-rajapintojen käyttäminen asiakkaiden arvokkaiden tilitietojen siirtämiseen herättää luonnollisesti kysymyksiä liittyen sen tietoturvaan. Kellezi ym., (2019) mukaan pankkitietojen paljastaminen kolmansien osapuolien palveluntarjoajille avoimen API-rajapinnan avulla tuovat esiin useita kyberturvallisuuteen liittyviä ongelmia. Tämän tiedon ja aiemmin mainittujen yleisten API-tietoturvaongelmien perusteella aihe vaatii enemmän tutkimusta, sillä OB toimintamallia tullaan käyttämään tulevaisuudessa entistä enemmän ja riskinä on asiakkaiden tilitietojen vaarantaminen.

4.2 Tulokset ja johtopäätökset

Tässä tutkielmassa tunnistettiin kirjallisuuden perusteella muutamia riskejä API-rajapintoihin liittyen suoraan Open banking (OB) kontekstissa, mutta osa riskeistä piti johtaa yleisistä API tietoturvariskeistä argumentoiden. Riskit oli jaettu kahteen luokkaan; Organisatoriset ja käyttöönottoon liittyvä riskit sekä OB teknisiin riskeihin.

Ensimmäisen luokan riskeiksi tunnistettiin FinTech (financial technology) -yritysten ja suurien pankkien välinen yhteistyö. FinTech tarkoittaa yritystä, joka tarjoaa moderneja teknologiaratkaisuja rahoitusalalla (Saksonova & Kuzmina-Merlino, 2017). Nämä yritykset kehittävät yhdessä pankkien kanssa OB API-rajapintoja ja luovat samalla näitä uusia tuotteita ja palveluja markkinoille. Zachariadiksen ja Ozcanin (2017) mukaan FinTech yritykset ovat huolissaan siitä, kuinka nopeasti pankit hyväksyvät uusia tuotteita markkinoille, ja kertovat yhdeksi mahdolliseksi syyksi pankkien kokemattomuuden näiden julkaisuprosessien läpikäymisestä, sillä ennen tätä pankit ovat vastanneet itse tietoturvasta.

Myös Tang ym., (2015) mainitsema julkisten rajapintojen julkaisemisen haasteet ovat tässä riskinä, sillä pankit joutuvat julkaisemaan nyt rajapintoja julkiseen käyttöön tutuksi käyneen sisäisen käytön sijaan, jossa on monia pankille uusia asioita otettava huomioon. Myös Leaden ym., (2017) mainitsema rajapintojen kontrolloinnin haasteet voivat koitua riskiksi, sillä pankit ovat kokemattomia myös julkisten rajapintojen kontrolloinnin suhteen. Nämä kaksi riskiä nojaa vahvasti siihen, että pankeilla ei ole paljon kokemusta tämän aihealueen saralta.

Dapp, (2015) kertoi artikkelissaan kontrolloinnin haasteiden ratkaisuksi Walled garden -strategian. Walled garden -strategia tarkoittaa IT ympäristön rajaamista yhteistyökumppaneiden ja asiakkaiden kanssa paremman kontrollin saavuttamiseksi ohjelmistoihin, mobiililaitteisiin ja niiden sisältöön (Dapp, 2015).

Toisen luokan riskeiksi, jotka liittyivät OB API teknisen tason riskeihin tunnistettiin tässä tutkielmassa erityisesti vanhan protokollan käyttö. TLS (Transport Layer Security) on mahdollisesti eniten käytetty turvallisuus protokolla ja sillä on jo yli 20 vuoden historia päivityksistä, korjauksista ja myös hyökkäyksistä. Tämän protokollan suosio on kannustanut hyökkääjiä etsimään siitä haavoittuvuuksia. (Bhargavan ym., 2013, Soldatos ym., 2020) TLS-protokollaa käytetään yhtenä OB tietoturvan perustana ja sitä on suositeltu myös PSD2 säännöksessä (Soldatos ym., 2020). Kellezi ym., (2019) tutkivat artikkelissaan Nordean OB API-rajapintaa sen hiekkalaatikkoversiossa ja löysivät myös siitä juuri TLS-protokollaan liittyvän haavoittuvuuden. Tämä luo merkittävän riskin OB API teknisellä tasolla.

Lopuksi tutkielmassa mainitaan OB API riskeiksi The Open Web Application Security Project (OWASP) yhteisön Top 10 listan yleisimmät API tietoturvariskit. Tässä listassa mainitut riskit pätevä kaikkien API-rajapintojen

kehittämiseen ja ylläpitoon, joten ne pätevät myös tässä tapauksessa. Mitään suoria löydöksiä kirjallisuudesta ei löytynyt, minkä avulla näitä voisi liittää juuri OB kontekstiin, mutta "API7:2019 - Security Misconfiguration "- (OWASP, 2019) toteutumiseen löytyi eniten tukea johtuen pankkien ja FinTech yritysten välisistä toiminnan eroista. Tämä tuki on pääteltävissä siitä, että tämä listan kohta käsittelee rajapinnan huolellisen turvallisuuden konfiguroinnin tärkeyttä suunnitteluvaiheessa.

Tutkielman perusteella voi tehdä johtopäätöksen, että OB API tietoturvaan liittyy monia riskejä niin teknisellä kuin myös organisatorisella tasolla. Näitä riskejä ei tule aliarvioida, sillä vaarannettuna ovat pankkipalveluita käyttävien asiakkaiden tilitiedot. Kaikkia riskejä ei ole välttämättä edes tunnistettu OB kontekstissa, sillä tutkimusta tästä aiheesta on vielä hyvin vähän. Erityisiä ratkaisuja näiden riskien vähentämiseen tässä tutkielmassa ei käyty kattavasti läpi, mutta yleisempien API kehityksen käytänteiden, kuten OWASP API Security Top 10 – 2019, noudattaminen auttaa. Lisäksi Dappin, (2015) mainitsema Walled garden -strategia nähtiin tässä tutkielmassa mahdollisena ratkaisuna API-tietoturvariskien hallitsemiseksi.

Jatkotutkimusaiheena tähän tutkielmaan liittyen tulisi tutustua tarkemmin olemassa oleviin OB API -ratkaisuihin ja niiden tietoturvaan. Aiheesta ei juuri löydy tutkimuksia ja tässäkin tutkielmassa käytetty Kellezi ym., (2019) tekemä tutkimus Nordean OB API-rajapinnasta oli vajaa API-rajapinnan dokumentaation osalta. OB API-rajapintojen tietoturva vaatii lisätukimusta ennen kuin rajapintoja on julkaistu mittavissa määrin pankkien asiakkaiden käytettäväksi. Näin voidaan varmistaa, ettei asiakkaille koidu mittavia vahinkoja kypsymättömän avoimen rajapinnan tietoturvan vuoksi.

LÄHTEET

Almehrej, A., Freitas, L., & Modesti, P. (2020). Security Analysis of the Open Banking Account and Transaction API Protocol. *arXiv preprint arXiv:2003.12776.*

Bhargavan, K., Fournet, C., Kohlweiss, M., Pironti, A., & Strub, P.-Y. (2013). Implementing TLS with Verified Cryptographic Security. 2013 *IEEE Symposium on Security and Privacy, 445–459. https://doi.org/10.1109/SP.2013.37*

Bhuiyan, T., Begum, A., Rahman, s, & Hadid, I. (2018). API vulnerabilities: Current status and dependencies. *International Journal of Engineering and Technology(UAE), 7, 9–13. https://doi.org/10.14419/ijet.v7i2.3.9957*

Boot, A., Hoffmann, P., Laeven, L., & Ratnovski, L. (2021). Fintech: What's old, what's new? *Journal of Financial Stability, 53, 100836. https://doi.org/10.1016/j.jfs.2020.100836*

Botta, A., Digiacomo, N., Höll, R., & Oakes, L. (2018). PSD2: Taking advantage of open-banking disruption. *McKinsey and Company.*

Brodsky, L., & Oakes, L. (2017). Data sharing and open banking. *McKinsey & Company, 1097, 1105.*

Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs. (2016, helmikuuta 24). Troy Hunt. https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

Dapp, T.-F., (2015). *Fintech reloaded – Traditional banks as digital ecosystems: With proven walled garden strategies into the future. 27.*

Haupert, V., & Gabert, S. (2019). Short Paper: How to Attack PSD2 Internet Banking. Teoksessa I. Goldberg & T. Moore (Toim.), *Financial Cryptography and Data Security* (ss. 234–242). Springer International Publishing. https://doi.org/10.1007/978-3-030-32101-7_15

How Open Banking is Revolutionizing the Banking Industry. (2019, marraskuuta 20). *A Professional Blog on Enterprise Softwares and Services.* https://www.enterpriseedges.com/open-banking-system

How to Use Open Banking API for Your Fintech App? (ei pvm.). Noudettu 19. marraskuuta 2022, osoitteesta https://www.uptech.team/blog/open-banking-api-for-your-fintech-app

Jacobson, D., Brail, G., Woods, D. (2011). Apis: A Strategy Guide. O'Reilly Media, Inc.

Kellezi, D., Boegelund, C., & Meng, W. (2019, December). Towards secure open banking architecture: an evaluation with OWASP. *International Conference on Network and System Security* (pp. 185-198). Springer, Cham.

Laplante, P., & Kshetri, N. (2021). Open banking: Definition and description. *Computer, 54*(10), 122-128.

Leaden, G., Zimmermann, M., DeCusatis, C., & Labouseur, A. G. (2017). An API honeypot for DDoS and XSS analysis. *2017 IEEE MIT Undergraduate Research Technology Conference (URTC),* 1–4. https://doi.org/10.1109/URTC.2017.8284180

Maksupalveludirektiivi PSD2. (2021, helmikuuta 9). Finanssiala. https://www.finanssiala.fi/aiheet/maksupalveludirektiivi-psd2/

Mosqueira-Rey, E., Alonso-Ríos, D., Moret-Bonillo, V., Fernández-Varela, I., & Álvarez-Estévez, D. (2018). A systematic approach to API usability: Taxonomy-derived criteria and a case study. *Information and Software Technology, 97*, 46–63. https://doi.org/10.1016/j.infsof.2017.12.010

Navaretti, G. B., Calzolari, G., Mansilla-Fernandez, J. M., & Pozzolo, A. F. (2018). *Fintech and Banking. Friends or Foes?* (SSRN Scholarly Paper Nro 3099337). https://doi.org/10.2139/ssrn.3099337

OWASP API Security Project | OWASP Foundation. (2019). Noudettu 14. marraskuuta 2022, osoitteesta https://owasp.org/www-project-api-security/

Premchand, A., & Choudhry, A. (2018, February). Open banking & APIs for transformation in banking. *2018 international conference on communication, computing and internet of things (IC3IoT)* (pp. 25-29). IEEE.

Romanova, I., Grima, S., Spiteri, J., & Kudinska, M. (2018). The Payment Services Directive II and Competitiveness: The Perspective of European Fintech Companies. *EUROPEAN RESEARCH STUDIES JOURNAL, XXI(Issue 2)*, 3–22. https://doi.org/10.35808/ersj/981

Saksonova, S., & Kuzmina-Merlino, I. (2017). Fintech as Financial Innovation—The Possibilities and Problems of Implementation. *EUROPEAN RESEARCH STUDIES JOURNAL, XX(Issue 3A)*, 961–973. https://doi.org/10.35808/ersj/757

Soldatos, J., Philpot, J., & Giunta, G. (Toim.). (2020). *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures.* Now Publishers. https://doi.org/10.1561/9781680836875

Tang, L., Ouyang, L., & Tsai, W.-T. (2015). Multi-factor web API security for securing Mobile Cloud. *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 2163–2168. https://doi.org/10.1109/FSKD.2015.7382287

Zachariadis, M., & Ozcan, P. (2017). The API economy and digital transformation in financial services: The case of open banking.