Eetu Karjalainen

KÄYTTÄJÄN TUNNISTUS VERKKOPALVELUISSA: FIDO-TEKNOLOGIAN JA MONIVAIHEISEN TUNNISTAUTUMISEN TURVALLISUUS JA KÄYTETTÄVYYS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Karjalainen, Eetu
Käyttäjän tunnistus verkkopalveluissa: Fido-teknologian ja monivaiheisen tunnistautumisen turvallisuus ja käytettävyys
Jyväskylä: Jyväskylän yliopisto, 2024, 23 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Saastamoinen, Anna

Digitalisaation kiihtyessä arkipäiväiset palvelut ovat yhä useammin saatavilla verkkopalveluina. Näin ollen käyttäjän luotettavan tunnistuksen merkitys korostuu etenkin tietoturvakriittisissä prosesseissa, kuten terveyspalveluihin kirjautuessa, kun ihmisten välinen suora vuorovaikutus vähenee. Tekstipohjaiset salasanat ovat edelleen hallitseva menetelmä käyttäjän tunnistuksessa verkkopalveluissa todennäköisesti niiden pitkän historian ansiosta, huolimatta monista turvallisuuspuutteista, joita kyseisen menetelmän käytössä on havaittu vuosien varrella. Tämän kirjallisuuskatsauksena tehdyn tutkielman tarkoituksena oli selvittää neljän vaihtoehtoisen tunnistautumismenetelmän teknisiä turvallisuusseikkoja, sekä niiden käytettävyyttä käyttäjän tunnistuksessa. Tavoitteena oli selvittää olisiko jokin menetelmä jo tarpeeksi kypsä molempien tarkasteltavien attribuuttien osalta korvaamaan tekstipohjaiset salasanat käyttäjän tunnistuksessa, sekä kuinka paljon loppukäyttäjien kokemus niiden käytettävyydestä vaikuttaa niiden hyväksyntään. Erityisenä kiinnostuksen kohteena oli se, kuinka loppukäyttäjät kokevat menetelmien teknisen turvallisuuden ja käytettävyyden yhteensovittamisen tärkeyden. Tulokset osoittavat käytettävyyden olevan merkittävämpi tekijä loppukäyttäjille kuin niiden tekninen turvallisuus huolimatta siitä, että useimmat käyttäjät ovat tietoisia käytettävyyden ja turvallisuuden välisestä käänteisestä riippuvuussuhteesta.

Asiasanat: Käyttäjän tunnistus, FIDO, salasanat, monivaiheinen tunnistautuminen

ABSTRACT

Karjalainen, Eetu
User authentication in web services: The security and usability of FIDO-technology and multi-factor authentication.
Jyväskylä: University of Jyväskylä, 2024, 23 pp.
Information Systems, bachelor's thesis
Supervisor(s): Saastamoinen, Anna

As digitalization accelerates and more services can be found online, the importance of user authentication especially in authentication-critical processes is becoming more and more important as we interact with humans less and less. The text-based passwords reign supreme as the main part of user authentication on web services mainly because of the perceived usability of this familiar method, despite many known security weaknesses they possess. The main purpose of this paper was to gain knowledge of the technical security features and perceived usability of four alternative authentication methods already out there, by doing a literature review. The goal was to find out if there would be one or more methods mature enough to contest the text-based passwords as the new way of authentication in the future, and which factor is more important to end users: security or usability. Particular interest was in how the end users see the tradeoff between security and usability of different methods. The results implied that to the end user, the perceived usability of each authentication method is more important than the security, even though some studies show that most of the users are aware of the negative effect it usually has on security.

Keywords: User authentication, FIDO, passwords, multi-factor authentication

TAULUKOT

SISÄLLYS

1 JOHDANTO

Digitalisaation lisääntyessä jatkuvasti, on ihmisillä alati kasvava määrä palveluita saatavillaan verkon välityksellä. Näihin palveluihin vaaditaan usein tunnistautumista, jotta voidaan varmistaa, että oikea henkilö pääsee käsiksi oikeisiin resursseihin. Käyttäjän tunnistus tapahtuu verkkopalveluissa yleensä käyttäjätunnusten avulla. Teknologioiden kehittyessä kuitenkin myös väärinkäyttäjien kyvyt kehittyvät, jolloin herää kysymys siitä, miten pysyä heidän edellään tietoturva-asioissa. Käyttäjän tunnistus on tärkeä osa tietoturvallisuutta, ja se pohjautuu edelleen suurilta osin tekstipohjaisiin salasanoihin (Sediyono, Santoso & Suhartono, 2013). Tutkimusten mukaan ihmisillä on keskimäärin kymmeniä käyttäjätunnusten salasanoja muistettavanaan (Fidoalliance, 2024; Wang, Zhang, Zhang & Wang, 2020). Näistä salasanoista suurin osa on kierrätettyjä, tai vain vähäisesti muokattuja (Biddle, Chiasson & Van Oorschot, 2012; Campbell, Ma & Kleeman, 2011). Tekstipohjaiset salasanat aiheuttavat tietoturvan kannalta merkittäviä ongelmia, sillä jopa 60–80 % tietomurroista johtuu tunnuksista, jotka on saatu varastettua (Carrillo-Torres, Perez-Diaz, Cantoral-Ceballos & Vargas-Rosales, 2023; Verizon, 2022).

Tekstipohjaiset salasanat ovat erityisen alttiita sanakirja- ja väsytyshyökkäyksille (Alkhwaja ym., 2023), jotka ovat helposti automatisoitavissa, eli toisin sanoen vaativat vähäisen määrän vaivaa hyökkääjiltä. Tämän vuoksi on keksittävä vaihtoehtoisia tunnistusmenetelmiä, jotka ovat vähemmän alttiita etenkin näille automatisoitaville hyökkäysyrityksille. Tässä kirjallisuuskatsauksena tehdyssä kandidaatintutkielmassa perehdytään kahteen vaihtoehtoon lisätä käyttäjien tietoturvaa. Tarkastelu keskittyy valittujen menetelmien tekniseen turvallisuuteen, sekä niiden käytettävyyteen. Nimellisesti nämä vaihtoehdot ovat salasanaton FIDO-teknologia ja monivaiheinen tunnistautuminen. FIDO-teknologia on julkisen avaimen salaukseen pohjautuva käyttäjän tunnistuksen menetelmä, jonka tarkoituksena on parantaa käyttäjän tunnistuksen turvallisuutta poistamalla käyttäjätunnusten kalastelun riski, sekä parantaa tunnistusprosessin käytettävyyttä vähentämällä käyttäjien kokemaa kognitiivista kuormaa (Fidoalliance, 2024). Lyhenne FIDO tulee sanoista Fast Identity Online, ja se on yleisesti käytössä oleva termi kyseiselle menetelmälle. Monivaiheisesta

tunnistautumisesta puolestaan tarkastellaan tarkemmin kolmea yksittäistä tunnistautumismenetelmää, jotka ovat kertakäyttöiset salasanat, biometrinen tunnistautuminen ja graafiset salasanat. Tutkielman tavoitteena on selvittää näiden vaihtoehtojen teknistä tietoturvaa ja käyttäjien kokemaa käytettävyyttä käyttäjän tunnistuksen yhteydessä.

Keskeisinä käsitteinä tutkielman kannalta ovat FIDO-teknologia, monivaiheinen tunnistautuminen, sekä käyttäjän tunnistaminen. Tutkimuskysymys on:

- Mitä turvallisuus-, ja käytettävyyshyötyjä monivaiheisella tunnistautumisella ja FIDO-teknologialla on suhteessa tekstipohjaisiin salasanoihin?

Lähteinä on käytetty pääasiassa JYKDOK-tietokannasta löytyviä vertaisarvioituja tieteellisiä julkaisuja, joiden julkaisukanavat ovat julkaisufoorumin mukaan pääsääntöisesti vähintään tasoa 1 ja niitä etsittäessä on käytetty muun muassa seuraavia hakusanoja, sekä niiden yhdistelmiä: *FIDO in user authentication, mfa in user authentication, usability in user authentication, password cracking* ja *security in user authentication*. Keskeisimpien artikkelien kohdalla haettiin myös uusia lähteitä lähdeviitteiden kautta. Lisäksi käsitteiden määrittelyyn on valittu luotettavalta vaikuttavia verkkosivuja, kuten FIDO-teknologian kehittäneen Fidoalliancen kotisivut, tukemaan tieteellisiä artikkeleita.

Tutkielman ensimmäisessä luvussa käsitellään käyttäjän tunnistuksen turvallisuuden ja käytettävyyden kriteereitä. Toisessa luvussa vertaillaan monivaiheisen tunnistautumisen eri menetelmiä sekä FIDO-teknologiaa niiden turvallisuuden ja käytettävyyden näkökulmista, ja lopuksi tehdään yhteenveto tutkielmassa tehdyistä havainnoista.

2 TUNNISTUSMENETELMIEN ARVIOINNIN MITTARIT

Käyttäjän tunnistukseen verkossa käytettäviä menetelmiä voidaan arvioida niiden teknisen turvallisuuden, sekä niiden koetun käytettävyyden näkökulmista. Käyttäjän tunnistuksessa käytettyihin menetelmiin liittyy yleensä vähintään yksi seuraavista: tietotekijä, omistustekijä, tai biometrinen tekijä (Ali, Dida & Elikana Sam, 2021; Ometov ym., 2018). Yleisin käyttäjän tunnistamiseen käytetty menetelmä on käyttäjätunnus-tekstisalasana-yhdistelmä (Campbell ym., 2011; Sediyono ym., 2013), joka pohjautuu täysin tietotekijään, eli johonkin jonka vain käyttäjä itse tietää. Kyseinen tunnistautumismenetelmä on kuitenkin teknisen turvallisuutensa osalta täysin riippuvainen salasanan monimutkaisuudesta, sillä liian monimutkainen salasana voi olla liian vaikea muistaa ja toisaalta liian yksinkertainen on helppo arvata (Sediyono ym., 2013). Usein tämä johtaa käyttäjien kohdalla ratkaisuihin, jotka priorisoivat käytettävyyttä jopa turvallisuuden kustannuksella (Gartner, 2023a). Verkkorikolliset ovatkin aikojen saatossa kehittäneet erilaisia menetelmiä, joiden avulla he pystyvät murtamaan käyttäjien salasanoja, minkä vuoksi on alettu kehittää vaihtoehtoisia tunnistautumistapoja joko tekstipohjaisten salasanojen tilalle, tai niiden rinnalle.

Campbell tutkimusryhmineen (2011) totesivat tutkimuksessaan, että pelkästään salasanojen turvallisuuden vahvistamiseen tähtäävillä rajoituksilla ei saavuteta riittävää muutosta ihmisten käytöksessä suhteessa tekstipohjaisten salasanojen turvallisuuteen. Esimerkiksi asettamalla rajoituksia merkkijonon pituuteen tai käytettäviin merkkeihin käyttäjät päätyvät todennäköisesti edelleen kierrättämään samaa salasanapohjaa, jota muokataan vain marginaalisesti rajoitusten mukaiseksi (Campbell ym., 2011; Gartner, 2023a). Tässä luvussa tutustutaan käyttäjän tunnistuksen arvioinnin kriteereihin, jotka ovat menetelmien tekninen turvallisuus ja käytettävyys.

2.1 Käyttäjäntunnistuksen tekninen turvallisuus

Turvallisuus on yksi keskeinen osa käyttäjäntunnistusprosessia, ja sen voidaan katsoa sisältävän sekä itse tunnistautumismenetelmän teknisen turvallisuuden erilaisia hyökkäysmuotoja vastaan, että käyttäjien yksityisyyden suojan (Bonneau, Herley, van Oorschot & Stajano, 2012). Turvallinen tunnistautumismenetelmä tunnistaa luotettavasti käyttäjän oikeaksi, eikä päästä muita henkilöitä tai laitteita käsiksi käyttäjien tietoihin (Bonneau ym., 2012). Lisäksi turvallinen menetelmä suojaa käyttäjää tunnusten kalastelulta sekä muilta tunnetuilta internetin välityksellä toteutettavilta hyökkäysmenetelmiltä, joiden tarkoituksena on joko saada käyttäjätunnukset varastettua, tai päästä käsiksi toisten ihmisten resursseihin verkkopalveluissa (Bonneau ym., 2012).

Tunnistusmenetelmien tekninen turvallisuus pohjautuu sekä salasanojen tai suojausavainten salaukseen, että käytettyjen salausalgoritmien kestävyyteen murtoyrityksiä vastaan (Chakravarthy, Hauser & Bakken, 2010). Yksikään tunnistautumismenetelmä ei kuitenkaan ole ikuisesti turvallinen, sillä tietokoneiden laskentateho kasvaa jatkuvasti, jolloin tiettyyn aikaan turvalliseksi luotu menetelmä ei välttämättä olekaan enää riittävä suojaamaan käyttäjiä tulevaisuudessa (Chakravarthy ym., 2010).

Etenkin verkkopalveluissa käyttäjät tunnistetaan useimmiten kirjautumisprosessilla, jossa käyttäjät syöttävät käyttäjätunnuksen ja salasanan päästäkseen käsiksi omiin resursseihinsa kyseisessä palvelussa (Bonneau ym., 2012). Turvallisuus kiteytyy usein juuri kirjautumisen yhteydessä käytettävän salasanan kompleksisuuteen, vaikkakin hyökkääjien on mahdollista saada salasanat haltuunsa muun muassa kalastelun tai näppäilytietoja tallentavien ohjelmien avulla (Bonneau ym., 2012; Fidoalliance, 2024; Verizon, 2022). Salasanojen turvallisuus on sitä parempi, mitä suurempi on niiden entropia. Toisin sanoen salasanat ovat sitä turvallisempia, mitä enemmän ne sisältävät informaatiota eli esimerkiksi kirjaimia, numeroita tai kuvapisteitä ja mitä satunnaisempia ne ovat (Wiedenbeck, Waters, Birget, Brodskiy & Memon, 2005).

Tekstipohjaisten salasanojen kohdalla tämä tarkoittaa kärjistetysti valitun merkkijonon pituutta. Pitkät ja satunnaiset tekstipohjaiset salasanat aiheuttavat käyttäjille kuitenkin haasteita, sillä ne ovat hankalia muistaa (Biddle ym., 2012; Wiedenbeck ym., 2005). Tästä syystä käyttäjät esimerkiksi valitsevatkin lyhyempiä salasanoja, tai käyttävät samaa salasanaa useammilla käyttäjätunnuksilla (Grawemeyer & Johnson, 2011), mikä mahdollistaa useamman käyttäjätunnuksen altistumisen yhdenkin onnistuneen tietomurron myötä.

Bonneau ja hänen työtoverinsa (2012) havaitsivat salasanojen korvaajiksi ehdotettuja menetelmiä käsittelevässä tutkimuksessaan, että useat kirjautumisvaihtoehdot ovat tekstipohjaisia salasanoja turvallisempia. Perusteena havainnolleen he esittivät väitteen, jonka mukaan valtaosa muiden vaihtoehtojen kehittäjistä priorisoivat menetelmiensä turvallisuutta käytettävyyden kustannuksella. Juuri heikkoa käytettävyyttä voidaan pitää

monen turvallisemman tunnistautumistavan kohdalla suurimpana syynä sille, että tekstipohjaisia salasanoja ei ole laajassa mittakaavassa onnistuttu syrjäyttämään millään turvallisemmalla menetelmällä.

2.2 Tunnistautumismenetelmän käytettävyys

Käytettävyys on turvallisuuden ohella toinen merkittävä tekijä tunnistautumisprosessissa. Sen voidaan katsoa sisältävän käyttäjien kokeman vaivan tunnistautumiseen vaaditun työn suhteen, sekä tunnistautumismenetelmän toimintavalmiuden (Bonneau ym., 2012).

Etenkin käyttäjien kokema vaiva vaikuttaa merkittäviltä osin turvallisuuskäyttäytymiseen, kuten riittävän vahvojen tekstipohjaisten salasanojen luomiseen (Gartner, 2023a ; Gunson, Marshall, Morton & Jack, 2011). Tekstipohjaisten salasanojen käytettävyys koetaan yleisesti parhaaksi (Bonneau ym., 2012; Zimmerman & Gerber, 2020), vaikka turvallisuusperiaatteiden mukaisesti jokaiseen verkkopalveluun pitäisi luoda uusi salasana. Tämä aiheuttaa käyttäjille kognitiivista kuormaa, minkä seurauksena käyttäjät todellisuudessa kierrättävät salasanojaan ja näin ollen jopa tietoisesti kasvattavat tietoturvariskejä sekä itselleen, että organisaatioille (Gartner, 2023a).

Toisaalta Gartnerin (2023a) mukaan noin puolet työntekijöistä kokee, että kyberturvan ohjeistus on esimerkiksi vaikeaa ymmärtää, joustamatonta, tai liian vaikeaa muistaa. Samassa tutkimuksessa noin puolet henkilöistä, jotka tunnustavat käyttävänsä heikkoja salasanoja perustelevat toimintaansa prosessin nopeuttamisella tai käytettävyyden parantumisella, ja näistä henkilöistä yli 90 % tiedostavat toimintansa kasvattavan kyberturvallisuusriskiä (Gartner, 2023a). Vaikuttaisi siis olevan niin, että käytettävyys on turvallisuutta merkittävämpi ihmisten käyttäytymiseen vaikuttavista tekijöistä ainakin turvallisuudeltaan eikriittisiksi koettujen prosessien yhteydessä. Gartnerin tutkimuksessa ei otettu kantaa prosessien turvallisuuskriittisyyteen, mutta voitaneen olettaa, että tulokset ovat jossain määrin yleistettävissä yleiseen asenteeseen työpaikoilla.

Kognitiivisen kuorman vähentämiseksi on kehitetty menetelmiä, jotka pohjautuvat omistustekijään tietotekijän sijaan. Tämä tarkoittaa sitä, että salasanan muistamisen sijaan tunnistautumiseen käytetään jotakin laitetta, kuten älypuhelinta tai suojausavainta (Bonneau ym., 2012; Lyastani, Schilling, Neumayr, Backes, & Bugiel, 2020), joka vain käyttäjällä itsellään on. Omistustekijään pohjautuvan tunnistautumisen lähtökohtana on minimoida muun muassa tunnusten kalastelun mahdollisuus internetin yli (Bonneau ym., 2012; Fidoalliance, 2024). Tunnistautumiseen erikseen käytettävät laitteet ja niiden muistamiseen liittyvät negatiiviset kokemukset voivat toisaalta heikentää käytettävyyskokemusta, ja hidastaa kyseisten teknologioiden yleistymistä niiden tuomista eduista huolimatta (Bonneau ym., 2012; Lyastani ym., 2020). Käytettävyyden ja turvallisuuden suhteen on siis tärkeää löytää kompromisseja, joissa käyttäjien kokema vaiva ei kasva liian suureksi, mutta tunnistautumisprosessi pysyy edelleen aidosti turvallisena.

Menetelmän toimintavalmiudella tarkoitetaan sen valmiutta tulla yleisempään käyttöön. Toimintavalmiuteen liittyy osaltaan myös sen tekninen turvallisuus, sillä uusien teknologioiden kohdalla harvoin kyetään ottamaan huomioon kaikkia mahdollisia keinoja joko huijata järjestelmää tai kiertää sen turvallisuusominaisuuksia (Bonneau ym., 2012). Joistakin menetelmistä on esimerkiksi saatu tutkimuksissa lupaavia tuloksia tekstipohjaisten salasanojen korvaajaksi (Wiedenbeck ym., 2005), mutta ne on joko myöhemmissä tutkimuksissa osoitettu liian haavoittuvaisiksi (Zhu, Yan, Gunabo, Maowei & Ning, 2014), tai niiden koetaan vaativan liian isoja muutoksia olemassa oleviin tunnistusmenetelmiin esimerkiksi palveluntarjoajien puolelta (Bonneau ym., 2012). Käytettävyyden voidaankin näin ollen katsoa koskevan sekä loppukäyttäjiä, että palveluntarjoajia omilla tahoillaan. Näistä kahdesta vaihtoehdosta kuitenkin loppukäyttäjien kokemuksella vaikuttaisi olevan suurempi merkitys uusien menetelmien käyttöönotolle etenkin isommassa mittakaavassa.

3 TUNNISTAUTUMISMENETELMÄT

Tässä luvussa käydään läpi monivaiheisen tunnistautumisen menetelmistä kertakäyttöiset salasanat, biometrinen tunnistautuminen ja graafiset salasanat, sekä salasanaton FIDO-teknologia niiden turvallisuuden ja käytettävyyden näkökulmasta.

Monivaiheisessa tunnistautumisessa käyttäjä tunnistetaan oikeaksi käyttäen kahta tai useampaa tunnistautumistekijää (TechTarget, 2023a). Usein tämä tarkoittaa tietotekijän yhdistämistä ainakin omistustekijän kanssa, käyttäen esimerkiksi tekstiviestiä tai mobiililaitteelle ladattavaa erillistä tunnistautumissovellusta, johon on yleensä yhdistetty myös käyttäjätunnusten ja salasanojen hallinta. Monivaiheinen tunnistautuminen on laajasti käytössä esimerkiksi yliopistoissa ja isommissa kaupallisissa yrityksissä, koska sen koetaan parantavan tunnistautumisprosessin tietoturvaa ja olevan käytettävyydeltään hyväksyttävällä tasolla.

Salasanattomalla kirjautumisella tarkoitetaan tässä yhteydessä tunnistautumisvaihtoehtoa, jossa käyttäjän ei tarvitse turvautua tietotekijään. Toisin sanoen palveluihin kirjauduttaessa käyttäjätunnuksen yhteydessä käytetään laitteistopohjaista tunnistautumismenetelmää salasanan sijaan (Ali ym., 2021). Näin käyttäjän tunnistus pohjautuu omistustekjiään tietotekijän sijaan, eikä käyttäjän välttämättä tarvitse muistaa salasanoja tai turvakysymyksiä.

Yhteenvetona voidaan lyhyesti todeta kaikkien vertailtujen menetelmien omaavan sekä vahvuuksia, että heikkouksia. Näitä havaintoja on koottu yhteen taulukossa 1.

TAULUKKO 1 Yhteenveto vertailluista menetelmistä

Tunnistautumismenetelmä	**Vahvuudet**	**Heikkoudet**
Tekstipohjaiset salasanat	- Hyvä käytettävyys käyttäjien näkökulmasta (Sediyono ym., 2013)	- Suuri kognitiivinen kuorma johuten salasanojen suuresta

	- Laajasti käytössä eri verkkopalveluissa (Campbell ym., 2011) - Toimintavalmis (Campbell ym., 2011)	määrästä (Campbell ym., 2011) - Arvattavissa/Kalastelt avissa (Sediyono ym., 2013)
Kertakäyttöiset salasanat	- Lisää tunnistautumisprose ssin turvallisuutta tuomalla tietotekijän rinnalle omistustekijän (Sediyono ym., 2013) - Kohtalainen käytettävyys (Binbeshr ym., 2023) - Toimintavalmis (Reyes ym., 2018)	- Lisätty vaihe tunnistautumisessa koetaan usein heikentyneenä käytettävyytenä (Gunson ym., 2011) - Kalasteltavissa (Reyes ym., 2018)
Biometrinen tunnistautuminen	- Lisää tunnistautumisprose ssin turvallisuutta edelleen tuomalla mukaan biometrisen tekijän edellä mainittujen lisäksi (Harikrishnan ym., 2024) - Kohtalainen käytettävyys (Harikrishnan ym., 2024) - Toimintavalmis (Ometov ym., 2018)	- Lisätty vaihe tunnistautumisessa koetaan usein heikentyneenä käytettävyytenä (Gunson ym., 2011) - Käyttäjän yksityisyydensuoja voi vaarantua (Acar ym., 2019)
Graafiset salasanat	- Käyttäjät muistavat monimutkaisempia salasanoja graafisina kuin tekstipohjaisina (Wiedenbeck ym., 2005)	- Turvallisuushuolia aiheuttavat kuvissa ilmenevät hotspotit (Wiedenbeck ym., 2005) - Ei vielä toimintavalmis (Van Oorschot & Thorpe, 2011)
FIDO-teknologia	- Kalastelun kestävä tunnistautumismene telmä (Fidoalliance, 2024 ; Lyastani ym., 2020) - Pieni kognitiivinen kuorma verrattuna tekstipohjaisiin salasanoihin (Lyastani ym., 2020) - Laitteistoon pohjautuva	- Epätietoisuus menetelmän toimintaperiaatteesta (Lyastani ym., 2020) - Suojausavainten fyysinen kestävyys toistaiseksi tuntematon - Vaatii vaihtoehtoisen kirjautumismenetelmä n siltä varalta että suojausavain hajoaa tai katoaa.

	tunnistautuminen mahdollista (Fidoalliance, 2024)	- Ei vielä toimintavalmis (Lyastani ym., 2020)

3.1 Kertakäyttöiset salasanat

Kertakäyttöinen salasana on salasana, joka on voimassa vain yhden kirjautumisen tai suorituksen yhteydessä (Sediyono ym., 2013). Niitä luodaan todentamisprosessin yhteydessä satunnaisesti, ja pääasiassa kolmella tavalla: aikasynkronisaatiolla todennuspalvelimen ja todentautuvan käyttäjän välillä, käyttämällä matemaattisia algoritmeja luomaan uusi salasana edellisen pohjalta, tai luomalla salasana johonkin haasteeseen, esimerkiksi palvelimen valitsemaan satunnaiseen numeroon perustuen (Sediyono ym., 2013). Yksi yleisimmistä edellä mainituista todennuskeinoista on SMS-pohjaiset kertakäyttöiset salasanat, jotka perustuvat juuri aikasynkronisaatioon (Reyes, Festijo & Medina, 2018). Aikasynkronisaatio tarkoittaa sitä, että kertakäyttöinen salasana luodaan sillä ajanhetkellä, jolloin käyttäjä yrittää tunnistautua johonkin palveluun, jossa on käytössä kyseinen monivaiheisen tunnistautumisen muoto (Reyes ym., 2018). Kertakäyttöiset salasanat ovat voimassa vain lyhyen ajan niiden luomisesta, jolloin niiden murtaminen on käytännössä mahdotonta johtuen nykytietokoneiden laskentakapasiteetin rajoituksista (Sediyono ym., 2013).

Kertakäyttöiset salasanat parantavat todennusprosessin turvallisuutta muun muassa siten, että ne eivät ole tekstipohjaisten salasanojen tapaan haavoittuvaisia sanakirja-, tai toistohyökkäyksille (Sediyono ym., 2013). Toistohyökkäyksessä hyökkääjä on esimerkiksi tallentanut käyttäjän syötettä ja yrittää kirjautua itse käyttäen tallentamiaan tietoja (Naha, Teixeira, Ahlén & Dey, 2023). Sanakirjahyökkäyksessä puolestaan hyökkääjät kokeilevat sanoja eri sanakirjoista yrittäen päästä sisään käyttäjän resursseihin. Toisaalta jotkin kertakäyttöiset salasanat ovat edelleen alttiita muun muassa kalastelu-, ja salakuunteluhyökkäyksille (Reyes ym., 2018), joten tietojen paremmalle salaukselle on edelleen tarvetta.

Reyes ja hänen tutkimusryhmänsä (2018) esittelevät tutkimuksessaan parannellun version Blowfish-algoritmista, jossa bittimäärä on laajennettu 128 bittiin, tarkoituksenaan parantaa kertakäyttösalasanojen turvallisuutta. Alkuperäinen Blowfish-algoritmi on yleiskäyttöinen symmetrisen avaimen salausalgoritmi, jota ei ole patentoitu tai muuten salattu esimerkiksi valtioiden toimesta. Nostamalla bittimäärää 128:aan, havaittiin jonkin verran parannuksia yleisimpiä salauksen purkamiseen käytettyjä hyökkäysmenetelmiä vastaan (Reyes ym., 2018). Toisin sanoen kertakäyttöisten salasanojen suojausta voidaan edelleen parantaa suhteellisen helposti käyttämällä edistyneitä salaustekniikoita niiden salaamiseen hyökkääjiltä.

Kertakäyttöiset salasanat koetaan käytettävyydeltään yleisesti hyvinä, mutta käytettävyyteen vaikuttaa muun muassa syöttökierrosten määrä

yksittäisen kirjautumisen yhteydessä, syötettävien salasanojen pituus sekä kuinka kriittiseksi tunnistusprosessin turvallisuus koetaan käsiteltävien tietojen kannalta (Binbeshr, Por, Kiyah, Zaidan & Imam, 2023). Binbeshr kollegoineen havaitsivat tutkimuksessaan, että mitä kriittisemmästä prosessista on kyse, sitä valmiimpia käyttäjät ovat tinkimään käytettävyydestä turvallisuuden kustannuksella.

3.2 Biometrinen tunnistautuminen

Biometrinen tunnistautuminen tarkoittaa käyttäjän todentamista yksilöllisiin biologisiin ominaisuuksiin, kuten sormenjälkeen, kasvonpiirteisiin, tai käyttäytymismalleihin perustuen (TechTarget, 2023b). Biometrisen tunnistautumisen käyttö vaatii laitteen, jossa on jokin sensori biometristen ominaisuuksien skannaamiseksi. Tämä tarkoittaa nykypäivänä useimmiten älypuhelinta, joissa on lähes poikkeuksetta sisäänrakennettuna jonkinlainen biometrinen tunnistautumisominaisuus, kuten kasvojen-, tai sormenjälkitunnistus. Laite lukee halutun biometrisen ominaisuuden, ja joko tallentaa sen suoraan muistiinsa, tai laskee siitä tiivisteen, jota käytetään käyttäjän tunnistamiseen kirjautumisprosessissa. Yleisimmät biometrisen todentamisen menetelmät ovat kasvojen-, äänen-, ja sormenjälkitunnistus (Harikrishnan, Kumar, Jospeh & Nair, 2024; TechTarget, 2023a). Sormenjälkitunnistuksella saavutetaan hyvä luotettavuuden ja nopeuden taso, mutta siihen liittyy vielä jonkin verran haavoittuvuuksia (Harikrishnan ym., 2024). Tästäkin huolimatta sormenjälkitunnistuksesta on tullut vallitseva biometrisen tunnistamisen menetelmä etenkin monivaiheisen tunnistautumisen alkuaikoina, johtuen siitä, että teknologia on laajalti käytössä älypuhelimissa (Ometov ym., 2018), jotka usein toimivat omistustekijänä osana monivaiheista tunnistautumista.

Biometristen ominaisuuksien käytön voidaan sanoa parantavan käyttäjän tunnistuksen luotettavuutta merkittävästi, sillä niitä on käytännössä mahdotonta arvata. Toisaalta mikäli biometrisiä tietoja tallennetaan suoraan verkkopalveluiden tietokantoihin, herää kysymys käyttäjien yksityisyyden suojasta (Acar, Liu, Beyah, Akkaya & Uluagac, 2019; Biddle ym., 2012). Ihmisten biometriset ominaisuudet ovat luonteeltaan pysyviä (Harikrishnan ym., 2024), joten mikäli niitä tallennetaan tietokantoihin suojaamattomina, ja tietokanta joutuu tietomurron kohteeksi, ovat käyttäjien biometriset tiedot menetetty pysyvästi. Tämän vuoksi olisikin syytä käsitellä käyttäjien biometrisiä tietoja siten, että niistä muodostettaisiin salattu tiiviste (Harikrishnan ym., 2024), kuten verkkoliikenteelle ja tekstipohjaisille salasanoille tehdään (The Interactive Material, ei pvm.). Tiivisteiden etuna on erityisesti se, että niitä voidaan muodostaa vaihtelevilla menetelmillä, jolloin yhden tiivisteen murtaminen ei välttämättä paljasta kriittistä tietoa käyttäjästä. Näin ollen biometristen ominaisuuksien käytöstä tulisi turvallisempaa myös mahdollinen tietojen menetys huomioon ottaen, koska olemassa olevien salausmenetelmien avulla luodut tiivisteet ovat lisäksi käytännössä mahdotonta purkaa järkevässä ajassa (The Interactive Material, ei pvm.).

Käytettävyydeltään biometrinen tunnistautuminen koetaan yleensä hyväksi (Zimmermann & Gerber, 2020). Tutkimuksessaan Zimmermann ja Gerber havaitsivat esimerkiksi sormenjälkitunnistuksen olevan käyttäjien mielestä lähes tekstipohjaisen salasanan tasolla käytettävyydeltään, kun mitattiin muun muassa koettua vaivaa suhteessa turvallisuushyötyyn. Samaan aikaan tekstisalasanojen käyttö koettiin tutkimuksessa turvallisuudeltaan keskikastiin tutkittujen tunnistautumistapojen keskuudessa (Zimmermann & Gerber, 2020), mikä osaltaan tukee Gartnerin (2023a) analyysissä tehtyjä havaintoja siitä, että käyttäjät tuntuisivat olevan tietoisia salasanojen potentiaalisista heikkouksista suhteessa muihin tunnistautumismenetelmiin. Samaan aikaan salasanat kuitenkin vaikuttavat edelleen olevan käyttäjien mielestä riittävä suojaus käyttäjän tunnistuksessa.

3.3 Graafiset salasanat

Graafisia salasanoja on tutkittu jopa tekstipohjaisten salasanojen korvaajana vuodesta 1999 alkaen, ja niiden toiminta perustuu tekstipohjaisten salasanojen tapaan tietotekijään (Biddle ym., 2012). Toisin sanoen alfanumeeriset tekstisalasanat korvattaisiin kuvapohjaisella tiedolla käyttäjän tunnistamiseksi (Martinez-Diaz, Fierrez & Galbally, 2016).

Graafisen salasanan mallit, joissa käyttäjät piirtävät itse kuvan, joka toimii salasanana voivat aiheuttaa ongelmia (Martinez-Diaz ym., 2016). Käyttäjillä saattaa esimerkiksi olla vaikeuksia toistaa luomansa salasanapiirros riittävällä tarkkuudella, jotta testijärjestelmä olisi tunnistanut käyttäjän oikein (Martinez-Diaz ym., 2016). Konseptina itse piirretyt graafiset salasanat ovat siis parhaimmillaan turvallisuudeltaan hyvällä tasolla, mutta samaan aikaan niiden replikoiminen riittävällä tarkkuudella voi tuottaa käyttäjille haasteita.

Wiedenbeck ja hänen kollegansa (2005) tutkivat graafista salasanaa nimeltään PassPoints, jonka toiminta perustuu siihen, että satunnaisesta kuvasta klikataan haluamiaan pisteitä, joista muodostuu käyttäjälle salasana. Kyseinen menetelmä osoittautui käytettävyydeltään ja oikeellisuudeltaan lähes alfanumeerisia salasanoja vastaavaksi jo verrattain lyhyen opettelujakson jälkeen (Wiedenbeck ym., 2005). Tutkimuksessa käyttäjien kokemuksiin vaikutti todennäköisesti se, että tutkittu menetelmä oli testiryhmäläisille täysin uusi, eikä sitä käytetty tutkimuksen aikana säännöllisesti (Wiedenbeck ym., 2005). Toisaalta kyseinen havainto osaltaan lisää uskoa kyseisen menetelmän käytettävyydestä, mikäli sen käyttö yleistyisi.

Turvallisuudeltaan graafiset salasanat yleisesti eivät vaikuttaisi olevan merkittävästi parempia kuin alfanumeeriset salasanat huolimatta siitä, millainen menetelmä niiden luomiseen valitaan. Itse piirrettyjen graafisten salasanojen kohdalla väärennökset luovat pääasiallisen turvallisuusuhan salasanojen murtamiselle (Martinez-Diaz ym., 2016). Wiedenbeckin ja kollegoiden (2005) mallissa tutkijat puolestaan nimesivät menetelmän turvallisuushuoleksi niin sanotut hotspotit. Hotspoteilla tarkoitetaan yksityiskohtia, joihin käyttäjien huomio

todennäköisimmin kiinnittyy kuvissa ja tästä syystä todennäköisimmin päätyvät käyttäjien salasanoihin graafisissa menetelmissä (Van Oorschot & Thorpe, 2011; Wiedenbeck ym., 2005).

Van Oorschot ja Thorpe (2011) vahvistivat tutkimuksessaan hotspottien olevan merkittävä turvallisuusuhka graafisille salasanoille, ja havaitsivat joidenkin kuvien kohdalla riskin olevan erityisen suuri. Tutkimuksessa onnistuttiin toisaalta arvaamaan käyttäjien salasanoja myös sellaisista kuvista, joiden oli muissa tutkimuksissa väitetty olevan vähemmän alttiita hotspoteille (Van Oorschot & Thorpe, 2011). Graafiset salasanat vaikuttaisivat siis olevan alfanumeeristen salasanojen tapaan alttiita ainakin väsytyshyökkäyksille, minkä vuoksi ne todennäköisesti eivät ole yleistyneet hyväksi koetusta käytettävyydestään huolimatta.

3.4 FIDO-teknologia

Tässä alaluvussa tutustutaan Fidoalliancen kehittämään salasanattomaan FIDO (Fast Identity Online) -teknologian turvallisuuteen ja käytettävyyteen. Se voidaan nähdä tekstipohjaisen salasanojen potentiaalisimpana syrjäyttäjänä erityisesti turvallisuutensa ja käytettävyytensä vuoksi (Lyastani ym., 2020). FIDO-teknologian tarkoitus on kasvattaa käyttäjän tunnistuksen turvallisuutta ja luotettavuutta, sekä poistaa käyttäjiltä tekstipohjaisten salasanojen muistamiseen liittyvä kognitiivinen kuorma. Fidoalliance on lisäksi julkaissut kolme vaihtoehtoisia tapoja käyttää FIDO-teknologiaa tunnistautumiseen, tarjotakseen käyttäjille ja palveluntarjoajille lisää vaihtoehtoja sen käyttöönottoon. Nämä ovat FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF) ja Client to Authenticator Protocols (CTAP), jotka yhdessä tunnetaan termillä FIDO2 (Fidoalliance, 2024). Näiden vaihtoehtoisten menetelmien on tarkoitus madaltaa salasanattoman kirjautumisen käyttöönottokynnystä, mutta tässä tutkielmassa keskitytään FIDO-teknologian perusperiaatteisiin.

FIDO-teknologia mahdollistaa käyttäjien salasanattoman tunnistautumisen käyttäen julkisen avaimen salausmenetelmää (Fidoalliance, 2024). Julkisen avaimen salausmenetelmässä tieto salataan julkisella salausavaimella, ja puretaan yksityisellä avaimella, jotka ovat molemmilla tiedonvaihtoon osallistuvilla osapuolilla omansa (Fidoalliance, 2024). Erona perinteisempään salasanan avulla tapahtuvaan tunnistautumiseen on se, että FIDO-teknologiaa käytettäessä palvelin vastaanottaa käyttäjän rekisteröimän julkisen avaimen salasanasta muodostetun tiivisteen sijaan, ja tätä avainta verrataan palvelimen omaan yksityiseen avaimeen joka on yhdistetty kyseiseen käyttäjätunnukseen (Fidoalliance, 2024). Lisäksi käyttäjän kannalta kriittistä informaatiota, kuten biometrisiä tietoja ei tallenneta palveluntarjoajien palvelimille, koska tunnistautuminen pohjautuu mainittuihin avaimiin (Fidoalliance, 2024). Arkielämän vastaava esimerkki on kotiovi ja kotiavain. Kotiovi vastaa salauksessa käytettävää julkista avainta, jonka kaikki näkevät. Kotiavain puolestaan on yksityinen avain, joka avaa vain tietyn oven. Löytämällä tai

varastamalla pelkän avaimen on käytännössä mahdotonta järkevässä ajassa löytää oikea ovi, johon kyseinen avain käy.

FIDO- teknologian turvallisuus perustuu siihen, että kirjautumistietoja ei voi ryöstää verkon välityksellä (Fidoalliance, 2024). Salasanasta muodostettu tiiviste tallennetaan perinteisessä kirjautumismallissa verkkosivun palvelimelle, jolloin on olemassa mahdollisuus sille, että kuka tahansa voi päästä siihen käsiksi murtautumalla kyseiselle palvelimelle. Pelkästään julkisen avaimen avulla ei siis voida saada kirjautumisoikeuksia keneltäkään, vaan tunnistautuminen vaatii myös yksityiset avaimet, jotka ovat tallessa käyttäjän laitteella sekä verkkopalvelimella (Fidoalliance, 2024).

FIDO-teknologian turvallisuutta voi etenkin menetelmän mahdollisesti yleistyessä heikentää suojausavainten tuotantoketjuun käsiksi pääsevät rikolliset (Schink, Wagner, Unterstein & Heyszl, 2021). Käyttäjillä ei ole yleensä kykyä tai edes ymmärrystä tutkia fyysisten suojausavainten sisältöä tai toimintaa tarkemmin (Schink ym., 2021). Näin ollen suojausavainten valmistajille olisi saatava esimerkiksi jonkinlainen luotettava sertifikointijärjestelmä joka olisi lisäksi saatava käyttäjien laajaan tietoisuuteen, jotta kyseisen uhan vaikutukset saataisiin minimoitua opettamalla käyttäjät luottamaan vain sertifioituihin suojausavaimiin.

FIDO-teknologian käytettävyyden kokemukseen vaikuttavat etenkin menetelmän tuntemattomuus, sekä se, että se poikkeaa käyttäjille näkyvältä toiminnallisuudeltaan suuresti perinteisistä salasanoista. Siitä huolimatta FIDO-teknologia koetaan käytettävyydeltään verrattain hyvänä ainkin rajallisen otannan laboratoriotutkimuksissa (Lyastani ym., 2020; Zimmermann & Gerber, 2020). Isoimpana etuna kyseisellä menetelmällä tuntuisi olevan se, että suojausavaimen käytön myötä käyttäjien kognitiivinen kuorma pienenee merkittävästi verrattuna tekstipohjaisiin salasanoihin, sillä ainoa muistettava asia on suojausavain itsessään (Lyastani ym., 2020).

Toisaalta käytettävyyden kokemusta heikentää pelko esimerkiksi suojausavaimen kadottamisesta ja sitä myötä menetettyjen käyttäjätilien palautusprosessin epäselvistä tai jopa vaillinnaisista kuvauksista (Lyastani ym., 2020). Vaikka perinteisten tekstipohjaisten salasanojen resetoinneista aiheutuu organisaatioille vuosittain myös päänvaivaa sekä kustannuskia (Gartner, 2023b), on salasanojen resetoinnille olemassa vakiintuneet menetelmät jotka ovat käyttäjille tuttuja. Nämä vakiintuneet käytännöt luovat turvallisuuden tuntua mahdollisia poikkeustilanteita tarkasteltaessa.

Yksi FIDO-teknologian käyttöön liittyvä potentiaalinen ongelma johon ei vielä löydy tutkimusaineistoa voisi olla suojausavainten fyysinen kestävyys. Kyseinen ominaisuus on rinnastettavissa suojausavaimen kadottamiseen, sillä avaimen hajotessa on käyttäjän tunnistus käytännössä mahdotonta ilman vaihtoehtoista menetelmää. FIDO-teknologian toimintaperiaate on lisäksi yleisellä tasolla käyttäjille verrattain tuntematon (Lyastani ym., 2020). FIDO-teknologia ei siis ole vielä toimintavalmiudeltaan riittävällä tasolla, jotta siitä tulisi vallitseva menetelmä käyttäjän tunnistuksessa (Gartner, 2023b).

4 YHTEENVETO

Tässä tutkielmassa selvitettiin kirjallisuuskatsauksen avulla muita kuin tekstipohjaisiin salasanoihin pohjautuvia käyttäjän tunnistukseen käytettäviä menetelmiä niiden turvallisuuden ja käytettävyyden näkökulmista. Tutkielmassa keskityttiin turvallisuuden kannalta pääasiassa tarkasteltujen menetelmien teknisiin toteutuksiin, sekä osin niiden tarjoamaan yksityisyyden suojaan, sillä käyttäjät voivat toimillaan mitätöidä käytännössä minkä tahansa menetelmän turvallisuuden. Käytettävyys puolestaan jakautui käyttäjien kokemaan vaivaan tunnistautumisprosessissa, sekä kunkin menetelmän toimintavalmiuteen.

Tutkielmassa havaittiin, että tarkastellut menetelmät tarjoavat tekstipohjaisten salasanojen tunnettujen ongelmien ratkaisuiksi hyvinkin erilaisia teknisiä ratkaisuja. Nykyisistä ongelmista isoimpana erottui tekstipohjaisten salasanojen suuren lukumäärän tuoma kognitiivinen kuorma, jonka seurauksena käyttäjät turvautuvat joko heikkoihin salasanoihin tai salasanojen kierrättämiseen. Tämä ongelma on pyritty ratkaisemaan joko lisäämällä tunnistautumisprosessiin tunnistautumisen kerroksia tietotekijän rinnalle, tai jopa poistamalla tietotekijä tunnistautumisprosessista kokonaan.

Käytettävyyden osalta tutkielmassa todetaan, että käyttäjien kokema vaiva tunnistautumisprosessin aikana on merkittävä tekijä uusien teknologioiden hyväksymisen kannalta. Tekstipohjaisten salasanojen etuna tuntuisi olevan se tosiasia, että ne ovat olleet käytössä jo hyvin pitkään, minkä vuoksi niiden toiminnallisuus on käyttäjille tuttu. Vaikka uusia menetelmiä tutkittaessa on havaittu käytettävyyden kannalta hyviäkin tuloksia käyttäjien palautteen perusteella, liittyy niihin joka tapauksessa jonkin verran huolta osin niiden tuntemattomuuden vuoksi.

Tutkielman tavoitteena oli kartoittaa käyttäjän tunnistuksessa jo käytössä olevia menetelmiä. Tarkasteluun pyrittiin valikoimaan menetelmiä, joiden toimintaperiaatteet sisältävät eri käyttäjän tunnistukseen liittyvät tekijät, jotta kyseisten tekijöiden turvallisuudesta ja käytettävyydestä saataisiin mahdollisimman kattava näkemys. Tutkielman tuloksista voidaan päätellä, että tekstipohjaisten salasanojen korvaajaksi on jo olemassa teknologioita tai

menetelmiä, jotka ovat turvallisuudeltaan niitä parempia, mutta useimmiten häviävät niille käytettävyydessä (Taulukko 1). Järjestelmien kehittäjien tulisi pyrkiä ottamaan käytettävyys paremmin huomioon turvallisempia järjestelmiä luotaessa, jotta tekstipohjaisista salasanoista voitaisiin tulevaisuudessa luopua. Organisaatioiden tietoturva-asiantuntijoiden puolestaan tulisi ottaa kyberturvan ohjeistuksessa huomioon sen ymmärrettävyys. Lisäksi organisaatioiden yleistä tietoturvakulttuuria luotaessa on muistettava perustella etenkin käytettävyyttä heikentävät ratkaisut riittävällä tarkkuudella, jotta käyttäjät hyväksyisivät turvallisempia toimintatapoja helpommin.

Tutkielmassa pyrittiin hyödyntämään vain luotettavalta vaikuttavia ja viimeaikaisia lähteitä, mutta teknologian nopeasta kehityksestä johtuen se sisältää joitakin rajoitteita. Ottaen huomioon muun muassa tekoälyn viimeaikaisen kehityksen, voivat etenkin valittujen menetelmien turvallisuuteen liittyvät tutkimustulokset olla joko osittain tai kokonaan vanhentuneita, johtuen muun muassa tekoälyn tuomista automatisointimahdollisuuksista. Lisäksi osa tarkastelluista menetelmistä on tullut laajempaan käyttöön vasta viime vuosien aikana, jolloin niistä ei välttämättä ole saatavilla yhtä paljon tutkimusaineistoa kuin pidempään käytössä olleilla. Tarkasteltaessa käyttäjien kokemuksia eri menetelmien käytettävyydestä tulee muistaa myös se, että ihmiset saattavat joko vähätellä tai kärjistää mielipiteitään käytettävistä menetelmistä ja että muutosjohtamisen merkitystä ei ainakaan tämän tutkielman lähteissä otettu huomioon.

Jatkotutkimusaiheina kannattaisi ottaa käyttäjän tunnistusmenetelmistä vertailuun mukaan myös tämän tutkielman rajauksen ulkopuolelle jäänyt Zero Trust, sekä FIDO-teknologiasta tutkimusta jossa fyysisenä suojausavaimena toimii älypuhelin. Älypuhelin suojausavaimena saattaa mahdollisesti madaltaa kynnystä kyseisen teknologian käyttöönottoon. Lisäksi muutosjohtamisen vaikutusta käyttäjien asenteisiin uusien tunnistautumismenetelmien käyttöönottovaiheessa olisi mielenkiintoista tutkia, ottaen huomioon sen, että käyttäjien kokemukset käytettävyydestä vaikuttaisivat olevan merkittävä tekijä uusien menetelmien hyväksynnässä. Koska tässä tutkielmassa ei otettu huomioon tekoälyn tuomia uhkia käyttäjän tunnistuksen turvallisuuteen, voisi olla mielenkiintoista kartoittaa niiden vaikutusta valittujen menetelmien turvallisuuteen.

LÄHTEET

Acar, A., Liu, W., Beyah, R., Akkaya, K. & Uluagac, A. (2019). A Privacy-preserving multifactor authentivation system. *Security and Privacy*, *2*(5). https://doi.org/10.1002/spy2.88

Ali, G., Dida, M.A. & Elikana Sam, A. (2021). A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications. *Future Internet*, *13*, 299. https://doi.org/10.3390/fi13120299

Alkhwaja, I., Albugami, M., Alkhwaja, A., Alghamdi, M., Abahussain, H., Alfawaz, F., Abdullah, A. & Min-Allah, N. (2023). Password cracking with brute force algorithm and dictionary attack using parallel programming. *Applied sciences, 13*(10), 5979. https://doi.org/10.3390/app13105979

Biddle, R., Chiasson, S. & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, *44*(4), 1-41

Binbeshr, F., Por, L. Y., Kiyah, M. L. Mat, Zaidan A. A. & Imam, M. (2023). Secure PIN-Entry Method Using One-Time PIN (OTP). *IEEE Access, 11*, 18121-18133 DOI: https://doi.org/10.1109/ACCESS.2023.3243114

Bonneau, J., Herley, C., van Oorschot, P., C. & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *IEEE Symposium on Security and Privacy*, 553-567

Campbell, J., Ma, W. & Kleeman, D. (2011). Impact of Restrictive Composition Policy on User Password Choices. *Behaviour & Information technology, 30*(3) 379-388 https://doi.org/10.1080/0144929X.2010.492876

Carrillo-Torres, D., Pérez-Díaz, J., Cantoral-Ceballos, J. &Vargas-Rosales, C. (2023). A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations. *Applied Sciences, 13*(3), 1374. https://doi.org/10.3390/app13031374

Chakravarthy, R., Hauser, C. & Bakken, D., E. (2010). Long-lived authentication protocols for process control systems. *International Journal of criticalt infrastructure protection, 3(3)*, 174-181.

Fidoalliance. (haettu 1.4.2024). *User Authentication Specifications overview.* https://fidoalliance.org/specifications/

Gartner a (28.8.2023). *Craft a Simple, Effective Password Policy*. https://ssofed.gartner.com/sp/startSSO.ping?PartnerIdpId=https://idp.jyu.fi/nidp/saml2/metadata&TargetResource=https%3A%2F%2Fwww.gartner.com%2Fdocument%2F4687299%3Fref%3Dd-linkShare

Gartner b (päivitetty viimerksi 22.2.2023). *Take 3 Steps Towards Passwordless Authentication*. https://www.gartner.com/document/4007059?ref=solrAll&refval=408196075&

Grawemeyer, B. & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256-267

Gunson, N., Marshall, D., Morton, H., Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers and security*, *30*(4), 208-220

Harikrishnan, D., Kumar, N., Jospeh, S. & Nair, K. K. (2024). Towards a Fast and secure fingerprint authentication system based on a novel encoding scheme. *International Journal of Electrical Engineering & Education, 61*(1) 100-112 http://dx.doi.org/10.1177/0020720919883803

Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020). Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. *IEEE Symposium on Security and Privacy.*

Martinez-Diaz, M., Fierrez, J. & Galbally, J. (2016). Graphical Password-Based User Authentication With Free-Form Doodles. *IEEE Transactions on human-machine systems*, *46*(4), 607-614.

Naha, A., Teixeira, A., Ahlén, A. & Dey, S. (2023). Sequential Detection of Replay Attacks. *IEEE Transactions on Automatic Control, 68*(3) 1941-1948.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. & Koycheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1.

Reyes, A., Festijo, E. & Medina, R. (2018). Securing One Time Password For Multi Factor Out-Of-Band Authentication through a 128-bit Blowfish Algorithm. *International Journal of Communication Networks and Information Security. 10*(1).

Schink, M., Wagner, A., Unterstein, F. & Heyszl, J. (2021). Security and Trust in Open Source Security Tokens. *IACR Transactions on Cryptographic Hardware and Embedded Systems, 3*, 176-201. https://doi.org/10.46586/tches.v2021.i3.176-201

Sediyono, E., Santoso, K. I. & Suhartono. (2013). Secure login by using One-time Password authentication based on MD5 Hash encrypted SMS. *International Conference on Advances in Computing, Communications and Informatics*, 1604-1608, DOI: 10.1109/ICACCI.2013.6637420.

TechTarget a (1.10.2023). *Definition of multi factor authentication.* https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

TechTarget b (1.8.2023). *Definition of biometric authentication.* https://www.techtarget.com/searchsecurity/definition/biometric-authentication

The Interactive Material. (ei pvm.). *Tietoverkot.* https://tim.jyu.fi/view/kurssit/tie/itkp104/2023-2024/teoria-1

Van Oorschot, P. C. & Thorpe, J. (2011). Exploiting Predictability in Click-Based Graphical Passwords. *Journal of Computer Security*, *19*(4), 669-702.

Verizon (2022). *Data Breach Investigations Report*. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

Wang, D., Zhang, X., Zhang, Z. & Wang, P. (2020). Understanding security failures of multi-factor authentication schemes for multi-server environments. *Computers & security 88*, 101619. https://doi.org/10.1016/j.cose.2019.101619

Wiedenbeck, S., Waters, J., Birget, J-C., Brodskiy, A. & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, *63*(1), 102-127. DOI: 10.1016/j.ijhcs.2005.04.010

Zhu, B. B., Yan, J., Gunabo, B., Maowei, Y. & Ning, X. (2014). Captcha as Graphical Password – A New Security Primitive Based on Hard AI Problems. *IEEE Transactions on Information Forensics And Security*, *9*(6), 891-904.

Zimmermann, V. & Gerber, N. (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.