Joonas Ojala

On aika unohtaa salasanat – salasanojen tietoturvahaasteita ja ratkaisuehdotuksia

Tietotekniikan kandidaatintutkielma

10. toukokuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Joonas Ojala

Yhteystiedot: joonas.a.ojala@student.jyu.fi

Työn nimi: On aika unohtaa salasanat – salasanojen tietoturvahaasteita ja ratkaisuehdotuksia

Title in English: It's time to forget passwords – passwords' security challenges and proposed solutions

Työ: Kandidaatintutkielma

Sivumäärä: 30+0

Tiivistelmä: Salasanat ovat suosituin tunnistautumistapa, vaikka vaihtoehtoisia tunnistautumisjärjestelmiä on nykyään saatavilla. Tässä kirjallisuuskatsauksessa tarkastellaan yksivaiheisten salasanaa hyödyntävien tunnistautumisjärjestelmien tietoturvahaasteita sekä esitetään nykyaikaisia ratkaisuehdotuksia niille. Salasanapohjaiset tunnistautumisjärjestelmät vaativat yhteistyötä niin käyttäjien kuin tunnistautumisjärjestelmien puolesta, ja se yhteistyö on tasapainottelua tietoturvan ja käytännöllisyyden välillä. Salasananhallintajärjestelmät, keskitetyt tunnistautumisjärjestelmät ja monivaihetunnistautumiset minimoivat esitettyjä tietoturvahaasteita ja tarjoavat nykyaikaisen tavan hyödyntää salasanoja IoT-aikakaudella.

Avainsanat: IoT, salasana, tietoturva, tunnistautuminen, yksivaiheiset tunnistautumisjärjestelmät

Abstract: Passwords are the most popular type of authentication, even though alternative authentication systems have become available. This literature review examines today's security challenges of single-factor password-based authentication systems and presents some of the proposed solutions for them. The security of the authentication requires a cooperation between the end-users and the systems, and that cooperation is balancing between security and practicality. Passwordmanagers, single-password authentication systems and multi-factor authentications provide a modern way of managing passwords in today's IoT-age.

Keywords: authentication, IoT, password, security, single-factor authentication systems

Sisällys

1 JOHDANTO 1

2 SÄHKÖISET TUNNISTAUTUMISJÄRJESTELMÄT 3
2.1 Tietoon pohjautuvat järjestelmät 3
2.2 Omistukseen pohjautuvat järjestelmät 4
2.3 Biometriikkaan pohjautuvat järjestelmät 5

3 YKSIVAIHEISTEN SALASANAPOHJAISTEN TUNNISTAUTUMISJÄRJESTELMIEN TIETOTURVAHAASTEET 7
3.1 Järjestelmät ja tietoturvavaatimukset 8
3.2 Ihmiset ja tietoturvavaatimukset 9
3.3 Järjestelmien ja ihmisten yhteistyö 10

4 RATKAISUEHDOTUKSIA SALASANOJEN TIETOTURVAN PARANTAMISEKSI 13
4.1 Salasananhallintajärjestelmät 14
4.2 Keskitetyt tunnistautumisjärjestelmät 15
4.3 Yksivaiheisesta tunnistautumisesta monivaiheiseksi 16

5 YHTEENVETO 19

LÄHTEET 20

1 Johdanto

Tekstipohjaisia tunnistautumisjärjestelmiä, kuten salasanoja, on käytetty niin kauan kuin elektronisia tietojärjestelmiäkin. Nykyään on olemassa konsensus sen suhteen, että salasanoja hyödyntävät tunnistautumisjärjestelmät ja ihmiset ovat ongelmallinen yhdistelmä (Ometov ym. 2018; Rui ja Yan 2018). Voisi jopa väittää, että ihmisten tulisi välttää salasanojen käyttöä aina kuin se vain olisi mahdollista.

Tekstipohjaisten tunnistautumisjärjestelmien pitkän historian ansiosta niiden laajat hyökkäyspinta-alat ovat hyvin tiedossa. Aikaisempien salasanajärjestelmien ylläpito-ohjeiden päivittämisen sijaan salasanojen merkitystä tunnistautumisjärjestelmissä on pyritty minimoimaan hyödyntämällä vaihtoehtoisia tunnistautumismenetelmiä – joskus jopa kokonaan poistamalla tietoon pohjautuvat tunnistautumisvaiheet. Tietoon pohjautuvia tunnistautumismenetelmiä ei pidetäkään enää ainoana mahdollisuutena henkilöllisyyden todistamiseksi erilaisissa tietojärjestelmissä, vaan ne ovat vain yksi vaihtoehto eri tunnistautumisjärjestelmien kirjossa.

Henkilökohtaisten elektroniikkalaitteiden (engl. *internet of things*), eli IoT-laitteiden ansiosta aikaisemmin kalliiksi koetut biometriikkaan ja omistusmetriikkaan pohjautuvat tunnistautumisjärjestelmät ovat kasvattaneet suosiotaan räjähdysmäisesti (Chuat, Plocher ja Perrig 2020). Helpoiten sen huomaa älypuhelimista, joissa biometriikat ovat jopa korvanneet aikaisemmat tietoon pohjautuvat lukitukset (Ometov ym. 2018). Monien organisaatioiden tunnistautumisjärjestelmissä ei riitä enää pelkkä salasanan syöttö henkilöllisyyden todistamiseksi, vaan tunnistautumisvaiheiden määrää on voitu kasvattaa kahdeksi tai useammaksi.

Salasanoja hyödyntäviä yksivaiheisia tunnistautumisjärjestelmiä käytetään kuitenkin yhä laajasti kaikkialla, vaikka useita vaihtoehtoja niiden korvaamiseksi on olemassa. Tekstipohjaisten yksivaiheisten tunnistautumisjärjestelmien tietoturvaa tutkitaankin yhä aktiivisesti, sillä niitä käyttäviin tietojärjestelmiin kohdistuu jatkuvasti kyberhyökkäyksiä. Yksikin vuodettu salasanatietokanta voi vaarantaa useita samankaltaisia tunnistautumisjärjestelmiä, sillä samoja salasanoja käytetään useissa järjestelmissä.

Tässä tutkielmassa tarkastellaan, millaisia tietoturvauhkia salasanaa käyttävät tunnistautu-

misjärjestelmät kohtaavat nykyaikana. Lisäksi kartoitetaan, millaisia erilaisia ratkaisuehdotuksia näiden tietoturvauhkien minimoimiseksi on kehitetty.

Tutkielma etenee seuraavanlaisesti. Tutkielman toisessa luvussa käydään läpi yleisimpien saatavilla olevien tunnistautumisjärjestelmien pääpiirteet ja eroavaisuudet. Kolmannessa luvussa pohditaan salasanoja hyödyntävien tunnistautumisjärjestelmien tietoturvahaasteita niin organisaatio- kuin käyttäjänäkökulmasta. Neljännessä luvussa esitetään, millaisia ratkaisuehdotuksia listattujen tietoturvahaasteiden parantamiseksi on esitetty.

2 Sähköiset tunnistautumisjärjestelmät

Tavanomaisten tunnistautumisjärjestelmien tehtävänä on varmistaa tietojärjestelmän käyttäjän henkilöllisyys kirjautuessa tietojärjestelmään (Alt ja Schneegass 2022; Kyberturvallisuuskeskus 2022; Sasse, Brostoff ja Weirich 2001). Käyttäjän henkilöllisyyden varmistus tapahtuu siten, että järjestelmä pyytää käyttäjältä jotain ennalta määriteltyä asiaa, jonka ainoastaan kyseinen käyttäjä voi antaa. Jos käyttäjän antama asia vastaa tunnistautumisjärjestelmään tallennettua tietoa, on käyttäjän henkilöllisyys varmistettu ja tunnistautumisjärjestelmän tehtävä päättynyt.

Tavanomaisten tunnistautumisjärjestelmien eri tunnistautumismenetelmät jaetaan usein kolmeen pääkategoriaan; tieto-, omistus-, ja biometriikkaan pohjautuviin tekniikoihin (Wang ym. 2020; Barkadehi ym. 2018; Ometov ym. 2018). Myös Suomessa vahvojen tunnistautumisjärjestelmien eri menetelmien jako perustuu edellä mainittuun jakoon (Kyberturvallisuuskeskus 2022).

2.1 Tietoon pohjautuvat järjestelmät

Yksinkertaisuudessaan tietoon pohjautuvassa tunnistautumisjärjestelmässä kirjaudutaan salaisuudella, jonka käyttäjä on tallentanut järjestelmään. Järjestelmä vertaa käyttäjän antamaa tietoa, eli salaisuutta, järjestelmässä tallennettuna olevaan tietoon, ja jos tiedot vastaavat toisiaan, on kirjautuminen onnistunut. (Liao, Lee ja Hwang 2006, s. 728.)

Merkkijonoja käyttävät salasanat ovat selvästi käytetyin tapa tunnistautua tietojärjestelmien tunnistautumisjärjestelmissä, ja niitä on hyödynnetty niin kauan kuin tietojärjestelmiä on ollut olemassa (Zimmermann ja Gerber 2020; Zezschwitz, Luca ja Hussmann 2013; Herley ja Van Oorschot 2011). Vaihtoehtoisia tietoon pohjautuvia tunnistautumisjärjestelmiä ovat esimerkiksi erilaiset PIN-koodit sekä joistain IoT-laitteista löytyvät graafiset kuviolukitukset.

Toisin kuin kahdessa muussa päämenetelmässä, Altin ja Schneegassin (2022, s. 84, 85) mukaan tietoon pohjautuvissa tunnistautumisjärjestelmissä tunnistautumisessa voidaan käyttää tietoa, josta ei voida päätellä käyttäjästä mitään. Vastaavasti käyttäjien tiedot eivät ole keske-

nään tasavertaisia keskenään – toisen tallentama tieto voi sisältää yksityisempää tietoa kuin toisen (Taylor ja Garry 2019). Lisäksi toisen tallentama tieto voi olla vaikeampaa murtaa kuin toisen, sillä salasanan entropialla on vaikutusta sen murrettavuuteen suojatusta tietokannasta (Schafer ja Pan 2019; Heen ja Neumann 2017).

Salasanoja käyttävän tunnistautumisjärjestelmän tietovuodon tapahtuessa hyökkääjien on helppo hyödyntää saamaansa tietoa, sillä tunnistukseen tarvittava tieto on saatavilla. Salasanapohjaisia tunnistautumisjärjestelmiä kohtaan hyökätäänkin jatkuvasti, mikä aiheuttaa mittavia vahinkoja järjestelmän käyttäjille. (Mohamedali ja Fadlalla 2017.) Tietovuodon arkuus riippuu käyttäjän käyttämästä salaisesta tiedosta sekä siitä, mihin muualle samaa tai samantapaista salasanaa on käytetty. Tiedon varastamisen helppous riippuu monesta tekijästä ja usein vaihtelee käyttäjien kesken. Salasanan vaihto on yksinkertaista verrattuna muihin menetelmiin – riittää, että järjestelmään tallennettu tieto vaihdetaan uuteen tietoon.

2.2 Omistukseen pohjautuvat järjestelmät

Omistukseen pohjautuvassa tunnistautumisjärjestelmässä käyttäjä tunnistautuu hallussaan olevalla objektilla[1] (Kyberturvallisuuskeskus 2022). Objekti voisi olla esimerkiksi käyttäjän oma IoT-laite, kuten puhelin, tai tunnistautumisjärjestelmän erillinen avain, kuten avainlukulista. Käyttäjän jo hallussa olevaa objektia voidaan hyödyntää, jolloin erillisiä objektin esinekustannuksia ei synny. Objekti voi olla myös sähköisessä muodossa, kuten sähköpostitili. Tällöin fyysistä objektia ei tarvita, mutta pääsy sähköiseen objektiin vaaditaan. Objektin kadotessa se on korvattava uudella vastaavalla objektilla, mikä voi lisätä kustannuksia joko käyttäjälle tai organisaatioille riippuen käytettävästä objektista. (Stajano 2011.)

Omistukseen pohjautuvia tunnistautumisjärjestelmiä pidetään yleisesti ylläpitokustannuksiltaan korkeampina kuin tietoon pohjautuvia järjestelmiä. Oletus ei välttämättä pidä enää paikkansa, sillä IoT-laitteiden lukumäärä on kasvussa, ja Wangin ym. (2020) mukaan niiden ansiosta omistuspohjaiset tunnistautumisjärjestelmät ovat helppo toteuttaa. Wang ym. luokittelevat omistuspohjaiset tunnistautumismenetelmät kuitenkin heikoimmaksi tietoturvaltaan kolmesta tunnistautumismenetelmästä (Wang ym. 2020). Omistuspohjaisia tunnistautumis-

1. Tunnistautumisessa käyttäjän käyttämä esine, joka voi olla joko fyysisessä tai sähköisessä muodossa.

menetelmiä on käytetty siitä huolimatta jo laajasti myös ennen IoT-aikakautta – salasanapohjaisissa tunnistautumisjärjestelmissä hävinneen salasanan palautus tehdään usein sähköpostitilin kautta (Innocenti ym. 2021; Li ym. 2020). Palautuksessa voidaan hyödyntää esimerkiksi kertakäyttöistä salasanaa (engl. *one-time password*), eli OTPta. Se toimii siten, että järjestelmä lähettää koodin käyttäjän hallussa olevaan objektiin, josta käyttäjän tulee syöttää se tietyn aikaikkunan sisällä tunnistautumisjärjestelmään (Awasthi 2015). Chuat, Plocher ja Perrig väittävät, että älypuhelinta mukana kantavien käyttäjien osuus on nykyään jo niin suuri, että SMS OTPt olisivat kustannustehokkaasti toteutettavissa (Chuat, Plocher ja Perrig 2020).

Tietovuotonäkökulmasta omistukseen pohjautuvien tunnistautumisjärjestelmien hyöty on siinä, että objektin tietovuoto ei riskeeraa käyttäjän tunnuksia toisin kuin kahdessa muussa menetelmässä, koska suoja perustuu objektin hallussapitoon. Riskinä toki on, että objekti varastetaan tai kloonataan. (Wang ym. 2020, s. 15; Barkadehi ym. 2018.)

2.3 Biometriikkaan pohjautuvat järjestelmät

Biometriikalla tarkoitetaan tunnistautumista, jossa käyttäjästä mitataan jotain fyysistä ominaisuutta, kuten sormenjälkeä tai iiristä. Biometriikaksi voidaan luokitella myös käyttäjän tekeminen, joka on Altin ja Schneegassin (2022) mukaan mitattavissa. Jokaisella ihmisellä on uniikki tapa esimerkiksi kävellä tai kirjoittaa. Altin ja Schneegassin mukaan tekemistä mittaavat järjestelmät eivät kuitenkaan ole vielä tarpeeksi kehittyneitä, jotta niitä voitaisiin vielä käyttää yleisissä tunnistautumisjärjestelmissä (Alt ja Schneegass 2022). Myös staattiset biometriikat ovat vasta alkumetreillään – Ruin ja Yanin (2018) mukaan staattista biometriikkaa mittaavista tunnistautumisjärjestelmistä ainoastaan sormenjälki olisi tarpeeksi kypsä yleiseen käyttöön tunnistautumisjärjestelmissä. Tilanne saattaa tosin muuttua hyvinkin lähitulevaisuudessa, sillä älypuhelimiin kehitetään jatkuvasti erilaisia tunnistautumisjärjestelmiä, jotka hyödyntävät älypuhelinten sensoreita, kuten mikrofonia, kameraa ja sormenjälkitunnistinta (Chuat, Plocher ja Perrig 2020). Biometriikka koetaankin käyttäjäystävälliseksi tunnistautumisjärjestelmäksi, koska se ei vaadi mitään muistettavaa tai kannettavaa asiaa (Morake, Khoza ja Bokaba 2021).

Toisin kuin yleisimmissä tietoon tai omistukseen perustuvissa tunnistautumisjärjestelmissä, biometriikkapohjaisissa tunnistautumisissa käyttäjän varmentaminen perustuu aina todennäköisyyteen; mittaustulokset harvoin vastaavat täysin tunnistautumisjärjestelmään tallennettua tietoa (Ometov ym. 2018). Biometriikkaa käyttävissä tunnistautumisjärjestelmissä onkin määriteltävä todennäköisyysraja, joka määrittelee sallitun enimmäiseron mittaustuloksen ja järjestelmässä olevan datan välillä. Mitä matalampi todennäköisyysraja on, sitä todennäköisempää on, että todellisen käyttäjän mittaustulos hyväksytään, mutta samalla riski väärän käyttäjän hyväksymiselle kasvaa. (Rui ja Yan 2018.)

Biometriikan hyödyntämisessä haasteena on se, että kaikilta ihmisiltä ei voida mitata tunnistautumiseen vaadittavaa biometriikkaa, kuten sormenjälkeä (Ometov ym. 2018, s. 9). Toinen biometriikkadatan haasteista on tietovuodossa vuodetun biometriikan korvaaminen. Toisin kuin tieto- tai omistuspohjaisissa menetelmissä, biometriikan muuttaminen on hankalaa, tai usein jopa mahdotonta (Ometov ym. 2018). Vuodettu biometriikka koetaan myös henkilökohtaiseksi – Rui ja Yan väittävätkin, että tietovuodot aiheuttavat sitä suuremmat tietoturvaongelmat vuodon uhreille, mitä pysyvämpää ja yksityiskohtaisempaa biometriikka on (Rui ja Yan 2018, s. 5995).

3 Yksivaiheisten salasanapohjaisten tunnistautumisjärjestelmien tietoturvahaasteet

Vaikka IoT-laitteet ovat helpottaneet erilaisten sähköisten tunnistautumisjärjestelmien kehitystä ja käyttöönottoa, yksivaiheiset salasanapohjaiset tunnistautumisjärjestelmät eivät ole katoamassa. Niillä on etumatka vaihtoehtoisiin toteutuksiin, ja Bonneau ym. (2012) esittävät, että etumatkan lisäksi kyseisten järjestelmien toteutus ja ylläpito on ylivertaisesti helpointa verrattuna muihin tunnistautumismenetelmiin. Lisäksi salasanapohjaisia tunnistautumisjärjestelmiä saatetaan ajatella siten, että niissä käyttäjien on mahdollista tallentaa anonyymiä tietoa, joka vuodettaessa ei paljastaisi mitään arkaluontoista tai yksityistä – asia, joka on Altin ja Schneegassin (2022, s. 83) mukaan haasteellista tehdä varsinkin biometrisissä tunnistautumismenetelmissä.

Vaikka toimiva salasanapohjainen tunnistautumisjärjestelmä olisikin helppo toteuttaa, ei samaa voi väittää niiden tietoturvasta tai ylläpidosta. Baumanin, Lun ja Linin (2015) mukaan uusia tietoturvattomia tunnistautumisjärjestelmiä luodaan jatkuvasti, koska tunnistautumisjärjestelmien tekoon ei tarvita IT-alan osaamista. Bauman, Lu ja Lin esittävät ongelmallisten tietojärjestelmien olemassaolon syiksi ymmärtämättömyyden, järjestelmän päivittämättömyyden ja osaamattomuuden (Bauman, Lu ja Lin 2015). Valitettavasti mikään ei estä haavoittuvaista tunnistautumisjärjestelmää palvelemasta, tai vuodettua salasanaa toimimasta.

Tunnistautumisjärjestelmien tietoturva on lähes aina pois käyttäjäkokemuksesta. Altin ja Schneegassin (2022) mukaan tunnistautuminen koetaan hidasteeksi todelliselle toiminnalle, ja sen takia siihen käytetty energia turhauttaa käyttäjiä. Samalla tavalla mitä vaativampi rekisteröintiprosessi ja tunnistautumisprosessi on, sitä raskaammaksi sen teko koetaan (Imamaliyev ja Khudoykulov 2021). Turhautuminen puolestaan lisää käyttäjällä tietoturvattomampaa käsittelyä tunnistautumisprosessissa (Khan, Coopamootoo ja Ng 2020).

Seuraavaksi tutkielmassa tarkastellaan tarkemmin salasanoja käyttävien tunnistautumisjärjestelmien tietoturvahaasteita. Nämä tietoturvahaasteet ilmenevät järjestelmissä sekä käyttäjien toiminnassa, mutta myös järjestelmien ja käyttäjien välisessä yhteistyössä.

3.1 Järjestelmät ja tietoturvavaatimukset

Salasanatunnistautumisjärjestelmät ovat itsessään haavoittuvaisia salasana- ja kommunikaatiokanavahyökkäyksille (AlJanah, Zhang ja Tay 2021, s. 130919). Lisäksi, kuten muissakin tietokannoissa, salasanatietokannan suojauksella on vaikutusta tunnistautumisjärjestelmän kaikkien salasanojen suojauksen kannalta.

Kolme yleisintä [1] tapaa suojata salasanatietokantoja ovat selväkielisenä, salasanojen tiivisteillä ja suolattujen salasanojen tiivisteillä. Selväkielisessä tietokannassa salasanat tallennetaan alkuperäisillä salasanoilla. Silloin tietokannan vuodon sattuessa kaikki salasanat vuotavat. Salasanojen tiivisteillä tallennetussa tietokannassa salasanoista tallennetaan tiivistefunktion tuloste, eli salasanan tiiviste. Teoriassa tiivisteistä on lähes mahdotonta päätellä alkuperäisiä syötteitä. Vanhentuneilla tiivistefunktioilla suojatut tietokannat voidaan kuitenkin murtaa jopa täysin esimerkiksi myöhemmin havaittujen haavoittuvuuksien ansiosta. Lisäksi samaa salasanaa käyttävät tiivisteet voidaan poimia tietokannasta, ja täten arvata hyödyntämällä jo vuodettuja tietokantoja. Suolatussa tiivistetietokannassa lisätään ennen tiivistefunktiota jokaiseen salasanaan *suola*, joka tekee tietokannan tiivisteistä uniikkeja, vaikka ne olisivatkin alun perin olleet sama salasana. Hyökkääjän on tällöin murrettava ensin *suolaus*, jotta salasanatietokannasta olisi mitään hyötyä hyökkääjälle.

Blauwin (2017) sekä Heenin ja Neumannin (2017) mukaan salasanat tulisi suojata ajantasaisilla suolatuilla salasanojen tiivistefunktioilla, jos se vain on mahdollista. Bauman, Lu ja Lin (2015) puolestaan väittävät, että pelkästään salasanojen tiivisteiden tallentaminen ajantasaisella tiivistefunktiolla voi antaa jo riittävän suojan. Tietyt järjestelmät eivät voi myöskään käyttää suolausta salasanoissaan, jolloin suojaustapana tulee käyttää ajantasaista tiivistefunktiota (Bauman, Lu ja Lin 2015). Pelkällä tiivistefunktiolla tallentaessa tulisi varmistaa, ettei tiivisteistä voi arvata niiden alkuperäisiä salasanoja, ja että salasanat ovat uniikkeja.

1. Kolmen listatun tavan lisäksi saatetaan mainita vielä yksi tapa, jossa tietokannan salasanat tallennetaan selväkielisinä, mutta tietokanta itse salataan avaimella. Kyseisessä tekniikassa hyökkääjän tarvitsee murtaa ainoastaan yksi avain, jotta koko tietokanta muuttuisi selväkieliseksi. Luokittelenkin kyseisen tekniikan samaksi, kuin selväkielisenä tallentamisen. Esimerkiksi Adobe tallensi salasanat mainitulla tavalla ainakin vuoteen 2013 asti, jolloin tietomurtojen yhteydessä salatun tietokannan kaikki salasanat vuodettiin – joita oli yhteensä noin 150 miljoonaa (Adobe 2021; Hern 2013).

Yleisimmät virheet salasanatietokannoissa ovat tietoturvattomalla tiivistefunktiolla tallentaminen tai suoraan selväkielisenä tallentaminen. Esimerkiksi Bauman, Lu ja Lin (2015) löysivät tutkimuksessaan, että Euroopan 500 kävijämäärältään suosituimmista sivuista jopa 11 tallensi salasanat selväkielisinä. Suosituimpien sivustojen lisäksi he löysivät myös yli 100 konferenssisivustoa, joissa salasanat oli tallennettu selväkielisinä (Bauman, Lu ja Lin 2015).

Ajantasainen suojaus päivittyy jatkuvasti sitä mukaan, kun uusia vuotoja löytyy. Kyberturvallisuuskeskus esimerkiksi julisti *SHA-1* tiivistefunktion lopullisesti murretuksi, ja kehotti siirtymään vielä murtamattomiin *SHA-2* ja *SHA-3* tiivistefunktioihin (Kyberturvallisuuskeskus 2020). *SHA-1* tiivistefunktiota on käytetty 1990-luvulta lähtien salasanatietokantojen suojaamiseen.

Toiseksi, AlJanah'n, Zhangin ja Tayn (2021) mukaan salasanoja käyttävät tunnistautumisjärjestelmät ovat alttiita asiakkaan ja järjestelmän välisen kommunikointikanavan (engl. *client-server communication channel*) hyökkäyksille. Kommunikaatiokanavan hyökkäyksiä vastaan voidaan suojautua ainoastaan hyödyntämällä tietoturvallisesti ajantasaista kommunikaatiokanavatoteutusta (Bauman, Lu ja Lin 2015). Ma ym. tarkastelivat Googlen Android-sovelluskaupasta 16387 satunnaista ilmaista sovellusta, ja löysivät salasanojen kommunikaatiokanavan toteutuksissa puutteita noin 90 % sovelluksista (Ma ym. 2019).

Hyökkäysten lisäksi tunnistautumisjärjestelmä on mahdollista murtaa erilaisin luovin keinoin. Luovia hyökkäystapoja ovat esimerkiksi hyökkäykset tunnistautumisjärjestelmien salasanan palautusjärjestelmiin. Unohtuneiden salasanojen palautusjärjestelmät ovatkin usein hyökkäysten kohteena (Innocenti ym. 2021; Moallem 2011). Raponi ja Pietro (2018) tarkastelivat 174 eri nettisivua Euroopan TOP-1000 suosituimmista sivuista, joista he löysivät 76 sivua, jotka sisälsivät haavoittuvuuksia erilaisille luoville hyökkäyksille. Samalla tavalla Heen ja Neumann (2017) osoittivat, että käyttäjätunnukset voidaan varastaa murtamatta yhtäkään salasanaa tunnistautumisjärjestelmien muiden aukkojen ansiosta.

3.2 Ihmiset ja tietoturvavaatimukset

Morris ja Thompson (1979) kertoivat siitä jo yli 40 vuotta sitten – vaikka tunnistautumisjärjestelmässä ei olisi tiedossa olevia murtokohteita, voi tietojärjestelmään silti murtautua

käyttäjien tietoturvattomien salasanojen takia. Ilman salasanarajoituksia, kuten pituutta tai merkkien lukumäärä, ihmiset luovat heikkoja ja arvattavia salasanoja (Alebouyeh ja Bidgoly 2021). Tilannetta ei kuitenkaan helpota se, että ihmiset luovat silti heikkoja ja arvattavia salasanoja, vaikka salasananluontimääritykset olisivatkin olemassa.

Taylor ja Garry (2019) osoittivat, että ihmiset hyödyntävät salasanoja henkilökohtaisten asioiden muistamiseen – kuten syntymäpäivien, puhelinnumeroiden tai merkittävien tapahtumien ylös kirjaamiseen. AlSabah, Oligeri ja Riley (2018) huomasivat, että niinkin arkaluontoisessa tietojärjestelmässä kuin pankissa, käyttäjien salasanoista paljastui helposti arvattavia osoitteita, nimiä, päivämääriä sekä puhelinnumeroja.

Lisäksi käyttäjät uusiokäyttävät salasanojaan eri järjestelmissä – mikä on usein vastoin tunnistautumisjärjestelmien ohjeita. Vaikka osa käyttäjistä voikin tehdä tietoisen päätöksen salasanan uudelleenkäytöstä, niin osa saattaa tehdä sen vahingossa. Salasanojen muistaminen onkin kognitiivisesti työlästä, minkä takia ihmiset joutuvat turvautumaan tietoturvattomiin salasananhallintakäytänteihin, jotka sisältävät myös niiden ylös kirjaamiseen turvattomasti (Stobert ja Biddle 2018).

Bangin ym. (2012) mukaan käyttäjät eivät ole tietoisia käyttämiensä salasanojen tietoturvatilanteesta, kuten kuinka vähän erilaisia uniikkeja salasanoja he todellisuudessa käyttävät. Ja kun osallistujille kerrottiin heidän heikoista salasanakäytänteistään, niin ainoastaan 4 % heistä päivitti salasanansa (Bang ym. 2012). Ihmisillä onkin todettu olevan vahva vastarinta päivittää jo totuttuja tapoja hallinnoida salasanoja eri järjestelmissä (Renaud, Otondo ja Warkentin 2019). Imamaliyevin ja Khudoykulovin (2021) mukaan käytetyimmätkään tunnistautumisjärjestelmät eivät pysty estämään käyttäjiä luomasta yksinkertaisia ja heikkoja salasanoja.

3.3 Järjestelmien ja ihmisten yhteistyö

Käyttäjien huonoja salasanakäytänteitä on vaikea päivittää, kun eri järjestelmät ohjeistavat erilaisia salasanakäytänteitä, jotka ovat keskenään ristiriidassa (He, Alem ja Wang 2020). Toki vaikka ylläpito-ohjeet olisivatkin yhtenäiset, käyttäisivät ihmiset siltikin heikkoja salasanoja kyseisissä tunnistautumisjärjestelmissä (He, Alem ja Wang 2020; Mohamedali ja

Fadlalla 2017). Syy on hyvin yksinkertainen; ihmiset eivät pysty muistamaan useampaa kuin muutaman monimutkaisen salasanan (Bang ym. 2012). Uniikkeja salasanoja ei yksinkertaisesti voi olla niin monta, kuin mitä tunnistautumisjärjestelmät vaativat. Toki Lorenzin, Kikkasin ja Kloosterin (2013) mukaan toinen syy voi olla se, etteivät käyttäjät ymmärrä perusteluita salasanakäytännöille ja täten sivuuttavat ne. Hyvät ohjeet eivät myöskään takaa sitä, että käyttäjät ymmärtäisivät ohjeet samalla tavalla kuin ylläpito-ohjeiden kirjoittajat (Lorenz, Kikkas ja Klooster 2013).

Lisäksi ihmisten ja tunnistautumisjärjestelmien suhteeseen liittyy uusi haaste – IoT-laitteilla salasanojen syöttö koetaan entistä raskaammaksi (Zezschwitz, Luca ja Hussmann 2013). Samaan tulokseen tulivat Farcasin ja Chan-tin (2015), joiden mukaan IoT-laitteilla salasanojen syöttö tunnistautumisjärjestelmiin on käyttäjäkokemukseltaan heikkoa, jos saatavilla ei ole näppäimistöä. Heidän mukaansa onkin odotettavissa, että salasanaa hyödyntävien tietojärjestelmien tietoturva tulee kärsimään, kun käyttäjät hakevat tietoturvaa enemmän parempaa käyttäjäkokemusta tekemällä salasanoista entistä yksinkertaisempia. Lisäksi käyttäjien salasanojen tietoturvallisuus heikkenee sitä mukaa, mitä useampia salasanoja hyödyntäviä tunnistautumisjärjestelmiä he käyttävät. (Farcasin ja Chan-tin 2015.)

Ihmisillä on taipumusta uusiokäyttää monimutkaisimpia salasanojaan toisissa järjestelmissä enemmän kuin yksinkertaisia salasanojaan, mikä tekee monimutkaisista salasanoista hyödyttömiä, jos hyökkääjä murtaa heikon sivun (He, Alem ja Wang 2020; Bailey, Dürmuth ja Paar 2014). Ongelmallista tästä tekee se, että käyttäjät eivät voi itse päätellä tunnistautumisjärjestelmistä, kuinka tietoturvallisia ne ovat (Bauman, Lu ja Lin 2015, s. 257–261). Imamaliyevin ja Khudoykulovin (2021) mukaan heikkoja salasanakäytänteitä hyödyntäviä käyttäjiä ei auta kukaan.

Lisäksi on huomattu, että vuodetuissa tietokannoissa salasanat noudattavat Zipfin lakia (Alebouyeh ja Bidgoly 2021; Wang ja Wang 2016). Käytännössä Zipfin laki tarkoittaa sitä, että käytetyin salasana esiintyy aina vuodetuissa tietokannoissa noin kaksi kertaa niin useasti kuin toiseksi yleisin salasana. Vastaavasti käytetyin salasana esiintyy noin kolme kertaa niin useasti kuin kolmanneksi yleisin salasana, ja niin edelleen. Salasanojen tiivisteillä suojatut tietokannat sivuuttavatkin usein sen faktan, että ihmiset käyttävät keskenään samoja salasanoja. Tämän myötä varsinkin vanhentuneilla tiivistefunktiolla tallennetut ihmisten salasa-

natietokannat ovatkin helppo murtokohde hyökkääjille, sillä yleisimmin käytetyt salasanat voidaan arvata hyödyntämällä jo vuodettuja tietokantoja (Pelchen ym. 2019). Esimerkiksi AlSabah, Oligeri ja Riley (2018) mursivat vuoden 2016 *md5*-tiivisteillä suojatusta Lähi-idän pankin tietokannasta 79,760 salasanaa, mikä oli 81.66 % koko vuodetusta tietokannasta. Ainoastaan vaikeat, eli uniikit ja entropialtaan monimutkaiset salasanat jäivät murtamatta (AlSabah, Oligeri ja Riley 2018).

4 Ratkaisuehdotuksia salasanojen tietoturvan parantamiseksi

Vaikka salasanapohjaiset tunnistautumisjärjestelmät ovatkin teknisesti yksinkertaisia ja helppoja toteuttaa, niiden tietoturva ei sitä ole. Todistuksena tästä voidaan pitää jo vuodettujen tietokantojen suurta lukumäärää. Salasanapohjaiset tunnistautumisjärjestelmät ovat hankalia implementoida tietoturvallisesti – aikaisemmin tietoturvallisina pidetyt toteutukset voivat olla jo murrettuja, mutta sellaista tietoa on vaikea löytää, jos etsijällä ei ole kattavaa kyberturvaosaamista.

Lisäksi tunnistautumisjärjestelmää toteuttaessa otetaan harvoin huomioon käyttäjien tarpeet, vaikka käyttäjillä on suuri rooli tunnistautumisjärjestelmän tietoturvallisuudessa. Käyttäjiä kiinnostaa valitettavasti tietoturvaa enemmän tunnistautumisjärjestelmien käyttäjäkokemus – asia, jota harvoin huomioidaan tunnistautumisjärjestelmien toteutuksessa. Käyttäjäkokemus on varsinkin otettava huomioon IoT-pohjaisissa tunnistautumisjärjestelmissä, joissa salasanoja ei voida välttämättä kirjoittaa näppäimistön avulla.

Toisen osapuolen huomioimatta jättämisen lisäksi salasanapohjaisissa tunnistautumisjärjestelmissä vallitsee epäluottamus – käyttäjät eivät voi luottaa siihen, että heidän käyttämänsä tunnistautumisjärjestelmät ovat tietoturvallisesti ajan tasalla (Heen ja Neumann 2017). Tunnistautumisjärjestelmillä ei ole myöskään keinoa selvittää sitä, kuinka tietoturvallisia käyttäjien salasanat todella ovat; käytetäänkö salasanoja esimerkiksi muissa heikoimmissa tunnistautumisjärjestelmissä tai ovatko salasanat muiden tiedossa. Esitettyjen syiden vuoksi tietoturvan parantamiseksi on ehdotettu salasananhallintajärjestelmien (engl. *passwordmanagers*) käyttöä käyttäjille, keskitettyjen tunnistautumisjärjestelmien käyttöönottoa organisaatioille, sekä useampaa tunnistautumisvaihetta käyttäjien ja järjestelmien yhteistyön merkityksen vähentämiseksi.

4.1 Salasananhallintajärjestelmät

Kuten jo aikaisemmin kävi ilmi, salasanojen luominen ja ylläpito on haastavaa käyttäjille, eivätkä käyttäjien nykyisellään keksimät salasanat täytä vaatimuksia, joilla tunnistautumisjärjestelmät olisivat tietoturvallisia. Salasanojen heikkouden lisäksi käyttäjillä on haasteita hallinnoida salasanoja turvallisesti, mikä puolestaan johtaa esimerkiksi siihen, että salasanoja uusiokäytetään muissa tunnistautumisjärjestelmissä. Ongelmallista salasanojen uusiokäyttämisessä on se, että tunnistautumisjärjestelmät eivät ole keskenään yhtä tietoturvallisia; käyttäjien käyttämiä salasanoja vuodetaan ja varastetaan jatkuvasti, koska tunnistautumisjärjestelmien tietoturvallinen toteutus on haastavaa. Käyttäjiltä puuttuukin keino varmistaa käyttämiensä tunnistautumisjärjestelmien tietoturvan ajantasaisuus, mikä puolestaan tarkoittaa sitä, että käyttäjät eivät voi luottaa siihen, että salasanat olisivat suojattuna tunnistautumisjärjestelmissä. Salasananhallintajärjestelmät oikein käytettyinä minimoivat edellä mainittuja haasteita käyttäjien näkökulmasta – tunnistautumisjärjestelmien tietoturva riippuisi tällöin tunnistautumisjärjestelmien toteutuksesta, koska käyttäjille esitetyt tietoturvavaatimukset täyttyisivät. Lisäksi Doğanayn ja Küpçün (2020) mukaan salasananhallintajärjestelmät suojaavat oikein käytettynä käyttäjiä heikkojen salasanojen lisäksi myös tietojenkalasteluyrityksiltä.

Käytännössä salasananhallintajärjestelmällä tarkoitetaan käyttäjän elektronisessa objektissa sijaitsevaa sovellusta, jonka avulla käyttäjä voi luoda ja hallinnoida eri tunnistautumisjärjestelmien salasanoja tietoturvallisesti. Salasanat voivat tällöin täyttää aina järjestelmän, sekä käyttäjän itsensä, asettamat tietoturvatasot salasanoille. Salasananhallintajärjestelmää käyttäessä käyttäjällä tulee olla avain, kuten salasana, jolla salasananhallintajärjestelmän tietokanta salataan (engl. *encrypt*). Kyseistä avainta käytetään, kun salasananhallintajärjestelmän salasanoihin tarvitsee päästä käsiksi esimerkiksi tunnistautumisvaiheissa. (Blauw 2017.)

Salasananhallintajärjestelmää tuleekin ajatella siten, että tietoon pohjautuvat tunnistautumisjärjestelmät muuttuvat omistuspohjaisiksi järjestelmiksi. Käyttäjä todistaa henkilöllisyytensä salasanojen sijaan objektilla, joka on tässä tapauksessa käyttäjän hallussa oleva salasananhallintajärjestelmä. Salasananhallintajärjestelmän tietokannan salaaminen avaimella puolestaan estää salasanojen vahingollisen vuotamisen, jota voi tapahtua muilla ylöskirjaamistekniikoilla. Esimerkiksi Kimin, Yaon, Dunin ym. (2022) mukaan varsinkin iäkkäät ihmiset kirjaavat

salasanojaan ylös.

Salasananhallintajärjestelmät ovat itsessään tunnistautumisjärjestelmiä, minkä takia ne ovat alttiita samanlaisille hyökkäyksille kuin muutkin tunnistautumisjärjestelmät – tosin Blauwin (2017) mukaan pienemmässä mittakaavassa. Tiedostettu haaste salasananhallintajärjestelmillä on se, kuinka ihmiset saadaan käyttämään niitä. Kuten tunnistautumisjärjestelmissä, niin salasananhallintajärjestelmissäkin käyttäjiä vaivaa pelko tietoturvattomasta järjestelmästä (Ayyagari, Lim ja Hoxha 2019). Ymmärtämättömyys salasananhallintajärjestelmien toiminnasta sekä salasanojen luovuttaminen uuden järjestelmän haltuun hidastaakin, ellei jopa estä, osaa käyttäjistä siirtymästä salasananhallintajärjestelmiin (Ayyagari, Lim ja Hoxha 2019). Sama haaste on myös organisaatiotasolla (Farooq ym. 2021), mikä puolestaan johtaa siihen, että tunnistautumisjärjestelmät eivät aina tue salasananhallintajärjestelmiä siten, että niitä voitaisiin käyttää tietoturvallisesti osana kirjautumisprosessia (Blauw 2017; Fahl ym. 2013). Salasananhallintajärjestelmä ei myöskään ratkaise tunnistautumisjärjestelmän näkökannalta tietoturvattomien salasanojen käyttöä, koska vastuu salasananhallintajärjestelmien oikeinkäytöstä on käyttäjillä.

4.2 Keskitetyt tunnistautumisjärjestelmät

Vaikka salasananhallintajärjestelmät tarjoavat käyttäjille tavan hallinnoida omia tilejä ajantasaisella tietoturvalla, niin Doğanayn ja Küpçün (2020) mukaan tunnistautumisjärjestelmien on mahdotonta valvoa niiden oikeaoppista käyttöä. Ratkaisuksi on ehdotettu keskitettyä tunnistautumisjärjestelmää, joka siirtäisi salasanojen ylläpitovastuuta käyttäjiltä järjestelmille.

Keskitetyllä tunnistautumisjärjestelmällä tarkoitetaan tunnistautumisjärjestelmää, jonka avulla kirjaudutaan useampaan tunnistautumisjärjestelmään yhden, keskitetyn tunnistautumisjärjestelmän kautta (Doğanay ja Küpçü 2020). Samoin kuin salasananhallintajärjestelmässä, keskitetyssä tunnistautumisjärjestelmässä käyttäjä kirjautuu useaan eri tunnistautumisjärjestelmään yhdellä ja samalla avaimella, kuten salasanalla (İşler, Küpçü ja Coskun 2019). Keskitettyjä tunnistautumisjärjestelmiä kutsutaan myös lyhenteellä SPA, joka tulee englanninkielisestä sanasta *single-password authentication* (Doğanay ja Küpçü 2020; İşler, Küpçü ja Coskun 2019). Esimerkkeinä jo käytössä olevista keskitetystä tunnistautumisjärjestelmistä

voidaan pitää Facebookia (Facebook 2022), Googlea (Google 2022) ja Suomi.fi-palvelua (Suomi.fi 2022).

Keskitettyä tunnistautumisjärjestelmää voikin ajatella salasananhallintajärjestelmänä, jonka tietoturvasta on vastuussa tunnistautumisjärjestelmä käyttäjän sijasta. Doğanay ja Küpçü (2020) sekä İşler, Küpçü ja Coskun (2019) väittävät, että keskitetyt tunnistautumisjärjestelmät tarjoavat samat hyödyt kuin mitä salasananhallintajärjestelmät tarjoavat oikein käytettyinä, mutta kaikille käyttäjille. Keskitetty tunnistautumisjärjestelmä pienentää käyttäjien epätasa-arvoa, joka juontuu käyttäjien erilaisista salasanojen hallinnointitavoista. Hatzivasilis (2020) mukaan suurten organisaatioiden keskitettyjen tunnistautumisjärjestelmien hyödyntäminen on kannattavaa pienille organisaatioille, koska heidän ei tarvitsisi ylläpitää oman tunnistautumisjärjestelmän tietoturvaa.

Käyttäjänäkökulmasta keskitetty tunnistautumisjärjestelmä vähentää eri käyttäjätilien ylläpitoa. Riskinä tosin on, että keskitetyn tunnistautumisjärjestelmän käyttäjät käyttävät samoja salasanoja tietoturvattomissa järjestelmissä. Bang ym. (2012) mielestä salasanoja hyödyntävissä järjestelmissä tulisikin aina olettaa, että käyttäjät uusiokäyttävät salasanojaan muissakin järjestelmissä. Keskitetyt tunnistautumisjärjestelmät eivät myöskään takaa käyttäjille sitä, että niiden suojaus olisi ajantasalla.

4.3 Yksivaiheisesta tunnistautumisesta monivaiheiseksi

Vaikka salasananhallintajärjestelmät ja keskitetyt tunnistautumisjärjestelmät minimoivat tietoturvaongelmia joita ihmiset ja tunnistautumisjärjestelmät saattavat toisilleen aiheuttaa, eivät ne ratkaise osapuolten välillä vallitsevaa luottamuspulaa. Salasanoja käyttävät tunnistautumisjärjestelmät vaativatkin yhteistyötä käyttäjien ja tunnistautumisjärjestelmien välillä, mutta ilman luottamusta yhteistyöllä ei merkitystä. Ratkaisuksi on esitetty salasanojen merkityksen pienentämistä tunnistautumisjärjestelmissä muuttamalla tunnistautumisjärjestelmät yksivaiheisista monivaiheisiksi (Chuat, Plocher ja Perrig 2020; Ometov ym. 2018). Chuat'n, Plocherin ja Perrigin mukaan älypuhelimet mahdollistavat kustannustehokkaat monivaiheiset tunnistautumisjärjestelmät (Chuat, Plocher ja Perrig 2020). Tunnistautumisvaiheita lisättäessä, salasanojen tietoturvariskien merkitys supistuu kokonaistietoturvassa, jol-

loin myös käyttäjän ja tunnistautumisjärjestelmän välisen luottamuspulan laajakantoisuus vähenee. Voidaankin ajatella, että monivaiheisessa tunnistautumisessa hyväksytään se, että niin käyttäjien kuin tunnistautumisjärjestelmien tietoturvassa saattaa ilmetä tietoturvapuutteita.

Monivaihetunnistautumista (engl. *multi-factor authentication*), eli MFAta, kutsutaan myös vahvaksi tunnistautumiseksi (Kyberturvallisuuskeskus 2022). Lisäksi kaksivaiheisia tunnistautumisjärjestelmiä (engl. *two-factor authentication*) saatetaan kutsua myös lyhenteellä 2FA. Yksivaiheisia tunnistautumisjärjestelmiä (engl. *single-factor authentication*) on puolestaan ruvettu kutsumaan SFAksi. SFAta pidetään yleisesti heikkoina tunnistautumisena, koska tunnistautumisjärjestelmän murtumiskohtia on ainoastaan yksi.

Ennen itse tunnistautumista voidaan hyödyntää tunnistautuvasta käyttäjästä saatavia metatietoja määrittelemään tunnistautumisvaiheiden lukumäärän. Järjestelmä voisi esimerkiksi lisätä tunnistautumisvaiheita, mikäli käyttäjän IP-osoite ei ole entuudestaan tuttu, tai vähentää niitä, jos käyttäjä tunnistautuu organisaation sisäverkosta. (Dasgupta, Roy ja Nag 2016). Monivaiheisessa tunnistautumisessa voidaan hyödyntää myös useampaa kuin yhtä tunnistautumismenetelmää.

Monivaiheisten tunnistautumisjärjestelmien haasteena on saavuttaa se sama yksinkertaisuus, mitä salasanat tarjoavat tunnistautumisessa (Rui ja Yan 2018). Koska Zimmermannin ja Gerberin (2020) tutkimuksen mukaan tunnistautuminen on käyttäjille toissijainen asia, ja tärkeämpää on käyttäjäkokemus ja palvelun nopea saanti, voisi biometriikasta olla hyötyä tunnistautumisprosessissa. Biometriikka koetaan tunnistautumismenetelmien kolmesta pääkategoriasta käyttäjäystävällisimmäksi (Ometov ym. 2018), ja lisäksi biometriikkaa mittaavia sensoreita löytyy usein erilaisista IoT-laitteista, jotka ovat jo valmiiksi yleisesti huonompia merkkijonojen, kuten salasanojen syöttämiseen. Zimmermannin ja Gerberin (2020) tutkimuksessa käyttäjät kokivat biometriikan myös tietoturvalliseksi. Tosin pieni merkitsevä osa tulkitsi sormenjäljen tietoturvattomaksi (Zimmermann ja Gerber 2020).

Monivaiheiset tunnistautumisjärjestelmät sisältävät myös omat tietoturvahaasteensa, joiden ratkaiseminen saattaa olla haastavaa. Onkin ennustettu, että tulevaisuudessa tunnistautumisjärjestelmien olemus muuttuu biometriikkatapaisemmaksi, jossa tunnistautumisjärjestelmä

on toiminnassa koko käyttäjän session ajan pelkän alkukirjautumisen sijasta. Ometovin ym. (2018) mukaan jatkuvassa tunnistautumisessa käyttäjän autenttisuutta mitataan jatkuvasti erilaisilla käyttäytymisbiometriikoilla. Jatkuvaa tunnistautumista kutsutaankin myös passiiviseksi biometriikaksi (Ometov ym. 2018). Kuten biometriikassa, jatkuvassa tunnistautumisessakin käyttäjän autenttisuus määritellään todennäköisyyksillä. Jos käyttäjän autenttisuuden todennäköisyys pienenee ennalta määrätyn prosentin alapuolelle, kirjataan käyttäjä ulos tietojärjestelmästä. Voidaankin ajatella, että tavanomaiset tunnistautumisjärjestelmät noudattavat samaa todennäköisyysmenetelmää – alkukirjautumisen jälkeen käyttäjän autenttisuus on järjestelmän mukaan täydet 100 % aikakatkaisuun tai uloskirjautumiseen saakka, jolloin käyttäjän autenttisuuden todennäköisyydestä tulee 0 %.

5 Yhteenveto

Viimeistään IoT-aikakaudella salasanapohjaisten tunnistautumisjärjestelmien tarjoamat hyödyt voidaan kyseenalaistaa. Vaihtoehtoisia tunnistautumismenetelmiä voidaan hyödyntää käyttäjien jo kantamilla IoT-laitteilla, mikä poistaa vaihtoehtoisten tunnistautumisjärjestelmien laitekustannukset (Chuat, Plocher ja Perrig 2020).

Salasanapohjaiset tunnistautumisjärjestelmät eivät ole kuitenkaan poistumassa – niillä on selvä etumatka muihin tunnistautumisjärjestelmiin, ja niiden toteutus on yksinkertaista eikä vaadi alan asiantuntijuutta (Bauman, Lu ja Lin 2015). Valitettavasti salasanapohjaisten tunnistautumisjärjestelmien tietoturva ei ole yhtä yksinkertaista toteuttaa tai ylläpitää. Tietoturvattomia salasanajärjestelmiä on ja tulee olemaan jatkossakin.

Myös ihmisillä on iso rooli järjestelmien kokonaistietoturvan kannalta. Vaikka tunnistautumisjärjestelmä olisi ajantasaisesti suojattu, ei mikään estä käyttäjiä käyttämästä tietoturvattomia salasanoja kyseisissä järjestelmissä. Tietoturvattomia salasanoja luodaan, vaikka määritykset pyrkisivätkin ne estämään. Käyttäjät eivät huomioi tunnistautumisjärjestelmien asettamia vaatimuksia tietoturvallisille salasanoille – osin ihmisten kognitiivisten rajoitteiden takia, mutta osin myös omasta tahdosta. Käyttäjiä kiinnostaa tietoturvaa enemmän käyttäjäkokemus ja tunnistautuminen koetaan hidasteeksi todelliselle tekemiselle.

Salasanapohjaiset tunnistautumisjärjestelmät tarvitsevatkin käyttäjien ja tunnistautumisjärjestelmien välille toimivan yhteistyön, jotta järjestelmä olisi tietoturvallinen. Yhteistyö ei kuitenkaan toimi, sillä osapuolten välillä vallitsee luottamuspula. Se juontuu siitä, että järjestelmät eivät voi tarkastaa, kuinka tietoturvallisia käyttäjien salasanat ovat, eivätkä käyttäjät voi tarkastaa, ovatko tunnistautumisjärjestelmät tietoturvallisia.

Tutkielmassa listatut ratkaisuehdotukset olivat salasanhallintajärjestelmät, keskitetyt tunnistautumisjärjestelmät ja monivaihetunnistautuminen. Nämä ratkaisuehdotukset pyrkivät vähentämään tietojärjestelmien ja käyttäjien välisen yhteistyön haasteita eri näkökannoilta. Tutkielmassa ei käsitelty ratkaisuehdotusten tietoturvaa, kuten vaikutuksia tietovuodon yhteydessä, mikä tulisi tulevaisuudessa ottaa huomioon. Jatkossa voitaisiin tutkia ratkaisuehdotusten tietoturvaa sekä sitä, miten niiden käyttöönottoa voitaisiin edistää.

Lähteet

Adobe. 2021. *Customer security alert.* Saatavilla WWW-muodossa, https://helpx.adobe.com/x-productkb/policy-pricing/customer-alert.html, viitattu 23.4.2022.

Alebouyeh, Zeinab, ja Amir Jalaly Bidgoly. 2021. "Zipf's law analysis on the leaked Iranian users' passwords". *Journal of Computer Virology and Hacking Techniques,* 1–16. https://doi.org/10.1007/s11416-021-00397-9.

AlJanah, Salem, Ning Zhang ja Siok Wah Tay. 2021. "A Survey on Smart Home Authentication: Toward Secure, Multi-Level and Interaction-Based Identification". *IEEE Access* 9:130914–130927. https://doi.org/10.1109/ACCESS.2021.3114152.

AlSabah, Mashael, Gabriele Oligeri ja Ryan Riley. 2018. "Your culture is in your password: An analysis of a demographically-diverse password dataset". *Computers & security* 77:427–441. https://doi.org/10.1016/j.cose.2018.03.014.

Alt, Florian, ja Stefan Schneegass. 2022. "Beyond Passwords—Challenges and Opportunities of Future Authentication". *IEEE Security & Privacy* 20 (1): 82–86. https://doi.org/10.1109/MSEC.2021.3127459.

Awasthi, Akshay. 2015. "Reducing Identity Theft Using One-Time Passwords and SMS". *EDPACS* 52 (5): 9–19. https://doi.org/10.1080/07366981.2015.1104935.

Ayyagari, Ramakrishna, Jaejoo Lim ja Olger Hoxha. 2019. "Why do not we use password managers? A study on the intention to use password managers". *Contemporary Management Research* 15 (4): 227–245. https://doi.org/10.7903/cmr.19394.

Bailey, Daniel V, Markus Dürmuth ja Christof Paar. 2014. "Statistics on password re-use and adaptive strength for financial accounts". Teoksessa *International Conference on Security and Cryptography for Networks,* 218–235. Springer. https://doi.org/10.1007/978-3-319-10879-7_13.

Bang, Youngsok, Dong-Joo Lee, Yoon-Soo Bae ja Jae-Hyeon Ahn. 2012. “Improving information security management: An analysis of ID–password usage and a new login vulnerability measure”. *international journal of information management* 32 (5): 409–418. https://doi.org/10.1016/j.ijinfomgt.2012.01.001.

Barkadehi, Mohammadreza Hazhirpasand, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi ja Sarminah Samad. 2018. “Authentication systems: A literature review and classification”. *Telematics and Informatics* 35 (5): 1491–1511. https://doi.org/10.1016/j.tele.2018.03.018.

Bauman, Erick, Yafeng Lu ja Zhiqiang Lin. 2015. “Half a century of practice: Who is still storing plaintext passwords?” Teoksessa *International conference on information security practice and experience,* 253–267. Springer. https://doi.org/10.1007/978-3-319-17533-1_18.

Blauw, Frans F. 2017. “Dear Password, I Know You Too Well”. Teoksessa *International Conference on Human Aspects of Information Security, Privacy, and Trust,* 212–225. Springer. https://doi.org/10.1007/978-3-319-58460-7_14.

Bonneau, Joseph, Cormac Herley, Paul C Van Oorschot ja Frank Stajano. 2012. “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes”. Teoksessa *2012 IEEE Symposium on Security and Privacy,* 553–567. IEEE. https://doi.org/10.1109/SP.2012.44.

Chuat, Laurent, Sarah Plocher ja Adrian Perrig. 2020. “Zero-Knowledge User Authentication: An Old Idea Whose Time Has Come”. Teoksessa *Security Protocols XXVII,* toimittanut Jonathan Anderson, Frank Stajano, Bruce Christianson ja Vashek Matyáš, 203–212. Cham: Springer, Springer International Publishing. ISBN: 978-3-030-57043-9. https://doi.org/10.1007/978-3-030-57043-9_19.

Dasgupta, Dipankar, Arunava Roy ja Abhijit Nag. 2016. “Toward the design of adaptive selection strategies for multi-factor authentication”. *computers & security* 63:85–116. https://doi.org/10.1016/j.cose.2016.09.004.

Doğanay, Cansu, ja Alptekin Küpçü. 2020. “Comparative survey on single password authentication techniques”. Teoksessa *2020 International Conference on Information Security and Cryptology (ISCTURKEY),* 5–10. IEEE. https://doi.org/10.1109/ISCTURKEY51113.2020.9307989.

Facebook. 2022. *Using Facebook Login with Existing Login Systems.* Saatavilla WWW-muodossa, https://developers.facebook.com/docs/facebook-login/guides/advanced/existing-system, viitattu 18.4.2022.

Fahl, Sascha, Marian Harbach, Marten Oltrogge, Thomas Muders ja Matthew Smith. 2013. “Hey, you, get off of my clipboard”. Teoksessa *International Conference on Financial Cryptography and Data Security,* 144–161. Springer. https://doi.org/10.1007/978-3-642-39884-1_12.

Farcasin, Michael, ja Eric Chan-tin. 2015. “Why we hate IT: two surveys on pre-generated and expiring passwords in an academic setting”. *Security and Communication Networks* 8 (13): 2361–2373. https://doi.org/10.1002/sec.1184.

Farooq, Ali, Alina Dubinina, Seppo Virtanen ja Jouni Isoaho. 2021. “Understanding dynamics of initial trust and its antecedents in password managers adoption intention among young adults”. *Procedia Computer Science* 184:266–274. https://doi.org/10.1016/j.procs.2021.03.036.

Google. 2022. *Use your Google Account to sign in to other apps or services.* Saatavilla WWW-muodossa, https://support.google.com/accounts/answer/112802, viitattu 18.4.2022.

Hatzivasilis, George. 2020. “Password Management: How Secure Is Your Login Process?” Teoksessa *International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity,* 157–177. Springer. https://doi.org/10.1007/978-3-030-62433-0_10.

He, Yongzhong, Endalew Elsabeth Alem ja Wei Wang. 2020. “Hybritus: a password strength checker by ensemble learning from the query feedbacks of websites”. *Frontiers of Computer Science* 14 (3): 1–14. https://doi.org/10.1007/s11704-019-7342-y.

Heen, Olivier, ja Christoph Neumann. 2017. “On the privacy impacts of publicly leaked password databases”. Teoksessa *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment,* 347–365. Springer. https://doi.org/10.1007/978-3-319-60876-1_16.

Herley, Cormac, ja Paul Van Oorschot. 2011. “A research agenda acknowledging the persistence of passwords”. *IEEE Security & privacy* 10 (1): 28–36. https://doi.org/10.1109/MSP.2011.150.

Hern, Alex. 2013. *Did your Adobe password leak? Now you and 150m others can check.* Saatavilla WWW-muodossa, https://www.theguardian.com/technology/2013/nov/07/adobe-password-leak-can-check, viitattu 24.4.2022.

Imamaliyev, Aybek, ja Zarif Khudoykulov. 2021. “Analysis Password-based Authentication Systems with Password Policy”. Teoksessa *2021 International Conference on Information Science and Communications Technologies (ICISCT),* 1–3. IEEE. https://doi.org/10.1109/ICISCT52966.2021.9670312.

Innocenti, Tommaso, Seyed Ali Mirheidari, Amin Kharraz, Bruno Crispo ja Engin Kirda. 2021. “You’ve Got (a Reset) Mail: A Security Analysis of Email-Based Password Reset Procedures”. Teoksessa *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment,* 1–20. Springer. https://doi.org/10.1007/978-3-030-80825-9_1.

İşler, Devriş, Alptekin Küpçü ja Aykut Coskun. 2019. “User perceptions of security and usability of mobile-based single password authentication and two-factor authentication”. Teoksessa *Data Privacy Management, Cryptocurrencies and Blockchain Technology,* 99–117. Springer. https://doi.org/10.1007/978-3-030-31500-9_7.

Khan, Laheem, Kovila PL Coopamootoo ja Magdalene Ng. 2020. “Not Annoying the User for Better Password Choice: Effect of Incidental Anger Emotion on Password Choice”. Teoksessa *International Conference on Human-Computer Interaction,* 143–161. Springer. https://doi.org/10.1007/978-3-030-50309-3_10.

Kim, Sunyoung, Willow Yao, Xiaotong Du ym. 2022. “Exploring Older Adults’ Adoption and Use of a Tablet Computer During COVID-19: Longitudinal Qualitative Study”. *JMIR aging* 5 (1): e32957. https://doi.org/10.2196/32957.

Kyberturvallisuuskeskus. 2020. *SHA-1-tiivistefunktio on lopullisesti murrettu.* Saatavilla WWW-muodossa, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/sha-1-tiivistefunktio-lopullisesti-murrettu, viitattu 18.4.2022.

———. 2022. *Sähköinen tunnistautuminen.* Saatavilla WWW-muodossa, https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen, viitattu 18.4.2022.

Li, Yue, Zeyu Chen, Haining Wang, Kun Sun ja Sushil Jajodia. 2020. “Understanding Account Recovery in the Wild and Its Security Implications”. *IEEE Transactions on Dependable and Secure Computing,* https://doi.org/10.1109/TDSC.2020.2975789.

Liao, I-En, Cheng-Chi Lee ja Min-Shiang Hwang. 2006. “A password authentication scheme over insecure networks”. *Journal of Computer and System Sciences* 72 (4): 727–740. https://doi.org/10.1016/j.jcss.2005.10.001.

Lorenz, Birgy, Kaido Kikkas ja Aare Klooster. 2013. ““The four most-used passwords are love, sex, secret, and god”: password security and training in different user groups”. Teoksessa *International Conference on Human Aspects of Information Security, Privacy, and Trust,* 276–283. Springer. https://doi.org/10.1007/978-3-642-39345-7_29.

Ma, Siqi, Elisa Bertino, Surya Nepal, Juanru Li, Diethelm Ostry, Robert H Deng ja Sanjay Jha. 2019. “Finding flaws from password authentication code in android apps”. Teoksessa *European Symposium on Research in Computer Security,* 619–637. Springer. https://doi.org/10.1007/978-3-030-29959-0_30.

Moallem, Abbas. 2011. “Did you forget your password?” Teoksessa *International Conference of Design, User Experience, and Usability,* 29–39. Springer. https://doi.org/10.1007/978-3-642-21708-1_4.

Mohamedali, Intisar A, ja Yahia Fadlalla. 2017. “Securing password in static password-based authentication: A review”. Teoksessa *2017 Sudan Conference on Computer Science and Information Technology (SCCSIT),* 1–5. IEEE. https://doi.org/10.1109/SCCSIT.2017.8293063.

Morake, Abraham, Lucas T Khoza ja Tebogo Bokaba. 2021. “Biometric technology in banking institutions:‘The customers’ perspectives’”. *SA Journal of Information Management* 23 (1): 12. https://doi.org/10.4102/sajim.v23i1.1407.

Morris, Robert, ja Ken Thompson. 1979. “Password security: A case history”. *Communications of the ACM* 22 (11): 594–597. https://doi.org/10.1145/359168.359172.

Ometov, Aleksandr, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen ja Yevgeni Koucheryavy. 2018. “Multi-factor authentication: A survey”. *Cryptography* 2 (1): 1. https://doi.org/10.3390/cryptography2010001.

Pelchen, Chris, David Jaeger, Feng Cheng ja Christoph Meinel. 2019. “The (Persistent) Threat of Weak Passwords: Implementation of a Semi-automatic Password-Cracking Algorithm”. Teoksessa *International Conference on Information Security Practice and Experience,* 464–475. Springer. https://doi.org/10.1007/978-3-030-34339-2_27.

Raponi, Simone, ja Roberto Di Pietro. 2018. “A spark is enough in a straw world: A study of websites password management in the wild”. Teoksessa *International Workshop on Security and Trust Management,* 37–53. Springer. https://doi.org/10.1007/978-3-030-01141-3_3.

Renaud, Karen, Robert Otondo ja Merrill Warkentin. 2019. ““This is the way ‘I’create my passwords”... does the endowment effect deter people from changing the way they create their passwords?” *Computers & Security* 82:241–260. https://doi.org/10.1016/j.cose.2018.12.018.

Rui, Zhang, ja Zheng Yan. 2018. “A survey on biometric authentication: Toward secure and privacy-preserving identification”. *IEEE access* 7:5994–6009. https://doi.org/10.1109/ACCESS.2018.2889996.

Sasse, Martina Angela, Sacha Brostoff ja Dirk Weirich. 2001. “Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security”. *BT technology journal* 19 (3): 122–131. https://doi.org/10.1023/A:1011902718709.

Schafer, Cameron R, ja Lei Pan. 2019. “Password Strength Estimators Trained on the Leaked Password Lists”. Teoksessa *International Conference on Applications and Techniques in Information Security,* 219–231. Springer. https://doi.org/10.1007/978-981-15-0871-4_17.

Stajano, Frank. 2011. “Pico: No more passwords!” Teoksessa *International Workshop on Security Protocols,* 49–81. Springer. https://doi.org/10.1007/978-3-642-25867-1_6.

Stobert, Elizabeth, ja Robert Biddle. 2018. “The password life cycle”. *ACM Transactions on Privacy and Security (TOPS)* 21 (3): 1–32. https://doi.org/10.1145/3183341.

Suomi.fi. 2022. *Eri tunnistusvälineillä tunnistautuminen.* Saatavilla WWW-muodossa, https://www.suomi.fi/ohjeet-ja-tuki/tietoa-tunnistuksesta/eri-tunnistusvalineilla-tunnistautumine n, viitattu 18.4.2022.

Taylor, Robbie J, ja Maryanne Garry. 2019. “People infuse their passwords with autobiographical information”. *Memory* 27 (5): 581–591. https://doi.org/10.1080/09658211.2018.1539499.

Wang, Chen, Yan Wang, Yingying Chen, Hongbo Liu ja Jian Liu. 2020. “User authentication on mobile devices: Approaches, threats and trends”. *Computer Networks* 170:107118. https://doi.org/10.1016/j.comnet.2020.107118.

Wang, Ding, ja Ping Wang. 2016. “On the implications of Zipf’s law in passwords”. Teoksessa *European Symposium on Research in Computer Security,* 111–131. Springer. https://doi.org/10.1007/978-3-319-45744-4_6.

Zezschwitz, Emanuel von, Alexander De Luca ja Heinrich Hussmann. 2013. “Survival of the shortest: A retrospective analysis of influencing factors on password composition”. Teoksessa *IFIP Conference on Human-Computer Interaction,* 460–467. Springer. https://doi.org/10.1007/978-3-642-40477-1_28.

Zimmermann, Verena, ja Nina Gerber. 2020. “The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes”. *International Journal of Human-Computer Studies* 133:26–44. https://doi.org/10.1016/j.ijhcs.2019.08.006.