Joel Tapio Lintunen

Tietoturvataivas vai -helvetti? Kirjallisuuskatsaus salasananhallintaohjelmissa havaituista tietoturva-aukoista

Tietotekniikan kandidaatintutkielma

30. huhtikuuta 2024

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Joel Tapio Lintunen

Yhteystiedot: joel.t.lintunen@student.jyu.fi

Työn nimi: Tietoturvataivas vai -helvetti? Kirjallisuuskatsaus salasananhallintaohjelmissa havaituista tietoturva-aukoista

Title in English: Information Security Heaven or Hell? A Literature Review of Vulnerabilities Found in Password Managers

Työ: Kandidaatintutkielma

Sivumäärä: 25+0

Tiivistelmä: Ihmiset vieroksuvat salasanaohjelmien periaatetta laittaa kaikki munat samaan koriin, koska tietoturvan pettäessä hyökkääjä pääsee käsiksi salasanaohjelman kaikkiin salasanoihin. Salasanojen uudelleenkäytöllä on samankaltaiset seuraukset, mutta salasanojen uudelleenkäyttö on silti yleistä. Salasanaohjelman käyttäjällä ei ole tarvetta uudelleenkäyttää salasanoja, koska uusia salasanoja pystyy generoimaan ja tallentamaan nopeasti. Toiset käyttäjät arvostavat nimenomaan näitä salasanaohjelmien käytännöllisiä puolia, kun taas toiset salasanaohjelmien tietoturvaominaisuuksia. Salasanaohjelman tietoturvaan vaikuttaa useampi asia, esimerkiksi salasanaohjelman ajoympäristö, salasanatietokannan salausalgoritmi ja lähdekoodin avoimuus. Tässä tutkielmassa kartoitetaan kolmentyyppisiä salasanaohjelmien haavoittuvuuksia: selaimessa tapahtuvia, salasanatietokantaan kohdistuvia ja käyttäjän laitteella ajettavaan haittaohjelmaan perustuvia haavoittuvuuksia. Haavoittuvuudet syntyvät johtuen erilaisista syistä, ja sen takia haavoittuvuuksien korjaamiseksi tehtävät asiat ovat tapauskohtaisia. Salasanaohjelmien ajoympäristöjä kehitetään jatkuvasti, joten myös salasanaohjelmien ylläpidon täytyy olla jatkuvaa, jotta salasanaohjelmat pysyvät tietoturvallisina.

Avainsanat: salasanaohjelma, salasananhallintaohjelma, salasanamanageri, tietoturvallisuus, ohjelmistoturvallisuus, kandidaatintutkielma

Abstract: People dislike password managers' idea to put all their eggs in one basket: if the security of a password manager fails, an attacker gets access to all the passwords stored in the password manager. The reuse of passwords has similar consequences, but password

reuse is commonplace nevertheless. Users of password managers don't have a need to reuse passwords because they can quickly generate and save new passwords. Some users especially appreciate these practical features, while others focus on the security features of password managers. There are multiple things that affect the information security of a password manager, for example the runtime environment, the encryption algorithm of the password database and the level of openness of the source code. This thesis surveys three types of password manager vulnerabilities: those that happen in web browsers, those that attack the password database and those that require an access to the host machine to run malware there. Because vulnerabilities are caused by different things, they also require different kinds of fixes. The runtime environments of password managers are being developed continuously, so password managers also require continuous maintenance to stay secure.

Keywords: password manager, password wallet, information security, software security, bachelor's thesis

Termiluettelo

Salasananhallintaohjelma	Ts. salasanaohjelma tai salasanamanageri. Ohjelma, jolla käyttäjä hallinnoi salasanatietokantaa.
Salasanapalvelu	Salasanaohjelma ohjelmistopalveluna, jossa salasanatietokanta on yleensä ulkoistettu palveluntarjoajan palvelimille.
Pääsalasana	Salasana, jolla salasanatietokanta avataan.
Vakiosalasana	Salasana tai salasanan runko, jota käyttäjä on taipuvainen uudelleenkäyttämään monessa palvelussa.
Salasanageneraattori	Ohjelma, joka luo uusia satunnaisia salasanoja.
Isäntäkone	Engl. *host computer* tai *host*. Tietokone, joka tarjoaa sovellusohjelmapalveluja käyttäjälleen tai verkkopalveluja muille verkon koneille.
Luonnollinen kieli	Kieli, jota ihmiset käyttävät sosiaalisessa kanssakäymisessä ja joka muuttuu ajan kuluessa kielen käytön seurauksena.
Selkokielinen teksti	Teksti, jota ei ole salattu.

Sisällys

1 Johdanto

Yksi yleisimmistä verkkopalveluiden kirjautumistavoista on käyttäjän todennus käyttäjän määrittelemän salasanan avulla (Haque, Wright ja Scielzo 2013). Tällöin suuri vastuu käyttäjän tietoturvan ylläpidosta on käyttäjällä itsellään. Käyttäjät eivät kuitenkaan usein ole huolellisia salasanojensa turvallisuuden suhteen vaan monesti uudelleenkäyttävät ja unohtavat salasanojaan (Florencio ja Herley 2007) ja käyttävät heikkoja salasanoja, millä voi olla vakavakin seuraus, esimerkiksi tietomurto tai identiteettivarkaus. Useasta luonnollisen kielen sanasta koostuvat tunnuslauseet parantavat salasanojen turvallisuutta verrattuna käyttäjän itsenäisesti valitsemiin salasanoihin (Yan ym. 2004) mutta on yhä käyttäjän vastuulla, että tunnuslauseet ovat tarpeeksi monipuolisia, jotta niitä ei saa sanakirjahyökkäyksellä murrettua. Salasananhallintaohjelmat eli salasanaohjelmat siirtävät vastuun salasanojen vahvuudesta, säilytyksestä ja kirjoittamisesta käyttäjältä salasanaohjelman ohjelmistokehittäjälle. Salasanaohjelmat tuovat samalla mukanaan omat tietoturvaongelmansa, joihin tässä kirjallisuuskatsauksessa perehdytään.

Tässä kirjallisuuskatsauksessa kartoitetaan, mitä tietoturva-aukkoja eli haavoittuvuuksia salasanaohjelmilla on havaittu, mistä salasanaohjelman ominaisuuksista haavoittuvuudet ovat johtuneet ja miten näitä ominaisuuksia on muutettu tai ehdotettu muutettavaksi haavoittuvuuksien korjaamiseksi. Tutkielman aiherajauksen ulkopuolelle jäävät haavoittuvuudet, jotka johtuvat käyttäjän inhimillisistä virheistä tai ohjelmistokehittäjän organisaatioturvallisuuden puutteista ja sisäpiiriuhasta. Tällaisia hyökkäysvektoreita ovat esimerkiksi avoimen salasanatietokannan jättäminen valvomatta, pääsalasanan selvittäminen käyttäjää manipuloimalla (engl. *social engineering*), käyttäjän sormenpainalluksien tarkkailu valvontakameralta ja haittaohjelman asentaminen salasanaohjelman ohjelmistopäivityksellä. Tutkielmassa on kaksi pääosaa: luku salasanaohjelmien ominaisuuksista, joka pyrkii kartoittamaan syitä, miksi kyseiset ominaisuudet ovat tärkeitä salasanaohjelmille, ja luku salasanaohjelmien haavoittuvuuksista, jossa käydään läpi salasanaohjelmissa havaittuja haavoittuvuuksia.

Salasanaohjelmien käytettävyyttä ja turvallisuutta on tutkittu jo aiemmin Chaudharyn ym. systemaattisessa kirjallisuuskatsauksessa (Chaudhary ym. 2019). Tähän tutkielmaan on valittu tutkimuksia kapeammalla otannalla, mutta salasanaohjelmiin kohdistuvia hyökkäyksiä

pyritään kuvailemaan tarkemmin. Lisäksi tutkielmaan on sisällytetty joitakin akateemisen kirjallisuuden ulkopuolisia hyökkäyksiä.

Kysymys salasanaohjelmien tietoturvasta on ajankohtainen IT-alan yritysten julkaisemien selvitysten perusteella, vaikkakaan niiden lähdemateriaalina käytettyjä kyselytutkimuksia ei ole sellaisenaan julkaistu. Selvitysten mukaan vuonna 2023 jo 30 prosenttia länsimaiden ja Japanin aikuisista käyttivät salasanaohjelmia (Bitwarden 2023) ja Yhdysvalloissa merkittävät harppaukset salasanaohjelmien käyttöasteessa ajoittuivat 2010-luvun loppuun ja 2020-luvun alkuun (Siber Systems ja uSamp 2015; Google ja The Harris Poll 2019a, 2019b). Yhdysvalloissa huomattavaa on myös Security.org-mediayrityksen selvityksissä (Security.org 2021, 2023a, 2023b) esiintullut siirtymä pienemmistä salasanapalveluista suurempiin. Googlen ja Applen ilmaisten salasanapalvelujen markkinaosuudet olivat nousseet yhteensä 15 prosentista 49 prosenttiin vuosina 2021–2023, kun taas ensisijaisesti salasanhallintaan erikoistuneiden yritysten markkinaosuudet joko pysyivät paikoillaan tai laskivat. Selvityksissä yhdeksi muutoksen syyksi arvellaan Lastpass-salasanapalveluun kohdistunutta tietomurtoa, joka sai paljon mediahuomiota vuonna 2022. Asiakkaat luottavat enemmän suuriksi koettuihin yrityksiin, ja asiakkaan luottamus on tärkeä edellytys myynnille (Phung, Yen ja Hsiao 2009), mikä ainakin yhtenä osatekijänä tukee selvitysten johtopäätöstä. Käyttäjien preferensseistä kerrotaan lisää luvussa 2.2.

Mainittakoon, että tietoturvan parantamiseksi ja salasananhallinnan aiheuttaman psyykkisen uupumuksen (*engl. password fatigue*) vähentämiseksi on kehitetty muitakin ratkaisuja kuin salasanaohjelmat. Erityisesti suuret teknologiayritykset tarjoavat kertakirjautumispalveluja (*engl. single sign-on*) OpenID Connect -protokollalla toteutettuna (Morkonda, Chiasson ja Oorschot 2021). Toinen ratkaisu on kertakäyttöiset salasanat (*engl. one-time password, OTP*), joita on käytetty esimerkiksi suomalaisten pankkien paperisissa tunnuslukulistoissa vuodesta 1982 lähtien (Kangasniemi 2020). Nykyään kryptografisilla tiivistefunktioilla luodut kertakäyttöiset HOTP- ja TOTP-salasanat ovat yleisiä kaksivaiheisen tunnistamisen toteutuksissa. Kolmas ratkaisu on FIDO 2.0 -standardin protokollat, jotka perustuvat julkisen avaimen menetelmään (*public-key cryptography*). Näillä vaihtoehtoisilla ratkaisuilla ja salasanaohjelmilla on yhteistä se, että käyttäjällä ei ole enää tarvetta muistaa useita salasanoja.

Tutkielman akateeminen lähdeaineisto on etsitty pääasiassa Scopus- ja Google Scholar -ha-

kupalveluilla. Hakusanoina on käytetty ainakin seuraavia termejä ja joitakin niiden yhdistelmiä: "password", "weak password", "password manager", "browser", "password fatigue", "single sign-on", "authentication methods"; "security", "brute force", "service", "memorization", "usage", "comparison", "review", "survey", "spyware", "malware", "encryption", "server", "injection", "compromised", "attack", "authentication", "usability". Lähdeaineiston etsinnässä on myös pienissä määrin käytetty Microsoft Copilot -keskustelubottia. Resurssien puutteen takia tutkielman tiedonhakua ei ole toteutettu järjestelmällisesti, ja kaikkea olennaista lähdeaineistoa ei ole käyty läpi.

2 Salasanaohjelmien ominaisuudet

Salasanaohjelmia käytetään salasanojen hallinnassa ja niiden tärkein tehtävä on tallettaa salasanat turvallisesti tietokantaan. Salasanatietokanta on salattu useimmiten pääsalasanalla, jotta käyttäjällä on täysi valta siitä, kuka pääsee käsiksi salasanoihin. Hyvältä salasanaohjelmalta odotetaan kuitenkin myös muita tietoturvaa ja käytettävyyttä parantavia ominaisuuksia.

2.1 Tietoturvallisuus

Salasanaohjelmat on Oeschin ja Ruotin tutkimuksessa jaettu kolmeen luokkaan: erilliset sovellusohjelmat, selainlaajennukset ja selaimeen sisäänrakennetut salasanaohjelmat (Oesch ja Ruoti 2020). Lisäksi salasanaohjelmat voidaan jakaa luokkiin sen perusteella, millä käyttöjärjestelmällä niitä ajetaan ja missä ne säilyttävät salasanojaan. Kun salasanaohjelmat hyödyntävät samoja selaimen tai käyttöjärjestelmän sovelluskirjastoja, ne altistuvat samoille haavoittuvuuksille. Koska selaimia ja käyttöjärjestelmiä päivitetään jatkuvasti, haavoittuvuudet saattavat syntyä, vaikka salasanaohjelman versio pysyy samana. Salasanaohjelmat ovat usein joko täysin paikallisia asennuksia tai sitten paikallisen asennuksen lisäksi salasanatietokanta synkronoidaan pilvipalvelimen avulla. Mitä useammalle eri laitteelle salasanaohjelma on asennettu ja mitä useammalla laitteella salasanatietokanta sijaitsee, sitä enemmän mahdollisia hyökkäysvektoreita hyökkääjällä on käytettävissään.

Salasanaohjelmien toimintatapoja ei ole kuitenkaan hakattu kiveen. McCarneyn ym. tutkimuksessa esitetään yleisistä salasanaohjelmista poikkeava salasanaohjelma, joka vaatii sekä sovellusohjelmaa että selainlaajennosta toimiakseen (McCarney ym. 2012). Selainlaajennos toimii alisteisena sovellusohjelmalle, millä saavutetaan turvaa selainlaajennoksen isäntäkoneella ajettavia haittaohjelmia vastaan. Salasanaohjelma toimii siten, että salasanoja säilytetään Android-laitteen sovellusohjelmassa ja selainlaajennos pyytää salasanoja ainoastaan tarvittaessa.

Tunnettujen salasanaohjelmien joukossa 256-bittinen AES on selvästi yleisin tietokannan salausalgoritmi (Arias-Cabarcos ym. 2016; Oesch ja Ruoti 2020). AES-algoritmin etuna on

sen laaja laitteistokiihdytystuki sekä x86- että mobiiliprosessoreissa. Muut salausalgoritmit ovat vähemmän käytettyjä, mutta esimerkiksi Keepass tukee myös ChaCha20-ja Twofish-algoritmia. Tunnetuissa salasanaohjelmissa käytettyjä avaimenjohdatusfunktioita (*engl. key derivation function*) ovat AES-KDF, PBKDF2, Argon2d ja Argon2id (Oesch ja Ruoti 2020; Keepass 2024). Yleensä avaimenjohdatusfunktiot johtavat salausavaimensa pääsalasanasta, mutta salasanaohjelmat, jotka eivät käytä pääsalasanaa, käyttävät lähtöarvonaan muuta tietoa.

Etenkin maksullisissa salasanapalveluissa salasanatietokantaa säilytetään palveluntarjoajan palvelimilla, ja asiakasohjelmat synkronoidaan pilvitietokannan kautta. Pilvipalveluissa korostuu käyttäjän luottamus palveluntarjoajan kykyyn säilyttää salasanatietokantaa turvallisesti (Karole, Saxena ja Christin 2011, s. 236). Jos salasanaohjelman lähdekoodi on avointa, käyttäjä voi varmistua siitä, että ohjelma täyttää lupauksensa. Andersonin mukaan sekä avoimen että suljetun lähdekoodin järjestelmillä on potentiaalia olla yhtä turvallisia, mutta todellisessa maailmassa turvallisuus riippuu monesta tekijästä, kuten resursseista, avoimuuden vaikutuksesta sovelluskehittäjien työntekoon ja sovelluskehittäjien yhteistyöstä (Anderson 2002).

2.2 Käytettävyys ja käyttäjien odotukset

Käytännöllisyys ja turvallisuus ovat salasanaohjelmien käyttäjille tärkeimpiä syitä käyttää salasanaohjelmia (Fagan ym. 2017). Kun eri käyttäjäryhmiä on tutkittu tarkemmin, on käyttäjäryhmillä havaittu erilaisia prioriteetteja (Pearman ym. 2019). Pearmanin ym. tutkimuksessa verkkoselaimeen sisäänrakennettuja salasanaohjelmia käyttäville tärkein asia on nimenomaan salasanaohjelman käytännöllisyys: salasanaohjelmaa on alettu käyttämään, koska se on ollut valmiina selaimessa ja sen ominaisuudet on koettu hyödyllisiksi. Tällaisia käytännöllisiä ominaisuuksia ovat automaattinen kirjautumislomakkeen täyttö ja salasanojen synkronisaatio laitteiden välillä. Erikseen asennettavien salasanaohjelmien käyttäjille tärkeää on salasanaohjelman turvallisuus, mikä näkyy käytännössä salasanaohjelman huolellisessa valinnassa ja turvallisuutta parantavien ominaisuuksien, kuten salasanageneraattorin, käytössä. Koska salasanageneraattorit tekevät uuden salasanan luomisesta helpompaa, olisi voinut olettaa, että niiden käyttö olisi yleistä myös sisäänrakennettujen salasanaohjelmien käyttäjien

keskuudessa. Tutkimuksen tulos on kuitenkin päinvastainen, mikä voi johtua ominaisuuden huonosta löydettävyydestä. Pearmanin ym. tutkimuksessa ehdotetaankin löydettävyyden parantamista lisäämällä salasanaohjelmaan kehote salasanageneraattoriominaisuuden käytölle, koska salasanojen tallentamisen kehotteet on jo todettu erittäin toimiviksi verkkoselaimissa.

Pearmanin ym. mukaan erikseen asennettavien salasanaohjelmien käyttäjät eivät ole lähtökohtaisesti halukkaita maksamaan salasanaohjelmista. Ne ihmiset, jotka ovat valmiita maksamaan, vaativat maksulliselta ohjelmalta erityistä turvallisuutta, erityistä käytännöllisyyttä tai jotain lisäominaisuuksia. Maksullisten salasanapalvelujen välinen kilpailu onkin yksi salasanaohjelmien kehitystä ohjaava tekijä.

Loppujen lopuksi salasanaohjelman turvallisuudella ei ole merkitystä, jos käyttäjä ei sitä käytä. Edes IT-alan koulutuksella ei ole todettu olevan merkittävää vaikutusta salasanaohjelmien käyttöasteeseen (Alodhyani, Theodorakopoulos ja Reinecke 2020), ja IT-ammattilaisten ja maallikoiden salasananhallintastrategioiden on huomattu olevan keskenään hyvin samankaltaisia (Stobert ja Biddle 2018). Stobertin ja Biddlen tutkimuksessa esiintulleita strategioita ovat salasanojen luokittelu tärkeyden mukaan, vakiosalasanan uudelleenkäyttäminen, uusien salasanojen muodostaminen vakiosalasanasta ja muulla tavoin salasanojen luominen systemaattisesti. Nämä strategiat pyrkivät ratkomaan samoja salasanojen luomiseen ja muistamiseen liittyviä ongelmia, joita salasanaohjelmat ratkaisevat. Silti yleinen syy olla käyttämättä salasanaohjelmia on ajatus sen tarpeettomuudesta (Fagan ym. 2017). Tämä viittaa siihen, että joko ihmiset eivät ole tietoisia salasanaohjelmien ominaisuuksista tai eivät tietoisuudesta huolimatta halua käyttää salasanaohjelmia.

Faganin ym. mukaan toinen yhtä yleinen syy olla käyttämättä salasanaohjelmia on huoli salasanaohjelman tietoturvasta. Salasanojen laittaminen samaan paikkaan herättää ihmisissä huolia kahdesta syystä: hyökkääjä voi päästä kaikkiin salasanoihin kerralla käsiksi, ja lisäksi käyttäjän unohtaessa pääsalasanansa käyttäjä ei enää itse pääse käsiksi salasanoihinsa (Pearman ym. 2019). Rayn ym. tutkimuksessa yli 60-vuotiaiden ihmisten salasanojen käytössä ja asennoitumisessa on havaittu joitakin eroja verrattuna Pearmanin ym. tutkimuksen nuoriin ja keski-ikäisiin painottuvaan osallistujajoukkoon (Ray ym. 2021). Salasanaohjelmia käyttämättömät vanhemmat ihmiset eivät uskoneet ikänsä takia tarvitsevansa salasanaohjelmia. Toisaalta he eivät myöskään sanoneet uudellenkäyttävänsä salasanoja toisin kuin Pearma-

nin ym. tutkimuksen salasanaohjelmia käyttämättömät nuoremmat ihmiset. Salasanaohjelmia käyttämättömät nuoremmat ihmiset erosivat vanhemmista myös siinä, että he ajattelivat käyttäjätunnustensa olevan liian vähäarvoisia vaatiakseen salasanaohjelmien tuomaa turvaa.

3 Haavoittuvuudet

Tässä luvussa käsitellään salasanaohjelmissa havaittuja haavoittuvuuksia esimerkkihyökkäysten avulla. Esimerkkihyökkäysten käsittely etenee taustoituksesta ja toteutustavasta mahdollisiin toimenpiteisiin haavoittuvuuksien korjaamiseksi. Esimerkit on ryhmitelty toteutustapojen mukaan.

3.1 Verkkosivun kirjautumislomakkeiden automaattinen täyttö

Verkkosivun kirjautumislomakkeen täyttäminen on helppo haaste salasanaohjelman selainlisäosalle, koska täytettävät kentät on usein selkeästi merkitty verkkosivun rakenteeseen. Vaikeaa sen sijaan on varmistaa, että lomake on sama kuin mikä se oli salasanaa tallennettaessa. Silverin ym. tutkimuksessa demonstroidaan vuonna 2014, että väliintulohyökkäyksellä (*engl. man-in-the-middle attack*) on mahdollista huijata käyttäjän salasanaohjelma antamaan useiden sivustojen käyttäjätunnukset käyttäjän huomaamatta (Silver ym. 2014). Väliintulohyökkäyksen riski salasanaohjelmille on tiedostettu jo aiemmin esimerkiksi Gonzalezin ym. samankaltaisessa tutkimuksessa, jossa väliintulohyökkäys on toteutettu ARP-väärennöksellä (Gonzalez, Chen ja Jackson 2013).

Silverin ym. tutkimuksen hyökkäys on mahdollinen, kun salasanaohjelma on asetettu täyttämään kirjautumislomakkeet automaattisesti ja käyttäjä liittyy pahan toimijan hallinnoimaan lähiverkkoon. Varsinaista hyökkäystä varten Silverin ym. tutkimuksessa esitetään kolmivaiheinen prosessi. Ensin käyttäjä ohjataan lähiverkon ylläpitäjän tervetulosivulle, jota hyökkääjä voi manipuloida. Toisessa vaiheessa hyökkääjä joko injektoi tervetulosivulle kirjautumislomakkeita sisältäviä iFrame-elementtejä, avaa kirjautumislomakkeita sisältäviä popup-ikkunoita tai uudelleenohjaa käyttäjän selaimen verkkosivuille, joiden tunnukset hyökkääjä haluaa varastaa. Kolmannessa vaiheessa salasanaohjelma täyttää kakkosvaiheen kirjautumislomakkeet, ja hyökkääjä kerää kirjautumistiedot talteen JavaScriptilla joko kopioimalla kirjautumistiedot täytetyltä lomakkeelta hyökkääjän kontrolloiman osoitteen lomakkeelle tai tarvittaessa muuttamalla lomakkeiden action-atribuuttia osoittamaan hyökkääjän kontrolloimaan osoitteeseen.

Silverin ym. tutkimuksessa selvitetään myös väliintulohyökkäysten toimivuutta HTTPS-sivustoilla ja XSS-injektion avulla. Hyökkäys toimii HTTPS-sivuilla joko vaihtamalla yhteyden varmennetta, hyödyntämällä sivuston XSS-haavoittuvuutta tai hyödyntämällä kohdesivun aktiivista sisältöä, joka ladataan HTTP-yhteyden avulla. Sivuston XSS-haavoittuvuus mahdollistaa hyökkäyksen toteuttamisen täysin toisesta tietoverkosta pelkästään huijaamalla käyttäjä hyökkääjän sivulle.

Silverin ym. mukaan yksinkertaisin tapa estää mahdolliset hyökkäykset on vaatia käyttäjältä jotain vuorovaikutusta ennen lomakkeen täyttöä. Vuorovaikutus voi olla esimerkiksi näppäimistöoikotien painaminen, klikkaus, salasanaohjelman lomakkeentäyttöpainikkeen valitseminen tai kirjautumiskenttään kirjoittaminen. Vuorovaikutus estää automaattiset hyökkäykset muttei hyökkäyksiä, jotka tapahtuvat käyttäjän kirjautuessa sisään. Toinen ehdotettu keino on tallentaa kirjautumislomakkeen action-atribuutti verkkotunnuksia tallentaessa ja verrata tallennettua atribuuttia ladattuun atribuuttiin verkkosivulle kirjautuessa. Tämä ehdotus ei ole kuitenkaan yhteensopiva esimerkiksi AJAX-lomakkeiden kanssa. Kolmantena keinona tutkimuksessa ehdotetaan sivustojen ylläpitäjille tapoja suojata käyttäjiään: HSTS-asetus estää sivustoa latautumasta HTTP:llä, CSP-käytännöt estävät XSS-hyökkäyksen toteuttamisen, ja kirjautumissivun isännöiminen toisella aliverkkotunnuksella pienentää sivuston hyökkäyspinta-alaa.

Koska HTTPS-yhteydet ovat melkein täysin syrjäyttäneet HTTP-yhteydet verkkoliikenteen yleisyydessä (Let's Encrypt 2024), väliintulohyökkäys HTTP-yhteyden avulla on nykyään pienempi riski kuin se oli Gonzalezin ym. ja Silverin ym. tutkimusten julkaisuaikaan. Väliintulohyökkäys HTTPS-yhteydellä on mahdollinen, jos käyttäjä ohittaa selaimen varmennevaroituksen, mutta varoitusten uudelleensuunnittelun ansiosta käyttäjät ohittavat varoituksia nykyään harvemmin kuin ennen (Felt ym. 2015). XSS-hyökkäykset ovat yhä merkittävä riski Internetissä, vaikka CSP-käytännöt ovatkin tehokas suoja monenlaisia XSS-haavoittuvuuksia vastaan (Hannousse, Yahiouche ja Nait-Hamoud 2024).

3.2 Salasanatietokantaan kohdistuvat hyökkäykset

Jos hyökkääjä aikoo hyödyntää jotain salasanatietokannan tietoturvan heikkoutta, hyökkääjän pitää ensin saada salasanatietokanta haltuunsa. Haltuunotto voi tapahtua joko tiedonsiirron aikana, pilvipalvelimelta tai käyttäjän koneelta. Kaksi ensimmäistä keinoa ovat mahdollisia, jos salasanaohjelma synkronoi tietokantansa lähettämällä sen internetin kautta, ja jälkimmäisin keino on mahdollinen, jos salasanaohjelma säilyttää tietokantaa käyttäjän laitteella edes väliaikaisesti. Salasanatietokannan synkronisaatio eri laitteiden välillä ja salasanaohjelman käyttäminen ilman Internetiä ovat yleisiä ominaisuuksia salasanaohjelmissa, joten hyökkääjällä on yleensä useita keinoja saada salasanatietokanta haltuunsa.

Gastin ja Rasmussenin tutkimuksen perusteella salasanaohjelmien tarjoama tietoturvallisuus vaihtelee paljon (Gasti ja Rasmussen 2012). Jotkut salasanaohjelmat eivät salaa tietokantaansa ollenkaan, toiset salaavat vain tärkeimmät tiedot kuten salasanat, ja kolmannet salaavat kaiken. Luonnollisesti salaamattomat tietokannat eivät tarjoa tietoturvaa ollenkaan, ja sen takia ne eivät ole järkeviä muissa kuin ainoastaan täysin paikallisesti asennetuissa salasanaohjelmissa. Osittain salatusta tietokannasta hyökkääjä voi kerätä tietoa, kuten URL-osoitteita, jota voi hyödyntää muissa hyökkäyksissä. Lisäksi heikosti salatusta salasanatietokannasta hyökkääjä voi arvioida tietokannan käyttäjätunnusten määrää ja pituutta.

Myös kokonaan salattuihin salasanatietokantoihin kohdistuu tietoturvauhkia. Salasanatietokantojen turvallisuutta selvitettiin Gastin ja Rasmussenin tutkimuksessa kahdella tavalla: erottamistestillä, jolla arvioidaan salasanatietokantojen kykyä pysyä joukosta erottamattomana riippumatta tietokannan tietueista, ja muokkaustestillä, jolla arvioidaan sitä, pystyykö hyökkääjä muokkaamaan salasanatietokantaa salasanaohjelman hyväksymällä tavalla. Kaikki selaimeen sisäänrakennetut salasanaohjelmat ja puolet muista salasanaohjelmista epäonnistuivat erottamistestissä. Kokonaan salatut salasanatietokannat, jotka epäonnistuivat erottamistestissä, ovat alttiita samanlaisille tietovuodoille kuin osittain salatut salasanatietokannat. Vain yksi salasanatietokanta onnistui ja loput epäonnistuivat muokkaustestissä. Muokkaustestissä ilmaistu salasanatietokannan muokkaaminen voi tarkoittaa sitä, että hyökkääjä poistaa tietueita, palauttaa tietueita niiden aiempiin arvoihin tai muokkaa tietueita kokonaan tai osittain. Tietueiden muokkaaminen voi muuttaa salasanaohjelman käytöstä, esimerkiksi hyökkääjän vaihtaessa alkuperäisen URL-osoitteen tilalle hyökkääjän sivun URL-osoitteen.

Useat selaimiin sisäänrakennetut salasanaohjelmat eivät käytä pääsalasanaa ja siirtävät vastuun salasanatietokannan salauksesta käyttöjärjestelmälle (Oesch ja Ruoti 2020). Tällöin salasanatietokanta on jonkun muun salasanan varassa, joka voi olla esimerkiksi käyttöjärjestelmän sisäänkirjautumissalasana. Tämä tilanne tarkoittaa käytännössä sitä, että käyttäjän salasanaohjelma on auki niin pitkään kuin käyttöjärjestelmä on auki.

Väsytyshyökkäyksessä salasanatietokannan salaus yritetään purkaa arvaamalla tietokannan salasana. Arvauksia tehdään niin kauan, kunnes jokin niistä osuu oikeaan. **Sanakirjahyökkäys** on väsytyshyökkäys, jossa salasana-arvausten määrää pyritään vähentämään käyttämällä arvauksissa luonnollisen kielen sanoja tai yleisesti käytettyjä salasanoja. Salauksessa avaimenjohdatusfunktion rooli on lisätä yksittäisten yritysten vaatimia resursseja toistamalla itseään rekursiivisesti useita kertoja. Avaimenjohdatusfunktion lisäämät resurssivaatimukset kertautuvat hyökkääjän useissa yrityksissä, mikä tekee hyökkäyksestä epäkäytännöllisen hitaan. Joidenkin salasanapalveluiden on havaittu olevan haavoittuvaisia väsytyshyökkäyksille johtuen avaimenjohdatusfunktion vähäisestä toistomäärästä (Zhao, Yue ja Sun 2013). Suojaus väsytyshyökkäyksiä vastaan on tärkeää erityisesti salasanapalveluiden tapauksessa, koska tietoturvauhka voi realisoitua niin, että hyökkääjä saa käsiinsä lukemattomien käyttäjien salasanatietokannat. Tällaisia tietomurtoja on tapahtunut aiemmin (Toubba 2023).

Gastin ja Rasmussenin tutkimuksessa korostetaan sitä, että IT-alan yleiset turvallisuuskäytännöt, kuten AES-CBC-salauksen käyttäminen, eivät takaa salasanatietokannan tietoturvaa. AES-algoritmin CBC-moodissa salattu salasanatietokanta onnistuu tutkimuksen erottamistestissä mutta epäonnistuu muokkaustestissä, koska CBC-moodi ei varmista salatun tiedon eheyttä. Yleisten käytäntöjen sijaan salasanatietokantojen suunnittelussa tulisikin huomioida, mitä tietoa hyökkääjä voi saada salatusta salasanatietokannasta ja miten hyökkääjä voi muokata salattua salasanatietokantaa.

3.3 Hyökkäykset vaarantuneelta isäntäkoneelta

Mitä lähempänä rautaa haittaohjelmaa ajetaan (*engl. bare-metal programming*), sitä helpompi haittaohjelman on ohittaa salasanaohjelman ajonaikaiset suojauskeinot. Tämän takia salasanaohjelmakehittäjät eivät aina edes pyri suojautumaan kaikkia isäntäkoneella tapahtuvia

hyökkäyksiä vastaan (Bevendorff 2017). Tehottomienkin suojausmekanismien etuna on, että suojausten kiertäminen vaatii hyökkääjältä enemmän työtä ja mahdollisesti salasanaohjelmakohtaisen haittaohjelman. Haittapuolena on vastaavasti salasanaohjelman sovelluskehitysresurssien tuhlaaminen.

Keepass-salasanaohjelmaa vastaan kehitetty tietomurtotyökalu KeeFarce on hyvä esimerkki siitä, miten mitään salasanaohjelmaa ei voi turvallisesti ajaa vaarantuneella koneella, johon hyökkääjä on saanut käyttöjärjestelmän alimpien tasojen oikeudet. Ajon aikana Keepass säilyttää salasanoja muistissa salattuina, ja salausavainta säilytetään Windows-käyttöjärjestelmän hallinnoimalla muistialueella DPAPI-ohjelmistorajapinnan kautta (Keepass 2015). KeeFarce käyttää DLL-injektiota ajaakseen haittaohjelmansa Keepass-prosessin kontekstissa ja pääsee näin käsiksi prosessin aliohjelmiin. KeeFarce kutsuu Keepassin vientimetodia, joka tallentaa koko salasanatietokannan selkokielisenä massamuistiin (Andzakovic 2015).

Keepass-ohjelmasta löydettiin myös varsinainen **muistiturvallisuushaavoittuvuus** vuonna 2023. Ohjelman pääsalasanan kirjoittamiseen käytetty SecureTextBoxEx-elementti tallensi muistiin selkokielisen merkkijonon jokaista pääsalasanan merkkiä kohden, ja tallennetut merkkijonot jäivät muistiin, vaikka ohjelman sulki (vdohney 2023). Haavoittuvuus korjattiin antamalla enemmän vastuuta SecureTextBoxEx-elementin toiminnasta Windows-käyttöjärjestelmän ohjelmistorajapinnalle ja lisäämällä muistiin valemerkkijonoja, jotta pääsalasanasta koostuvia merkkijonoja olisi vaikeampi tunnistaa (Reichl 2023).

Grayn ym. tutkimuksessa havaittiin, että muistiin tallennettu pääsalasana voi päätyä salaamattomana myös Windowsin sivutustiedostoon ainakin silloin, jos tietokoneessa on vain 1 GB muistia (Gray, Franqueira ja Yu 2016). Tutkimuksen toisen testitapauksen kohdalla huomattiin, että salasanaohjelman **väliaikaisiksi tarkoitetut tiedostot** voivat jäädä tietokoneen massamuistiin, jos jotain odottamatonta tapahtuu. Tutkimuksen mukaan Keepass-ohjelman tulostusominaisuus luo väliaikaisen HTML-tiedoston tulostusta varten, mutta HTML-tiedostoa ei poisteta, jos tulostus peruutetaan.

Vakoiluohjelmat kattavat suuren joukon enemmän tai vähemmän erikoistuneita haittaohjelmia. Keepass-salasanaohjelmassa on kaksi tapaa suojautua vähemmän erikoistuneita näppäimistökaappareita vastaan: pääsalasanaikkunoiden näyttäminen Windows-käyttöjärjestelmän

Secure Desktop -työpöydällä ja automaattisen kirjoittamisen hämäännyttäminen (*engl. obfuscation*) (Keepass 2024).

Isäntäkoneella tapahtuvia hyökkäyksiä on ennaltaehkäisty käyttöjärjestelmätasolla eristämällä sovelluksia toisistaan (*engl. application sandboxing*) ja rajoittamalla käyttäjän oikeuksia, esimerkiksi Android-mobiilikäyttöjärjestelmässä.

4 Yhteenveto

Salasanaohjelmat ovat kompromisseja tietoturvan tason ja käytettävyyden välillä. Huomattavaa on, että molemmilla ääripäillä on omat käyttäjäkuntansa: helppokäyttöisyyttä priorisoivat käyttäjät suosivat selaimeen sisäänrakennettuja salasanaohjelmia, jotka ovat monilta tietoturvaominaisuuksiltaan heikkoja, ja tietoturvaa priorisoivat käyttäjät suosivat erikseen asennettavia ja ominaisuuksiltaan rajoitettuja salasanaohjelmia, joiden hyökkäyspinta-ala on pidetty pienenä käytettävyyden kustannuksella. Salasanaohjelmien yleistymisen ja salasanaohjelmiin kohdistuneen tutkimuksen myötä salasanaohjelmien käytettävyys on parantunut huomattavasti 2000-luvulta 2020-luvulle. Vaikka uusien käytettävyysominaisuuksien kehitys on voinut heikentää salasanaohjelmien tietoturvaa, nämä ominaisuudet ovat tehneet salasanaohjelmista tarpeeksi hyödyllisiä, jotta ne ovat käyttäjilleen käyttämisen arvoisia.

Salasanaohjelmia ja niiden ajoympäristöinä toimivia selaimia ja käyttöjärjestelmiä kehitetään jatkuvasti, minkä takia vanhat haavoittuvuudet eivät ole enää yhtä merkityksellisiä kuin ennen. Salaamattomiin HTTP-yhteyksiin tukeutuvat hyökkäykset eivät ole enää suuri riski, kun melkein kaikki verkkoyhteydet käyttävät HTTPS-yhteyksiä (Let's Encrypt 2024). Toisaalta salasanaohjelmien ja niiden ajoympäristöjen kehitystyö mahdollistaa uusien haavoittuvuuksien synnyn. Uudet salasanaohjelmien ominaisuudet voivat sisältää haavoittuvuuksia, joita salasanaohjelmissa ei ennen ollut, kuten verkkolomakkeiden automaattisesta täytöstä kertovassa luvussa 3.1 on kuvailtu. Tietoturvallisuus on tärkeää ottaa huomioon salasanaohjelman kaikkien komponenttien kehityksessä, koska haavoittuvuudet voivat syntyä yllättävistä virheistä, kuten vääräntyyppisestä tai väärin ohjelmoidusta UI-elementistä.

Haavoittuvuudet ovat syntyneet erilaisista lähtökohdista, joten myös haavoittuvuuksien korjaamiseksi tehdyt asiat riippuvat täysin haavoittuvuudesta. Jotkut kyberhyökkäykset, kuten hyökkäys KeeFarce-ohjelmalla, eivät ole salasanaohjelmakehittäjien torjuttavissa järkevästi, ja ne johtuvat ensisijaisesti ajoympäristön kyberturvallisuuden puutteista. Tässä tutkielmassa kartoitettujen haavoittuvuuksien valossa hyvä salasanaohjelma on sellainen, jonka kehityksessä otetaan huomioon salasanaohjelmien korkeat tietoturvaodotukset ja johon tehdään muutoksia uusien tietoturvauhkien tullessa ilmi.

Tulevaisuuden tutkimuksessa olisi hyvä selvittää, miten salasanaohjelmien hyökkäyspinta-alaa saisi pienennettyä. Nykyään salasanaohjelmat toimivat niin, että käyttäjä asentaa salasanaohjelman ja salasanatietokannan kaikille käyttämilleen laitteille, jolloin hyökkäyspinta-ala on suuri. McCarneyn ym. tutkimuksessa esitettiin eri tavalla toimiva salasanaohjelma (McCarney ym. 2012), jota voisi olla mahdollista jatkokehittää. Kehitystyössä on tärkeää huomioida käytettävyys, koska käyttäjät eivät mielellään siirry käytettävyydeltään hyvistä salasanaohjelmista huonompiin.

Lähteet

Alodhyani, Fahad, George Theodorakopoulos ja Philipp Reinecke. 2020. “Password Managers—It’s All about Trust and Transparency”. *Future Internet* 12 (11). ISSN: 1999-5903. https://doi.org/10.3390/fi12110189. https://www.mdpi.com/1999-5903/12/11/189.

Anderson, Ross. 2002. “Security in open versus closed systems—the dance of Boltzmann, Coase and Moore”.

Andzakovic, Denis. 2015. “KeeFarce”, 17. marraskuuta 2015. Viitattu 23. maaliskuuta 2024. https://github.com/denandz/KeeFarce.

Arias-Cabarcos, Patricia, Andrés Marín, Diego Palacios, Florina Almenárez ja Daniel Díaz-Sánchez. 2016. “Comparing Password Management Software: Toward Usable and Secure Enterprise Authentication”. *IT Professional* 18 (5): 34–40. https://doi.org/10.1109/MITP.2016.81.

Bevendorff, Janek. 2017. “Generally, I’m not so sure if it is really worth the effort”. (Bevendorff on yksi KeePassXC-salasanaohjelman pääkehittäjistä.) 4. maaliskuuta 2017. Viitattu 11. maaliskuuta 2024. https://github.com/keepassxreboot/keepassxc/issues/375#issuecomment-284170952.

Bitwarden. 2023. “World Password Day Survey 2023”. Viitattu 9. maaliskuuta 2024. https://bitwarden.com/resources/world-password-day/.

Chaudhary, Sunil, Tiina Schafeitel-Tähtinen, Marko Helenius ja Eleni Berki. 2019. “Usability, security and trust in password managers: A quest for user-centric properties and features”. *Computer Science Review* 33:69–90. ISSN: 1574-0137. https://doi.org/https://doi.org/10.1016/j.cosrev.2019.03.002. https://www.sciencedirect.com/science/article/pii/S1574013718302533.

Fagan, Michael, Yusuf Albayram, Mohammad Maifi Hasan Khan ja Ross Buck. 2017. “An investigation into users’ considerations towards using password managers”. *Human-centric Computing and Information Sciences* 7:1–20. https://doi.org/https://doi.org/10.1186/s13673-017-0093-6.

Felt, Adrienne Porter, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris ja Jeff Grimes. 2015. “Improving SSL Warnings: Comprehension and Adherence”. Teoksessa *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems,* 2893–2902. CHI ’15. Seoul, Republic of Korea: Association for Computing Machinery. ISBN: 9781450331456. https://doi.org/10.1145/2702123.2702442. https://doi.org/10.1145/2702123.2702442.

Florencio, Dinei ja Cormac Herley. 2007. “A large-scale study of web password habits”. Teoksessa *Proceedings of the 16th International Conference on World Wide Web,* 657–666. WWW ’07. Banff, Alberta, Canada: Association for Computing Machinery. ISBN: 9781595936547. https://doi.org/10.1145/1242572.1242661.

Gasti, Paolo ja Kasper B. Rasmussen. 2012. “On the Security of Password Manager Database Formats”. Teoksessa *Computer Security – ESORICS 2012,* toimittanut Sara Foresti, Moti Yung ja Fabio Martinelli, 770–787. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-33167-1.

Gonzalez, Raul, Eric Yawei Chen ja Collin Jackson. 2013. “Automated Password Extraction Attack on Modern Password Managers”. *CoRR* abs/1309.1416. arXiv: 1309.1416. http://arxiv.org/abs/1309.1416.

Google ja The Harris Poll. 2019a. “Online Security Survey”. Viitattu 9. maaliskuuta 2024. https://services.google.com/fh/files/blogs/google_security_infographic.pdf.

———. 2019b. “The United States of P@ssw0rd$”. Viitattu 9. maaliskuuta 2024. https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf.

Gray, Joshua, Virginia N. L. Franqueira ja Yijun Yu. 2016. “Forensically-Sound Analysis of Security Risks of Using Local Password Managers”. Teoksessa *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW),* 114–121. ISBN: 978-150903694-3. https://doi.org/10.1109/REW.2016.034.

Hannousse, Abdelhakim, Salima Yahiouche ja Mohamed Cherif Nait-Hamoud. 2024. “Twenty-two years since revealing cross-site scripting attacks: A systematic mapping and a comprehensive survey”. *Computer Science Review* 52:100634. ISSN: 1574-0137. https://doi.org/https://doi.org/10.1016/j.cosrev.2024.100634. https://www.sciencedirect.com/science/article/pii/S1574013724000182.

Haque, SM Taiabul, Matthew Wright ja Shannon Scielzo. 2013. “A study of user password strategy for multiple accounts”. Teoksessa *Proceedings of the third ACM conference on Data and application security and privacy,* 173–176.

Kangasniemi, Tuomas. 2020. “Vuodesta 1978”. *Tekniikka & Talous,* numero 34 (23. lokakuuta 2020): 14. ISSN: 0785-997X.

Karole, Ambarish, Nitesh Saxena ja Nicolas Christin. 2011. “A Comparative Usability Evaluation of Traditional Password Managers”. Teoksessa *Information Security and Cryptology - ICISC 2010,* toimittanut Kyung-Hyune Rhee ja DaeHun Nyang, 233–251. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-24209-0.

Keepass. 2015. “Security”. Viitattu 10. maaliskuuta 2024. https://web.archive.org/web/20150727220110/http://keepass.info/help/base/security.html#secmemprot.

———. 2024. “Database Encryption”. Viitattu 9. huhtikuuta 2024. https://keepass.info/help/base/security.html.

Let’s Encrypt. 2024. “Let’s Encrypt Stats”, 21. huhtikuuta 2024. Viitattu 21. huhtikuuta 2024. https://letsencrypt.org/stats/#percent-pageloads.

McCarney, Daniel, David Barrera, Jeremy Clark, Sonia Chiasson ja Paul C. van Oorschot. 2012. “Tapas: design, implementation, and usability evaluation of a password manager”. Teoksessa *Proceedings of the 28th Annual Computer Security Applications Conference,* 89–98. ACSAC ’12. Orlando, Florida, USA: Association for Computing Machinery. ISBN: 9781450313124. https://doi.org/10.1145/2420950.2420964. https://doi.org/10.1145/2420950.2420964.

Morkonda, Srivathsan G., Sonia Chiasson ja Paul C. van Oorschot. 2021. “Empirical Analysis and Privacy Implications in OAuth-based Single Sign-On Systems”. Teoksessa *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society,* 195–208. Association for Computing Machinery. ISBN: 9781450385275. https://doi.org/10.1145/3463676.3485600.

Oesch, Sean ja Scott Ruoti. 2020. “That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers”. Teoksessa *29th USENIX Security Symposium (USENIX Security 20),* 2165–2182. USENIX Association, elokuu. ISBN: 978-1-939133-17-5. https://www.usenix.org/conference/usenixsecurity20/presentation/oesch.

Pearman, Sarah, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin ja Lorrie Faith Cranor. 2019. “Why people (don’t) use password managers effectively”. Teoksessa *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019),* 319–338. Santa Clara, CA: USENIX Association, elokuu. ISBN: 978-1-939133-05-2. https://www.usenix.org/conference/soups2019/presentation/pearman.

Phung, KD, KL Yen ja MH Hsiao. 2009. “Examining the factors associated with consumer’s trust in the context of business-to-consumer e-commerce”. Teoksessa *2009 IEEE International Conference on Industrial Engineering and Engineering Management,* 2241–2245. IEEE.

Ray, Hirak, Flynn Wolf, Ravi Kuber ja Adam J. Aviv. 2021. “Why Older Adults (Don’t) Use Password Managers”. Teoksessa *30th USENIX Security Symposium (USENIX Security 21),* 73–90. USENIX Association, elokuu. ISBN: 978-1-939133-24-3. https://www.usenix.org/conference/usenixsecurity21/presentation/ray.

Reichl, Dominik. 2023. “I’ve now implemented two enhancements”, 7. toukokuuta 2023. Viitattu 9. maaliskuuta 2024. https://sourceforge.net/p/keepass/discussion/329220/thread/f3438e6283/#0829.

Security.org. 2021. “Password Manager and Vault 2021 Annual Report: Usage, Awareness, and Market Size”, 6. joulukuuta 2021. Viitattu 22. helmikuuta 2024. https://www.security.org/digital-safety/password-manager-annual-report/2021/.

Security.org. 2023a. “Password Manager Annual Report 2022”, 13. marraskuuta 2023. Viitattu 22. helmikuuta 2024. https://www.security.org/digital-safety/password-manager-annual-report/2022/.

———. 2023b. “Password Manager Industry Report and Market Outlook in 2023”, 13. syyskuuta 2023. Viitattu 22. helmikuuta 2024. https://www.security.org/digital-safety/password-manager-annual-report/2023/.

Siber Systems ja uSamp. 2015. “US and UK Password Practices Leave Users Vulnerable, According to Survey Sponsored by Siber Systems”. Viitattu 9. maaliskuuta 2024. https://www.roboform.com/press-releases/150219-Password-Survey-Final.pdf.

Silver, David, Suman Jana, Dan Boneh, Eric Chen ja Collin Jackson. 2014. “Password Managers: Attacks and Defenses”. Teoksessa *23rd USENIX Security Symposium (USENIX Security 14),* 449–464. San Diego, CA: USENIX Association, elokuu. ISBN: 978-1-931971-15-7. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/silver.

Stobert, Elizabeth ja Robert Biddle. 2018. “The Password Life Cycle”. *ACM Trans. Priv. Secur.* (New York, NY, USA) 21, numero 3 (huhtikuu). ISSN: 2471-2566. https://doi.org/10.1145/3183341.

Toubba, Karim. 2023. “Security Incident Update and Recommended Actions”, 1. maaliskuuta 2023. Viitattu 30. huhtikuuta 2024. https://blog.lastpass.com/posts/2023/03/security-incident-update-recommended-actions.

vdohney. 2023. “KeePass 2.X Master Password Dumper (CVE-2023-32784)”, 17. elokuuta 2023. Viitattu 10. maaliskuuta 2024. https://github.com/vdohney/keepass-password-dumper.

Yan, Jeff, Blackwell Alan, Ross Anderson ja Alasdair Grant. 2004. “Password memorability and security: Empirical results”. *IEEE Security and Privacy* 2 (5): 25–31. ISSN: 15407993. https://doi.org/10.1109/MSP.2004.81.

Zhao, Rui, Chuan Yue ja Kun Sun. 2013. “Vulnerability and risk analysis of two commercial browser and cloud based password managers”. *ASE Science Journal* 1, numero 4 (syyskuu): 1–15.