Salainen, julkinen
kumpaa salasanasi on?

Kenneth Kahri
Tietotekniikkaosasto

Salasanan tulisi olla kuin kotiavain, jota ei luovuteta kenelle tahansa. Silti ihmiset käsittelevät salasanojaan luvattoman huolimattomasti.

Tietotekniikka-asioiden parissa työskentelevänä kohtaa salasanoihin liittyen monenmoista tottumusta ja toimintatapaa. On pitkää, pätkää, yksinkertaista ja ylivaikeaa. Synkempää on silloin, kun asiasta tulee puhe. Tällöin nimittäin jokin on järjestään vialla. Yleensä selvitään vähällä, salasanaa ei ole muistettu vaihtaa ennen sen vanhenemista tai salasana on vain unohtunut. Harvemmin, mutta tasaisin väliajoin, joudutaan selvittelemään kiharaisempia tapauksia: heikkoja salasanoja ja niiden väärinkäyttöä. Suurimmassa osassa tapauksista perimmäinen syy on ollut halu selvitä helpolla ja käyttää erittäin yksinkertaista salasanaa; säästetty vaiva on lähinnä minimaalinen, kun ottaa huomioon, että käyttäjätunnuksen omistaja on aina vastuussa tunnuksellaan tehdyistä asioista ja väärinkäyttö vaikuttaa aina kaikkiin muihinkin käyttäjiin.

Salasanoja on nykyään meillä kaikilla, siitä ei pääse yli eikä ympäri. Niitä on sähköpostiin, verkkopankkiin, pikaviestimiin, keskustelupalstoille ja vaikka minne. Kirjaudumme salasanalla niin moneen paikkaan, että se sujuu jo liki huomaamatta. Tämä ei ole mennyt ohi myöskään yhteiskunnan arveluttavammilta jäseniltä, kuten Nordean verkkopankkiasiakkaisiin kohdistunut tunnusten kalastelu tai käyttäjien vakoiluun erikoistuneet virukset osoittavat. Käyttäjätunnukset ovat rahanarvoista kauppatavaraa, joten jokainen meistä on kiinnostuksen kohteena.

Salasanoihin ja muuhukin sähköiseen tunnistamiseen liittyvä kulttuuri ei ole vielä ehtinyt syntyä eikä asettua luontevaksi osaksi jokapäiväistä elämää, joten emme ole omaksuneet sopivanlaista asennetta salasanojamme kohtaan. Tästä johtuen moni tekee salasanallaan asioita, joita ei tekisi kotiavaimillaan; analogia ei loppujen lopuksi ole kovin kaukana todellisuudesta, salasana on avain siihen lukkoon, jolla pidetään asiattomat poissa käyttäjän verkkopankista, sähköpostista ja muista henkilökohtaisista paikoista. Vai antaisitko kotiavaimesi satunnaiselle vastaantulijalle vain koska hän keksisi niitä pyytää? Tai suostuisitko lukitsemaan kotisi lukolla, jonka osaa auki kahvasta kääntämällä kuka vain? Lukoilla on väliä ja niin on salasanoillakin – yksinkertainen on pahasta, kun halutaan suojella jotakin arvokasta.

Millainen salasana?

Jotta salasanasta olisi todellista hyötyä, pitää sen olla riittävän monimutkainen. Toki monimutkainenkaan salasana ei ole täysin murtamaton. Oikea merkkiyhdistelmä on mahdollista arvata kokeilemalla läpi kaikki vaihtoehdot yksi kerrallaan; tarkoitus onkin tehdä arvaamisesta niin hankalaa, että siihen kuluu kohtuuttoman paljon aikaa.

Kunnollisen salasanan määräävimmät ominaisuudet ovat käytettyjen eri merkkien lukumäärä ja salasanan kokonaispituus. Mahdollisuuksien joukko lisääntyy räjähdysmäisesti kummankin määreen kasvaessa. Kannattaa kuitenkin huomata, että tämä pätee lähinnä satunnaisille merkkiyhdistelmille. Jonkin luonnollisen kielen sanan tai sanayhdistelmän käyttö tekee salasanasta erittäin helposti arvattavan, puhumattakaan siitä, että sana viittaisi omaan henkilöhistoriaan tai harrastukseen.

Mikä sitten on riittävän monimutkainen salasana? Sellainen, jonka arvaaminen on liki mahdotonta tai vähintään hyvin vaikeaa. Ehdottomana vähimmäispituutena voidaan pitää kahdeksaa merkkiä, kun käytetään sekaisin satunnaisia isoja ja pieniä kirjaimia A–Z, a–z sekä numeroita 0–9. Tällöin saadaan 62^8 eli 218 340 105 584 896 mahdollista vaihtoehtoa. Tietotekniikkaosaston järjestelmät eivät nykyään hyväksy tätä lyhyempiä salasanoja lainkaan. Pidempi on luonnollisesti

parempi, kuten on helppo itsekin nähdä. Kannattaa kuitenkin pitää pää kylmänä ennen kuin kiirehtii pää kolmantena jalkana vaihtamaan itselleen yli kahdeksan merkin salasanaa, se pitää vielä muistaa ulkoa, sillä mitä hyötyä on hyvästäkään salasanasta, jos se on kaiken kansan luettavana paperille kirjoitettuna monitorin kulmassa tai kirjoitusalustan alla?

Väkipakolla tai sanakirjalla

Monelle varmaan herää kysymys, miksei lyhyempikin salasana riittäisi, nouseehan mahdollisten vaihtoehtojen määrä silti inhimillisen käsityskyvyn ylitse. Syy on sama kuin käyttökohde eli tietokone. Suhteellisen uusi työasema kykenee käymään läpi useita miljoonia salasanavaihtoehtoja sekunnissa niin kutsutussa *brute force* -hyökkäyksessä. Vastaavanlainen, mutta nopeampi hyökkäystapa on *dictionary attack*, sanakirjahyökkäys, jossa tietokone käy läpi sanalistoja kokeillen niitä salasanoiksi.

Ensimmäinen menetelmä on takuuvarma, oikea salasana selviää aina. Vaadittava aika kunnollisen salasanan murtamiseksi on onneksi useimmiten sen verran pitkä, ettei *brute force* yleensä kuulu murtautujan työkalukokoelman kärkeen. Jälkimmäinen onkin huomattavasti käytetympi, kiitos huolimattomien käyttäjien. Liki aina löytyy joku, jonka salasana on suoraan sanakirjasta tai muutoin heikko, esimerkiksi sama kuin käyttäjätunnus. Siinä missä ensimmäistä käytetään yleensä yksittäisiä kohteita vastaan, koetellaan sanakirjahyökkäyksillä laajemmin jäätä. Tällaisia hyökkäyksiä kohdistetaan yliopiston järjestelmiin liki päivittäin, joten olemme luonnollisesti huolissamme käyttäjien salasanojen tilasta.

Arvaten tai kalastellen

Kolmas variaatio samasta teemasta on salasanan arvailu käyttäjän henkilöhistorian, harrastusten tai muun henkilökohtaisen piirteen perusteella. Tyttö- tai poikaystävän, lemmikin tai lapsen nimen käyttäminen salasanana on kovin inhimillistä, muttei millään muotoa vaikeasti arvattavaa. Samoin autonomistajilla on toisinaan tapana käyttää rekisteri- tai mallinumeroa. Lisäesimerkkejä jokainen voi keksiä itse.

Oikean vaihtoehdon etsiminen kokeilemalla on karkea tapa, kuin yrittäisi fileoida lohta tylsällä voiveitsellä. Hienostuneempi ja ennen kaikkea tehokkaampi tapa on sosiaalinen hakkerointi, *social engineering*, joka on verrattavissa hyvinkin mainitun lohen fileointiin kunnollisella fileerausveitsellä. Siistiä ja vaivatonta, jos yhtään tietää mitä tekee. Perusajatus on urkkia uhrilta sellaista tietoa, jota hän ei saisi paljastaa: salasanoja, käyttäjätunnuksia, kulkukoodeja, luottamuksellista tietoa tai materiaalia, liki mitä vain. Tuorein julkisuuteenkin päätynyt tapaus oli Nordean verkkopankkiasiakkaisiin kohdistunut urkintayritys. Pelottavaa kyllä, huolimatta pankin varoituksista ja huijausviestin erittäin huonosta suomenkielestä runsaat parikymmentä asiakasta luovutti verkkopankkinsa käyttäjätunnuksen ja varmistuskoodeja huijareille. Vaikka Nordea onnistuikin estämään suurimman osan varojen tilisiirroista, nousi kaapattujen eurojen yhteissumma noin 60 000 euroon.

Sosiaalisen hakkeroinnin välttäminen on perustaltaan hyvin yksinkertaista: mitään salaista ei saa luovuttaa kenellekään muulle missään olosuhteissa. Yhdelläkään ylläpitäjällä tai turvallisuusihmisella ei ole koskaan tarvetta kysyä käyttäjän salasanaa, PIN-koodia tai mitään muuta vastaavaa. Eikä niitä ikinä kysyttäisi sähköpostitse tai puhelimitse. Samaiset henkilöt eivät myöskään tarvitse salasanoja mihinkään, joten vapaaehtoisesti niitä ei saa luovuttaa.

Apua saa kysymällä

Vaikka tietotekniikan maailma tuntuu välillä oudolta ja pelottavalta, myös meille ammatiksemme siellä toimiville, ei saa antaa sen lannistaa, lähes kaikesta selviää käyttämällä tervettä järkeä, olemalla varovainen ja pitämällä mielessä sen, että tietokone on vain työkalu. On jokaisesta itsestään kiinni, käyttääkö työkalua oikein, väärin vai jotenkin siltä väliltä. Jos jokin asia askarruttaa, ei kysymistä pidä arastella, kukaan ei voi tietää kaikesta kaikkea.

Käyttölupiin ja salasanoihin liittyvissä asioissa saa apua käyttölupapalveluista joko käymällä henkilökohtaisesti kampuksen käyttölupapisteessä tai sähköpostitse osoitteesta *atk-luvat@helsinki.fi*. Väärinkäyttöhavainnot ja -epäilyt tulee ilmoittaa kampuksen tietoturvakoordinaattorille tai sähköpostitse osoitteeseen *atk-turva@helsinki.fi*.