Tampereen yliopisto

Miikka Mänttäri

MODERNI SALASANANHALLINTA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Toukokuu 2020

TIIVISTELMÄ

Miikka Mänttäri: Moderni salasananhallinta
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Toukokuu 2020

Salasanat ovat olleet käytössä vuosikymmeniä ja ovatkin yksi yleisimpiä ja helpoimpia tapoja toteuttaa käyttäjänvarmennus erilaisiin järjestelmiin. Tämän tutkielman tavoitteena on selvittää, miten salasanoja nykyään käytetään: osaavatko tai viitsivätkö käyttäjät luoda turvallisia salasanoja eri sovelluksiin, ja tietävätkö he mitkä eri salasanan osatekijät vaikuttavat positiivisesti tai negatiivisesti salasanan voimakkuuteen ja arvattavuuteen.

Tutkielma on kirjallisuuskatsaus salasanoihin. Tutkielmassa selvitetään lyhyesti, miksi juuri salasanat ovat ottaneet valta-aseman käyttäjänvarmennuksessa. Tämän jälkeen tarkastellaan, miten salasanoja murretaan: miten niin kutsutut sanakirjalistat, joihin hakkerit keräävät yleisimpiä salasanoja ja niiden osia, toimivat, sekä minkälaisia eroja palvelimeen kohdistetuissa sekä paikallisissa murroissa on. Vaikka salasanojen murto saattaa kuulostaa monimutkaiselta tehtävältä, se useimmiten perustuu kuitenkin vain salasanaehdokkaiden jatkuvaan iterointiin pienin muutoksin, eli käytännössä massa-arvauksiin. Vuodettujen salasanalistojen vaikeimmista salasana-käyttäjätunnus-yhdistelmistä harvoin edes välitetään, koska niin moni käyttäjä luo käyttäjätunnukselleen helposti arvattavan salasanan.

Tutkielma osoittaa, että vaikka salasanat ovat jo pitkään olleet osa päivittäistä kanssakäymistämme eri sovellusten kanssa, käyttäjillä ei ole niiden taustatoiminnasta syvempää tietämystä. Vaikka henkilökohtaiset salasanat tahdotaan suojata ulkopuolisilta, ovat harhaluulot eri suojausmetodeista ja näiden vaikutuksista yleisiä. Toisaalta edes koulutustausta ei suuremmin vaikuta käyttäjien halukkuuteen luoda vahvoja salasanoja, koska myös tietoturva-asiantuntijat suhtautuvat niihin välinpitämättömästi. Usein salasanat nähdään esteenä palvelun käytölle, sen sijaan että ne nähtäisiin tärkeänä turvallisuuden kerroksena.

Tutkielman loppupäässä tarkastellaan, miten käyttäjiä voisi ohjata luomaan turvallisempia salasanoja: kuinka muutama erilainen moderni sovellus tai järjestelmä indikoi käyttäjälle tämän luoman salasanan turvallisuutta, ja minkälaisia rajoitteita sovellusten ylläpitäjät voisivat asettaa – tai poistaa – sovellusten vaatimilta salasanoilta. Tutkielma päätetään yleispäteviin vinkkeihin: kuinka kuka tahansa voi luoda turvallisempia salasanoja, sekä miten salasanojen hallinnassa kannattaisi siirtyä käyttämään salasananhallintaohjelmia. Salasananhallintaohjelma tallentaa käyttäjän puolesta kaikki paitsi ohjelmaan kirjautumiseen käytetyn salasanan, mahdollistaen tehokkaan ja turvallisen salasanankäytön äärettömän monen ohjelman ja sovelluksen välillä.

Avainsanat: Salasana, tietoturva, salasanaturvallisuus, salasanakäytännöt, salasananhallinta

Sisällysluettelo

1 Johdanto

Salasanat ja näitä käyttävät ihmiset ovat tietoturvan heikko lenkki. Liian lyhyet ja palvelusta toiseen toistetut salasanat heikentävät järjestelmien ja käyttäjien tietoturvaa suuresti. Tässä tutkielmassa syvennytään salasanojen murtoon, käyttäjien salasanamielipiteisiin, sekä tekijöihin, jotka heikentävät ja vahvistavat salasanojen voimakkuuksia. Lopuksi käydään läpi katsaus, miten normaalin käyttäjän olisi mahdollista parantaa omaa salasanaturvallisuuttaan luomalla vahvempia ja muistettavampia salasanoja tai ottamalla käyttöönsä salasananhallintaohjelmia.

Salasanoissa on tietoturvan kannalta suuri riski: käyttäjät ovat harvoin kekseliäitä salasanojensa luonnissa. Vaikka palveluun luotaisiinkin uusi salasana, se on joko vain hieman muokattu versio aikaisemmista salasanoista, sisältää joitain viitteitä käytettävään palveluun, tai sisältää yleisiä merkki- ja numerosarjoja tai näiden korvaavuuksia, jotka näennäisesti vaikuttavat lisäävän salasanaturvallisuutta, mutta oikeasti osataan hakkereiden toimesta kiertää. Esimerkiksi ”o”-kirjaimen korvaaminen ”0”-numerolla ei sanakirjaa käyttävissä yleisimmissä salasananmurto-ohjelmissa lisää turvallisuutta ollenkaan.

Tutkielma on kirjallisuuskatsaus yleisimpiin salasananmurtomenetelmiin, käyttäjien käsityksiin salasanojen turvallisuudesta ja niiden murtamisesta sekä toimiin, mitä erilaiset palvelut ja organisaatiot ovat tehneet parantaakseen ja huonontaakseen salasanojen turvallisuutta. Tutkielmassa katsastetaan, minkälaisia yhtäläisyyksiä ja toisaalta väärinkäsityksiä käyttäjien ja tietomurtajien väliltä löytyy, ja onko näissä käsityksissä tietoturvan kannalta jotain vaarallista.

Tutkielman toisessa luvussa tutustutaan tietoturvan historiaan ja siihen, miten salasanat ovat päätyneet nykyiseen valta-asemaansa. Kolmannessa luvussa tutustutaan salasanojen murron taustoihin, mistä ja miten salasanoja murretaan. Neljännessä luvussa tutustutaan käyttäjien tietoisuuteen salasanojen heikkouksista ja näiden murroista, minkälaisia väärinkäsityksiä käyttäjillä saattaa salasanoja ja näiden murtamista kohtaan olla. Viidennessä luvussa käyn läpi, miten järjestelmät ja palveluiden tuottajat yrittävät ohjata käyttäjiä luomaan oikeaoppisia salasanoja, ja kuinka nämä ohjeistukset voivat itse asiassa ohjata käyttäjiä harhaan. Kuudennessa luvussa pohditaan, miten kuka tahansa pystyisi parantamaan omaa salasanaturvallisuuttaan, ja luomaan muistettavamman ja tietoturvallisemman salasanan. Kuudennessa luvussa käydään myös pienimuotoinen katsaus salasananhallintaohjelmiin.

Salasanat ovat oikeastaan aina olleet käyttäjien varmennuksen suosituin tapa: salasanvarmennus on helppoa ja halpaa ottaa järjestelmään käyttöön, ovat useimmille käyttäjille tuttuja, ovat helposti liikuteltavista paikasta toiseen, eivätkä vaadi käyttäjää

luovuttamaan biometrisiä tietojaan, kuten sormenjälkiään, sovelluksien haltuun (Biddle et al. 2012). Toisaalta salasanoissa on myös lukuisia ongelmia: käyttäjät harvoin luovat käyttämiinsä palveluihin tietoturvallisia salasanoja, ja vaikka luotu salasana olisikin vahva, sitä usein uudelleen käytetään eri palveluiden välillä, altistaen käyttäjän kaikki käyttäjätunnukset yhden palvelun tietomurron tapahtuessa (Ji et al. 2017). Vaikka salasanoja on käytetty käyttäjänvarmennukseen jo vuosikymmeniä, ei niihin ole koskaan viitsitty täysin panostaa: käyttäjillä esiintyy vaarallisia harhaluuloja sekä välinpitämättömyyttä omia salasanojaan kohtaan, vaikka henkilökohtaisen salasanan takana voi olla runsaasti henkilökohtaista dataa.

2 Miten salasanoja murretaan

Sivustoilta vuodetut salasanat ovat nykyään yleensä suojattu jonkinlaisella hajautusalgoritmilla, joka takaa sen, että sivustolta vuodettua salasana-käyttäjätunnus-yhdistelmää ei pääse suoraan väärinkäyttämään muihin palveluihin, vaan vuodettu salasana pitää ensin hajautusalgoritmin pohjalta murtaa. Palveluihin rekisteröityessä käyttäjän on mahdotonta tietää käytössä olevaa hajautusalgoritmia, tai edes onko sellaista käytössä ollenkaan, joten jokaiseen palveluun pitäisi suhtautua yhtä isona tietoturvariskinä. Edes suuriin teknologia-alan yrityksiin ei voi täysin sokeasti luottaa: esimerkiksi Facebook (2019) ilmoitti vuonna 2019 löytäneensä satoja miljoonia suojaamattomia salasanoja sisäisestä tietokannastaan.

Hajautusalgoritmiksi (hashing algorithm) kutsutaan algoritmia, joka muuttaa käyttäjän syöttämän salasanan, oli tämä sitten selkokielinen tai esimerkiksi pelkkä satunnainen merkkijono, oletuspituiseksi ”satunnaiseksi” merkkijonoksi tietyin kriteerein. Hajautusalgoritmin ideana on, että se on ikään kuin yksisuuntainen kone: Siihen voi syöttää salasanan, mutta hajautusalgoritmista saatua merkkijonoa ei voi enää syöttää takaisin algoritmiin ja saada salasanaa. Hajautusalgoritmien ideana on parantaa selkokielisten salasanojen tietoturvaa. (Das et al. 2014)

2.1 Väsytyshyökkäykset

Väsytyshyökkäyksillä pystytään yleensä murtamaan vain huonolla suojausalgoritmilla tai kokonaan suojaamattomat salasanat. Väsytyshyökkäyksessä käyttäjän salasanaa koitetaan arvata merkki kerrallaan muuttamalla ja lisäämällä niin pitkään, kunnes salasana murtuu. Nykyaikaiset salasananmurto-ohjelmat pystyvät tekemään jopa miljardeja arvauksia sekunnissa käytetystä hajautusalgoritmista riippuen (Ur et al. 2016),

joten heikkojen salasanojen kohdalla murto on mahdollista jo pelkällä raa'alla arvausvoimalla.

Väsytyshyökkäyksiä vastaan puolustautuminen toimii helpoiten pidentämällä salasanan merkkipituutta: koska kone joutuu jokaisen uuden merkin kohdalla käymään koko aakkoston yksi kerrallaan läpi, eikä myöskään aikaisempien merkkien oikeellisuutta voida tietää ennen kuin koko salasana on murrettu, salasanan arvaamiseen tarvittu teho nousee eksponentiaalisesti jokaisen uuden merkin kohdalla (Ji et al. 2017).

2.2 Sanakirjahyökkäykset

Sanakirjahyökkäykset perustuvat aikaisemmin vuodetuista salasanoista ja kohdekielen yleisimmistä sanoista kerättyihin sanakirjoihin. Suuria hyökkäyksiä varten sanakirjoja voidaan kerätä jopa tilannekohtaisesti (Ji et al. 2017). Hyökkäys perustuu samanlaiseen massa-arvaamiseen kuin väsytyshyökkäykset, mutta arvauksien määrää rajoitetaan sanakirjaan perustuvilla parametreilla. Esimerkiksi maailman yleisimmän salasanan, ”password”, jokainen variaatio murtuu sanakirjahyökkäyksillä sekunneissa. Hyökkäysohjelmat osaavat käytetyimmät kirjain- ja numerosubstituutit, kuten esimerkiksi ”A”-kirjaimen vaihtaminen numeroksi ”4”. (Ji et al. 2017)

Sanakirjahyökkäyksiä vastaan puolustautuminen ei ole läheskään yhtä helppoa, kuin väsytyshyökkäyksiä vastaan. Hakkerien käyttämiä sanakirjalistoja ei voi tietää ennakkoon, ja ne saattavat sisältää myös muista murretuista järjestelmistä johdettua dataa (Das et al. 2014). Sanakirjahyökkäyksiä käytetään usein väsytyshyökkäysten tukena, vähentäen näihin tarvittavaa tietokoneen laskennallista kykyä.

2.3 Palvelinhyökkäykset

Tässä kontekstissa palvelinhyökkäyksillä tarkoitetaan erilaisia verkkopalvelimiin kohdistuvia satunnaisia salasanojen arvausyrityksiä. Suurin osa verkkopalveluista rajoittaa käyttäjiin kohdistettuja salasanojen arvausyrityksiä esimerkiksi väliaikaisesti lukitsemalla käyttäjien tilejä. Samoin useat SSH-suojatut välityspalvelimet estävät samasta lähteestä tulevat uudet salasananratkaisuyritykset tietyn rajan jälkeen (Kakarla et al. 2018). Palveluun rekisteröityessä käyttäjä ei kuitenkaan voi lähes koskaan tietää minkälainen suojaus järjestelmällä on murtoyrityksiä vastaan, joten jokaiseen uuteen palveluun ja järjestelmään tulisi luoda mahdollisimman turvallinen salasana.

2.4 Vuodetut salasanalistat

Palvelinhyökkäyksiin verrattuna vaihtoehtoinen tapa murtaa salasanoja on vuodettujen, mutta hajautettujen salasana-käyttäjätunnus-yhdistelmien murtaminen paikallisesti hakkerin omalla tietokoneella. Useimmiten eri palveluista vuodetut käyttäjätaulut on suojattu jollain tavoin, eikä salasanoja ole tallennettu vain selkokielisenä järjestelmään

(Ji et al. 2018). Tämäkin tyyli perustuu useisiin erilaisiin salasanan arvausyrityksiin, joissa salasana-arvauksia ajetaan hajautusalgoritmista läpi, yrittäen saada palautuksena sama hajautettu merkkijono kuin vuodetulla käyttäjätunnuksella (Bosnjak et al. 2018).

Samassa tutkimuksessa Bosnjak ja muut (2018) huomasivat, että jopa 95% tutkimuksessa olleista Slovenialaisen yliopiston opiskelijoiden entisistä salasanoista saatiin murrettua normaalilla kuluttajille saatavilla olevalla näytönohjaimella muutamassa päivässä. Tutkijat päätyivät antamaan vain 0.5 %:lle testinä olleista salasanoista murtovarman luokittelun.

3 Käyttäjien suhtautuminen salasanoihin

Useiden tutkimusten mukaan (Ur et al. 2016; Duggan et al. 2012; Florencio & Herley 2007) käyttäjät jollain tasolla tiedostavat huonojen salasanakäytäntöjen riskit. Salasanoista tiedostetaan esimerkiksi, ettei niitä kannattaisi uudelleenkäyttää sivustojen ja palveluiden välillä (Duggan et al. 2012), mutta tätä tietoa ei hyödynnetä, tai edes ymmärretä hyödyntää uusiin järjestelmiin rekisteröityessä tai vanhojen järjestelmien salasanoja vaihtaessa. Usein salasanana tai sen pohjana käytetään jotain vanhaa salasanaa (Han et al. 2018; Florencio & Herley 2007), jolloin molempien salasanojen ja näiden takana olevien järjestelmien tietoturva heikentyy suuresti. Das ja muut (2014) huomasivat tutkimuksessaan, että noin 43-51 prosenttia internetin käyttäjistä uudelleenkäyttää salasanojaan eri palveluiden välillä. Dugganin ja muiden (2012) tutkimuksen mukaan yksi syy tälle tietoturvan kannalta ristiriitaiselle toiminnalle on se, että käyttäjät näkevät järjestelmien salasanat esteenä järjestelmän tai palvelun käytölle. Salasanoja ei siis koeta yhtenä turvallisuuden kerroksena, kuten vaikkapa fyysiset ovien lukitukset koetaan, vaan salasanat nähdään hidasteena toiminnoille joita sivustolle tai palveluun tullaan suorittamaan.

3.1 Teknisten ja ei-teknisten käyttäjien erot salasanakäytänteissä

Oikeaoppisen salasanaturvallisuuden laiminlyöminen ei rajoitu pelkkiin ei-teknisiin käyttäjiin, vaan Stobertin ja Biddlen (2018) mukaan myös tietoturvaekspertit suhtautuvat osaltaan laiminlyövästi salasanoihin. Käyttäjät koulutuksesta tai taustastaan huolimatta usein luokittelevat salasanoja erilaisiin luokkiin: esimerkiksi ”merkityksettömiksi” luokitellut järjestelmät ja salasanat ovat sellaisia, joihin ulkopuolisen pääsy ei haittaisi käyttäjää itseään suuresti. Näihin järjestelmiin käyttäjät usein uudelleenkäyttävät jotain yleistä salasanapohjaa tai salasanaansa, jolloin pahimmassa tapauksessa yhden ”merkityksettömän” järjestelmän tietomurto vaarantaa kaikki merkityksettömät tunnukset. (Stobert & Biddle 2018)

Omasta mielestään merkityksellisiin järjestelmiin, kuten esimerkiksi verkkopankkeihin ja henkilökohtaisiin terveysjärjestelmien tunnuksiin, käyttäjät pyrkivät usein luomaan turvallisen salasanan. Palveluiden sisältämä henkilökohtainen data ja käsittelymahdollisuus omaisuuteen nähdään suurena riskinä, jolta halutaan suojautua. Useiden eri tutkimusten perusteella käyttäjät pyrkivät luomaan yksilöllisiä ja mielestään turvallisia salasanoja näihin järjestelmiin. (Duggan et al. 2012; Florencio & Herley 2007; Stobert & Biddle 2018)

3.2 Yleisiä väärinkäsityksiä salasanoista

Kuten aiemmin on mainittu, erilaisten palveluiden käyttäjät eivät tarkoituksellisesti luo helposti murrettavia salasanoja. Vaikka laiskuudella ja välinpitämättömyydellä on oma osuutensa käyttäjien löyhään suhtautumiseen salasanoja kohtaan (Duggan et al. 2012; Ur et al. 2016), niin myös erilaiset väärinkäsitykset ja harhaluulot salasanojen näennäisestä turvallisuudesta johdattavat käyttäjiä harhaan. Esimerkiksi erilaiset numerosubstituutit, kuten ”A”-kirjaimen vaihtaminen ”4”-numeroksi, nähtiin tietoturvallisuutta parantavana toimena Urin ja muiden tutkimuksessa (2016), vaikka oikeasti modernit salasananhallintaohjelmat osaavat nämä substituutit kiertää, kuten luvussa 3 huomattiin. Myös näppäimistösarjojen, esimerkiksi ”asdfgh”, turvallisuus luokiteltiin osallistujien toimesta liian korkeaksi, koska koneellisesti loogisesti etenevät sarjat on helppo murtaa. (Ur et al. 2016)

Toisaalta tutkimuksessa huomattiin myös, että käyttäjät eivät luo salasanojaan aivan satunnaisesti: esimerkiksi merkkien määrän nostaminen koettiin lähes aina nostavan salasanan turvallisuutta. Kuitenkin, vaikka käyttäjät usein tiesivät esimerkiksi syntymäpäivien sisällyttämisen salasanaan olevan haitallista, monet tutkimukseen osallistujat myönsivät käyttävänsä epäturvallisia käytäntöjä luodessaan uusia salasanoja. (Ur et al. 2016)

Ur ja muut tutkijat (2016) huomasivat myös, että mitä ”turvallisemmaksi” tutkimuksen osallistujat luokittelivat salasanan, sitä ”vaikeammaksi” sen muistettavuus luokiteltiin. Esimerkiksi salasananhallintaohjelman luoma satunnainen merkkijono luokiteltiin turvalliseksi salasanaksi kaikkien osallistujien toimesta, mutta sen muistettavuuteen osallistujat eivät luottaneet. Toisaalta Woodsin ja Siposen (2017) tutkimuksen perusteella ihmisen muistikapasiteetti, tai tämän puute esimerkiksi huonomuististen kohdalla, ei yksinään selitä aiemmin mainittuja huonoja salasanaperiaatteita. Tutkimuksen perusteella jo ajatus salasanan unohtamisesta saa alitajunnassa aikaan ketjureaktion, jossa ihminen ennemminkin kuvittelee unohtaneensa salasanan, kuin oikeasti unohtaa sen. Tarvittaessa, ja itseensä uskoessa, Woods ja Siponen (2017) uskovat, että ihmisen olisi mahdollista muistaa nykyistä paljon enemmän

salasanoja erilaisiin järjestelmiin, vähentäen tarvetta uudelleenkäyttää salasanoja palveluiden välillä.

4 Käyttäjien ohjaaminen turvallisempiin salasanoihin

Tässä luvussa kuvailen kaksi eri tapaa ohjata käyttäjiä tekemään turvallisempia salasanoja. Ensimmäinen tapa, salasanojen voimamittarit, ovat rekisteröitymisvaiheen avustimia uusille käyttäjille, jotka aktiivisesti kuvaavat syötetyn salasanan mahdollista tietoturvan määrää. Toinen tapa ohjata käyttäjiä luomaan turvallisempia salasanoja on asettaa syötetylle salasanalle erilaisia rajoitteita: yleisiä rajoitteita ovat esimerkiksi tietty pituus ja vaatimus sille, että salasana sisältää normaalin aakkoston lisäksi erikoismerkkejä.

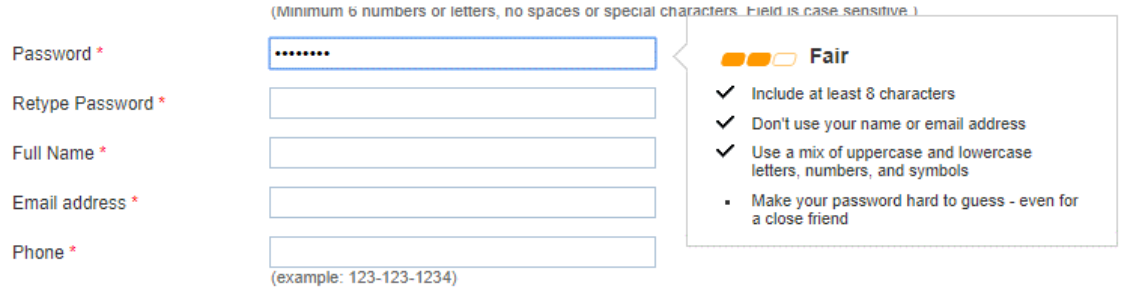
Salasanojen entropiaa (entropy) voidaan kutsua tässä kontekstissa salasanojen murtoon käytetyksi ajaksi. Entropiallisesti raskaat salasanat ovat hitaita murtaa ohjelmistollisesti, kun taas entropiallisesti kevyet salasanat saattavat murtua jopa muutamassa sekunnissa. Entropiaan vaikuttaa salasanan pituuden lisäksi myös sen kompleksisuus ja yleisyys: esimerkiksi eri kielien yleisimmät sanat eivät vahvista salasanan entropiaa, koska ne on kirjattu erilaisiin sanakirja -yhdistelmiin, joita hyökkääjät käyttävät yrittäessään murtaa salasanoja. (de Carné de Carnavalet & Mannan 2015)

4.1 Salasanojen voimamittarit

Useiden eri palveluiden rekisteröitymisvaiheessa on käytössä niin sanotut salasanojen voimamittarit (password strength meter), jotka reaaliaikaisesti kuvaavat käyttäjälle tämän syöttämän salasanan entropiallista voimakkuutta. Salasanan voimakkuutta kuvataan usein joko värein (vihreä, keltainen, punainen) tai sanoin (voimakas, keskiverto, heikko), tai näiden yhdistelmänä. Salasanan voimamittarin ”voimakas”- lopputulos ei kuitenkaan ole yksinään tae turvallisesta salasanasta, ja mittarit saattavat pahimmassa tapauksessa johtaa käyttäjiä harhaan antamalla liian vahvoja tuloksia liian heikoille salasanoille tai painottamalla vääriä asioita salasanasyötteessä. (de Carné de Carnavalet & Mannan 2015)

Kuvassa 1 on syötetty salasanakenttään merkkijono ”1234abcd”, jota järjestelmä kuvaa keskiverroksi tai kohtuulliseksi salasanaksi. Oikeasti kyseisen merkkijonon pystyisi, järjestelmässä käytetystä tietojentallennusratkaisusta riippuen, murtamaan sekunneissa, kuten luvussa 3 käytiin läpi. Käyttäjää yritetään kyllä ohjailla luomaan oikeaoppinen salasana kieltämällä oman nimen tai sähköpostitunnuksen käyttö, mutta

erikoismerkkien, numeroiden ja isojen sekä suurien kirjaimien niputtaminen yhteen kohtaan luo vääränlaista turvallisuudentunnetta käyttäjälle.



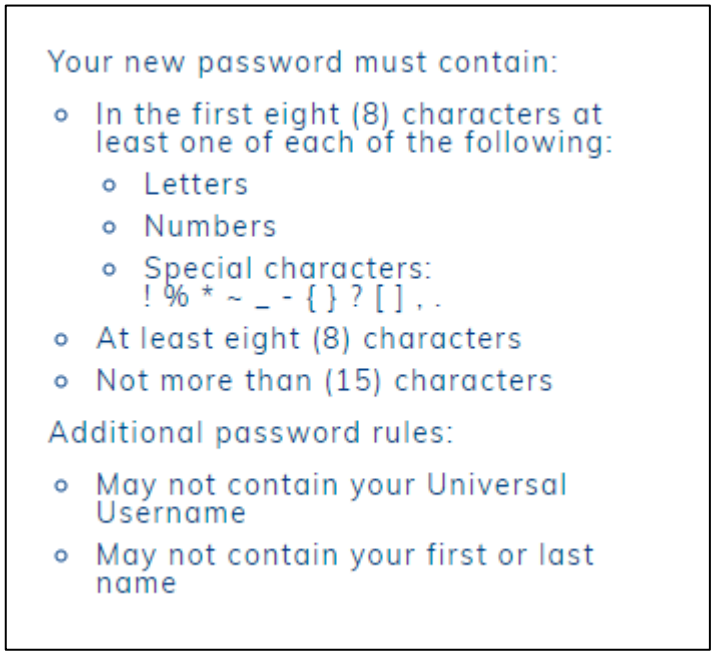
Kuva 1. Kuvakaappaus PayPal.com-rahansiirtosivuston (2020) rekisteröitymissivustolta, kun salasanaksi on syötetty 1234abcd.

Toisaalta salasanojen voimamittareita ei ole luotu tarkoituksellisesti ohjaamaan käyttäjiä harhaan, vaan tarkoituksena olisi saada käyttäjät luomaan turvallisempia salasanoja. Mittareiden jatkuvalla jatkokehityksellä niistä voidaan luoda hyödyllinen osa käyttäjien ja palveluiden tietoturvaa. Voimamittareita tutkineet Alqahtani ja muut (2019) huomasivat, että myös käyttäjien omat mielipiteet syötetyn salasanan turvallisuudesta vaikuttivat voimamittareihin luottamiseen: omasta mielestään ”turvallisen” salasanan luoneet käyttäjät eivät luottaneet voimamittarin tulokseen yhtä paljon, kuin satunnaisen salasanan saaneet käyttäjät.

Salasanojen voimamittareiden ulkomuodon muutoksilla voidaan myös ohjata käyttäjiä luomaan turvallisempia salasanoja. Yksinkertaisen kuvassa 1 esitellyn voimamittarin sijaan esimerkiksi emojeilla ja syötetyn salasanan parannusvinkkien antamisella käyttäjiä voidaan hienovaraisesti ohjata luomaan turvallisempia salasanoja (Furnell et al. 2018).

4.2 Salasanarajoitteet

Useilla verkkosivustoilla on käytössä erilaisia rajoitteita salasanojen luontiin, joilla koitetaan varmistaa ja ohjata käyttäjiä tekemään turvallisempia salasanoja. Kuvan 2 salasanarajoitteet on kaapattu Western Washington Universityn verkkosivuilta. Rajoitteita tehdessä on kuitenkin huomioitava, että liian tarkat ja rajoittavat salasanaparametrit itse asiassa auttavat hyökkääjiä murtautumaan järjestelmiin, koska hakkerit pystyvät tarkemmin rajaamaan salasanojen murtoon tarkoitetun sanakirjansa. Esimerkiksi kuvan 2 rajoitteista mahdollinen hakkeri voi poimia kustomoituun sanakirjaansa salasanan minimi- ja maksimipituuden sekä kaikki salasanassa mahdollisesti sallitut merkit.



Kuva 2. Western Washington University -yliopiston (2019) salasanaohjeistus uutta käyttäjää luodessa.

Vaikka liian rajoittavat salasanarajoitteet ja ehdot voivat vaikuttaa tietoturvaan negatiivisesti, niin tilanne ei useimmiten ole tämä. Oikein laadituilla rajoitteilla pystytäänkin lisäämään salasanan murtoon vaadittua entropiaa runsaasti: esimerkiksi erikoismerkkien ja pienten sekä suurten kirjaimien pakottaminen salasanaan nostaa salasanassa mahdollisesti käytettyä merkkien määrää jo suuresti, joka taas osaltaan voimistaa salasanan entropiaa (Ji et al. 2017). Koska suurin syy turvattomaan salasanojen luontiin on käyttäjien laiskuus ja tietämättömyys salasanojen voimakkuuden aiheuttajista, niin jopa tietämättömät ja laiskat käyttäjät voidaan ikään kuin ”pakottaa” käyttämään turvallisia salasanoja rajoittamalla näitä oikein (Furnell et al. 2018).

5 Hyvän salasanan piirteet

Hyvä salasana on samaan aikaan koneellisesti vaikea murtaa, ja käyttäjän helppo muistaa. Paradoksilta kuulostava lause ei kuitenkaan täysin ole sitä: koneellisessa salasananmurrossa haetaan usein suurien vuodettujen salasanalistojen heikoimpia lenkkejä (Ji et al. 2017), joten laskennallisesti raskaat salasanat saatetaan jopa jättää kokonaan huomiotta.

5.1 Salasanojen merkkipituus tärkeimpänä suojana

Useat eri tutkimukset (Bosnjak et al. 2018; Florencio & Herley 2007; Han et al. 2018; Ji et al. 2017; Ur et al. 2016) ovat päätyneet salasanojen luonnissa samaan lopputulokseen:

mitä enemmän merkkejä salasana sisältää, sitä vaikeampi se on murtaa. Salasanoja luodessa on kuitenkin hyvä muistaa, että tietyt usein käytetyt kirjain- ja numerosarjat eivät paranna salasanan turvallisuutta lähes ollenkaan: esimerkiksi merkkijono ”abcd” tai numerojono ”1234” parantavat salasanan turvallisuutta vain hyvin marginaalisesti (Ur et al. 2016). Mainitussa tavassa luoda salasanoja on kuitenkin pidettävä mielessä sen heikkous: sanakirjalistoilla jopa nämä kirjain-/numerosubstituutit on mahdollista huomioida ja kiertää, jos käyttäjältä on esimerkiksi aiemmin vuotanut salasana verkkoon (Han et al. 2018; Ji et al. 2017).

5.2 Salasananhallintaohjelmat

Sen sijaan, että käyttäjä koettaisi luoda ja muistaa manuaalisesti jokaiseen käyttämäänsä palveluun murtovarmaa salasanaa, joka on todella vaikeaa, ellei jopa mahdotonta, käyttäjien tulisi tietoturvaeksperttien mukaan ottaa käyttöönsä mahdollisimman laajasti jokin salasananhallintaohjelma (Ur et al. 2016).

Faganin ja muiden (2017) tutkimuksen mukaan salasananhallintaohjelmia jo nykyään käyttävillä käyttäjillä ohjelmaa ei otettu käyttöön sen turvallisuuden vuoksi, vaan ensisijainen painoarvo oli ohjelman helppokäyttöisyydellä. Taas sivutaan siis luvussa 4 mainittua käyttäjien ”laiskuutta” omia salasanojaan kohtaan. Salasanoja, tai salasananhallintaohjelmia, ei siis nähdä osana henkilökohtaista tietoturvaa, vaan ennemminkin hidasteena palveluiden käytölle. Samassa tutkimuksessa Fagan ja muut (2017) kysyivät salasananhallintaohjelmia käyttämättömiltä käyttäjiltä syitä tähän: suurimpana tekijänä salasananhallintaohjelmien käyttämättömyyteen paljastui käyttäjien epäilykset ohjelmien turvallisuudesta: Salasananhallintaohjelmien taustalla olevaa toimintaa ei ymmärretty, jolloin myöskään ohjelmiin ei uskallettu tai osattu luottaa.

Yleisesti eri salasananhallintaohjelmien toimintaperiaate on samanlainen: sovellukseen kirjaudutaan yhdellä yleissalasanalla, ja sovellus tallentaa kaikki käyttäjän muut salasanat omaan, hajautetusti suojattuun salasanatietokantaan. Sovellukset voivat tarkkailla, ettei käyttäjällä ole eri sivustoilla samaa salasanaa käytössä, ja ne tarjoavat rekisteröinti- tai salasananvaihtovaiheessa palveluihin vahvoja salasanoja. Tarkoituksena on poistaa käyttäjältä tarve muistaa lukuisia eri salasanoja, ja tallentaa jo olemassa olevat salasanat tietoturvallisesti joko käyttäjälle lokaalisti tai salasananhallintaohjelman palvelimille: esimerkiksi LastPass -ohjelma tallentaa salasanat omalle palvelimelleen, kun taas KeePass -ohjelma tallentaa salasanat käyttäjän omalle laitteelle eräänlaiseen tietokantaan. Salasananhallintaohjelmat käyttävät salasanojen turvaamiseen vahvoja hajautusalgoritmeja, jotka ovat vaikeita tai jopa mahdottomia murtaa ilman tietämystä ohjelman yleissalasanasta. (Price, 2017)

6 Yhteenveto

Tärkein asia omaa salasanaturvallisuutta tarkastellessa on salasanan merkkipituus: koska jokainen lisämerkki tuottaa salasanoja murtavalle tietokoneelle runsaasti lisää läpikäytävää entropiaa, eli vaadittujen arvauskertojen määrä nousee, olisi käyttäjien hyvä luoda mahdollisimman pitkiä salasanoja eri palveluihin. Toinen tärkeä aspekti salasanaturvallisuudessa on välttää salasanojen uudelleen käyttöä eri palveluiden ja järjestelmien välillä: jos yksi salasanasi vuodetaan verkkoon, niin kaikki samaa salasanaa käyttävät palvelut ovat murtoriskin alla. Vuodetuista salasanoista hakkerit voivatkin kasata erilaisia sanakirjalistoja, joilla voidaan kohdentaa murtoyrityksiä esimerkiksi tiettyihin käyttäjiin.

Vaikka useat käyttäjät jollain tasolla tiedostavatkin heikkojen salasanojen tuomat riskit, näihin ei viitsitä tai osata reagoida kunnolla. Usein salasanat nähdään esteenä palveluiden käytölle, sen sijaan että ne miellettäisiin hyödyllisenä turvallisuuden kerroksena. Käyttäjillä on myös runsaasti väärinkäsityksiä siitä, mikä tuottaa salasanaan lisää tietoturvaa ja mikä heikentää sitä: esimerkiksi tunnettujen kirjainyhdistelmien, kuten ”asdf” tai ”password” käyttö on salasanoissa todella yleistä.

Käyttäjien tekninen tietämys harvoin vaikuttaa salasanojen käyttöön. Niin tietoturvan asiantuntijat kuin peruskäyttäjätkin käyttävät paljon turvattomia salasanoja, eikä suhtautuminen salasanojen käyttöön vaihtele runsaasti eri käyttäjäkuntien välillä. Osa käyttäjistä kuitenkin pyrkii turvaamaan mielestään tärkeät palvelut, kuten esimerkiksi verkkopankit, uniikeilla salasanoilla.

Koska salasanoja vaativia palveluita on nykyään runsaasti, suositellaan käyttäjille salasananhallintaohjelmien käyttöönottoa. Ohjelman avulla käyttäjän ei tarvitsisi muistaa kuin yksi pääsalasana, jonka avulla pääsee kirjautumaan sovellukseen, ja sovellus muistaisi muut salasanat käyttäjän puolesta. Sovelluksien avulla on myös helppo luoda pitkiä ja turvallisia salasanoja ja tallentaa ne turvallisesti hajautettuna joko käyttäjän omalle laitteelle tai sovelluksen palvelimille.

7 Lähdeluettelo

Alqahtani, S., Li, S., Yuan, H., & Rusconi, P. (2019). Human-Generated and Machine-Generated Ratings of Password Strength: What Do Users Trust More? ICST Transactions on Security and Safety, 6(21), 162797. https://doi.org/10.4108/eai.13-7-2018.162797

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44(4), 1–42. https://doi.org/10.1145/2333112.2333114

Bosnjak, L., Sres, J., & Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 - Proceedings, 1161–1166. *https://doi.org/10.23919/MIPRO.2018.8400211*

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The Tangled Web of Password Reuse. February, 23–26. https://doi.org/10.14722/ndss.2014.23357

De Carné De Carnavalet, X., & Mannan, M. (2015). A large-scale evaluation of high-impact password strength meters. *ACM Transactions on Information and System Security*, *18*(1). https://doi.org/10.1145/2739044

Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human Computer Studies*, *70*(6), 415–431. https://doi.org/10.1016/j.ijhcs.2012.02.008

Facebook. (2019). *https://newsroom.fb.com/news/2019/03/keeping-passwords-secure/* haettu 28.02.2020

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. Human-centric Computing and Information Sciences, 7(1). https://doi.org/10.1186/s13673-017-0093-6

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *16th International World Wide Web Conference, WWW2007*, 657–666. *https://doi.org/10.1145/1242572.1242661*

Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. Computers and Security, 75, 1–9. https://doi.org/10.1016/j.cose.2018.01.016

Han, W., Li, Z., Ni, M., Gu, G., & Xu, W. (2018). Shadow Attacks Based on Password Reuses: A Quantitative Empirical Analysis. *IEEE Transactions on Dependable and Secure Computing*, *15*(2), 309–320. https://doi.org/10.1109/TDSC.2016.2568187

Hunt, T. (2017). Password reuse, credential stuffing and another billion records in Have I been pwned. https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned/ . haettu 28.2.2020

Ji, S., Yang, S., Hu, X., Han, W., Li, Z., & Beyah, R. (2017). Zero-Sum Password Cracking Game: A Large-Scale Empirical Study on the Crackability, Correlation, and Security of Passwords. *IEEE Transactions on Dependable and Secure Computing*, *14*(5), 550–564. https://doi.org/10.1109/TDSC.2015.2481884

Kakarla, T., Mairaj, A., & Javaid, A. Y. (2018). A Real-World Password Cracking Demonstration Using Open Source Tools for Instructional Use. IEEE International Conference on Electro Information Technology, 2018-May, 387–391. *https://doi.org/10.1109/EIT.2018.8500257*

Paypal.com. (2020). *https://www.paypal.com/welcome/signup/#/email_password*. Haettu 15.3.20

Price, R. (2017). Password managers are an essential way to protect yourself from hackers — here's how they work. *https://www.businessinsider.com/how-to-use-password-manager-store-protect-yourself-hackers-lastpass-1password-dashlane-2017-2?r=US&IR=T*. Haettu 17.5.20

Stobert, E., & Biddle, R. (2018). The password life cycle. *ACM Transactions on Privacy and Security*, *21*(3). https://doi.org/10.1145/3183341

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). Do users' perceptions of password security match reality? *Conference on Human Factors in Computing Systems - Proceedings*, 3748–3760. *https://doi.org/10.1145/2858036.2858546*

Western Washington University. (2019). *https://www.wwu.edu/*. Haettu 22.9.19

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human Computer Studies*, *111*(March 2017), 36–48. https://doi.org/10.1016/j.ijhcs.2017.11.002