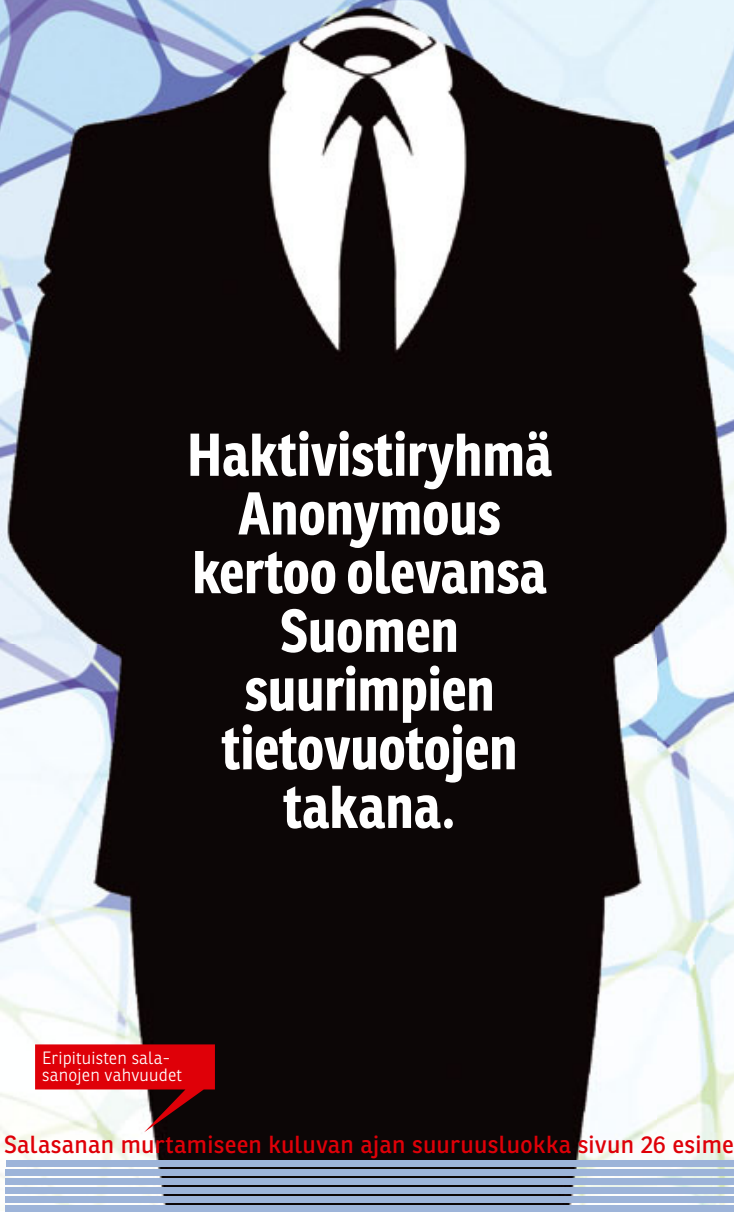
Näin tapahtui Suomen suurin tietovuoto

Marraskuun aikana Suomessa tapahtui neljä vakavaa tietovuotoa. Vuotaneita tietoja voidaan käyttää rikollisiin tarkoituksiin.

TEKSTI: **OSSI JÄÄSKELÄINEN**



Lauantaina 5.11. 16 000 suomalaisen nimet, osoitteet, sähköpostiosoitteet, puhelinnumerot ja henkilötunnukset vuotivat nettiin. Mukana oli esimerkiksi poliisin, tullin, verohallinnon ja ulkoasiainministeriön palveluksessa olevia henkilöitä. Kyseessä oli Suomen historian suurin henkilötietovuoto.

Tiedot vuotivat erilaisia koulutuspalveluita tarjoavilta tahoilta kuten Itä-Suomen yliopiston avoimen yliopiston järjestelmistä, Suomen Opiskelija-allianssi Osku ry:ltä sekä Työtehoseuralta. Tiedot on saatu todennäköisesti jonkun ohjelmiston haavoittuvuutta hyväksikäyttäen tietomurron avulla.

Seuraavana lauantaina 12.11. tietovuodot jatkuivat, kun 500 000 suomalaista sähköpostiosoitetta julkaistiin netissä. Sähköpostiosoitteet ovat peräisin ilmeisesti erilaisilta keskustelupalstoilta ja nettisivuilta. Kyseessä oli määrällisesti todennäköisesti Suomen suurin tietovuoto, vaikka sähköpostiosoitteiden lisäksi muita tietoja ei julkaistu.

Myöhemmin samana iltana netissä julkaistiin myös 15 000 a-, n- ja o-alkuista salasanaa, joiden väitettiin liittyvän vuotaneisiin sähköpostiosoitteisiin. Väitettä ei ole vahvistettu, mutta lista vaikuttaa ainakin osin aidolta. Joukossa on selvästi suomalaisten salasanojen kaltaisia merkkijonoja, mutta myös lukuisia epätodennäköisempiäkin merkkijonoja.

Keskiviikkona 16.11. tapahtui kolmas tietovuoto. Tällä kertaa netissä jaettiin 12 000 käyttäjätunnusta, salasanaa ja sähköpostiosoitetta. Tiedot olivat peräisin käytettyjen autojen kauppaan keskittyneestä Netcar.fi-palvelusta, josta tiedot varastettiin sql-injektiohyökkäyksen avulla tehdyn tietomurron kautta.

Maanantaina 28.11. tapahtui vielä neljäs tietovuoto, kun netissä jaettiin 73 000 käyttäjätunnusta, salasanaa ja sähköpostiosoitetta. Tiedot vuotivat Helistin.fi-keskustelupalstalta, jonka käyttämän PhpBB2-keskustelupalstaohjelmiston tuki ja tietoturvapäivitykset lopetettiin jo vuosia sitten.

Samat tunnukset toimivat myös useissa muissa Terve Median palveluissa. Terve Median palveluita ovat Verkkoklinikka.fi, Tohtori.fi, Poliklinikka.fi, Terkkari.fi, Terve24.fi, Kimallus.fi, Huoltamo.com, Pudottajat.fi, Terverekry.fi, Mustapippuri.fi sekä Laakariportaali.fi. Pelkästään Lääkäriportaalilla on yli 15 000 käyttäjää eli 86 prosenttia suomalaisista lääkäreistä

Eripituisten salasanojen vahvuudet

Salasanan murtamiseen kuluvan ajan suuruusluokka sivun 26 esimerkkilaitteistolla. **Minuutti:** salasanan pituus 6 merkkiä tai alle

Miten suuren uhkan tietovuodot aiheuttavat?

Osoitteen ja puhelinnumeron vuotaminen nettiin ei ole useimmissa tapauksissa vaarallista. Samat tiedot löytyvät esimerkiksi puhelinluettelosta tai numeropalvelusta. Listassa voi kuitenkin olla esimerkiksi viranomaisten salaisia yhteystietoja.

Nettiin vuotanut jättimäinen sähköpostiosoitelista ei sekään uhkaa kenenkään tietoturvaa. Lista toki voi toimia osoitelähteenä roskapostittajille, mutta muuta konkreettista haittaa siitä tuskin on. Vasta jos sähköpostiosoitteisiin yhdistetään tieto siitä, mistä palvelusta tiedot on saatu, sekä sähköpostiosoitteisiin liitetyt tunnukset ja salasanat, lista voi olla vaarallinen.

Sähköpostitunnusten tai -osoitteiden salasanoja ei siis ole julkistettu. Salasanat ovat peräisin niistä palveluista, mistä tiedot on saatu, kuten keskustelupalstoilta. Ellet käytä samaa salasanaa kaikkialla, sähköpostisi salasana on turvassa.

Vuotaneet salasanat eivät siis yksinään ole uhka. Pelkällä salasanalla ei tee mitään – vasta, kun salasana yhdistetään käyttäjätunnukseen tai sähköpostiosoitteeseen, tietoturva on vaarassa. Toistaiseksi ei ole julkaistu listaa, jossa jättivuodon yhteydessä mahdollisesti saadut salasanat yhdistettäisiin muihin tietoihin.

Jos eri palveluissa on käytössä eri salasana, käyttäjätunnuksen ja salasanan yhdistävä lista ei sekään ole vielä vaarallinen, ellei listalla kerrota lisäksi, mihin verkkopalveluun käyttäjätunnus ja salasana käyvät, kuten esimerkiksi Netcar.fi- ja Helistin.fi-murtojen yhteydessä kävi.

Tietovuodot olivat kuitenkin erittäin hyvä ja konkreettinen muistutus siitä, että samaa salasanaa ei missään nimessä kannata käyttää eri palveluissa, ja että salasanan kannattaa olla riittävän monimutkainen ja etenkin riittävän pitkä.

Tietovuotojen takia etenkin tärkeiden palveluiden kuten sähköpostin, verkkokauppojen sekä maksupalveluiden kuten PayPalin salasanat on syytä vaihtaa turvallisempiin.

Henkilötunnus: avain identiteettivarkauteen

Henkilötunnus on vuotaneista tiedoista potentiaalisesti vaarallisin. Monessa palvelussa aina viranomaisten asiointipalveluita myöten henkilötunnusta käytetään ikään kuin salasanana. Oikean henkilötunnuksen kertomalla voi turhan usein vahvistaa olevansa kyseinen henkilö, vaikka käyttäjä pitäisi aina tunnistaa jollain muulla keinolla kuin pelkällä henkilötunnuksella.

Henkilötunnuksen voi saada selville esimerkiksi julkisista asiakirjoista. Henkilötunnuksen ei pitäisi olla salassa pidettävää tietoa, eikä sen avulla pitäisi päästä tunnistautumaan palveluihin.

Käytännössä pelkällä osoitetiedolla ja henkilötunnuksella voi esimerkiksi tilata internetistä tavaraa. Näin tietovuodon jälkeen tehtiinkin: poliisi tiedotti viikko henkilötietovuodon jälkeen, että vuotaneilla henkilötiedoilla on tilattu netistä tavaraa kymmenillä tuhansilla euroilla heti vuodon jälkeisinä päivinä.

Jos oma henkilötunnus oli vuotaneiden tietojen joukossa, kannattaa esimerkiksi postia ja muita yhteydenottoja seurata tarkasti. Jos postiluukusta alkaa putoilla esimerkiksi osamaksutositteita, rikollinen on voinut käyttää henkilötietojasi tavaroiden tai palveluiden maksamiseen. Tällöin on otettava välittömästi yhteyttä poliisiin.

Kuka on vastuussa, jos tietomurto tapahtuu?

Periaatteessa vastuu on aina sillä taholla, joka ylläpitää esimerkiksi asiakas- tai henkilörekisteriä. Vastuukysymys on kuitenkin käytännössä hankalampi.

Jos www-sivujen tekninen toteutus ja ylläpito on ostettu yritykseltä A, nettisivut ja tietokanta sijaitsevat fyysisesti yrityksen B palvelimella ja tietomurto tapahtuu yrityksen C valmistaman ohjelmiston kautta, on epäselvää, kuka lopulta on vastuussa. Etenkin, jos murto on kohdistunut esimerkiksi avoimeen lähdekoodiin perustuvaan ohjelmistoon. Tällöin ei edes ole olemassa ketään yksittäistä tahoa, joka olisi vastuussa.

Vastuu jakaantuu moneen palaseen: sovelluskehittäjä on vastuussa tietoon tulleiden tietoturvareikien ja haavoittuvuuksien paikkaamisesta. Sivuston tekninen ylläpitäjä on vastuussa päivitysten asentamisesta. Ja palveluntarjoajan on omalta osaltaan pidettävä huolta, että palvelin ja esimerkiksi julkaisujärjestelmän taustalla olevat sovellukset kuten tietokantapalvelin sekä palvelimen käyttöjärjestelmä ovat ajan tasalla.

Vastuullinen taho riippuu siis siitä, mitä kautta tai mihin järjestelmään tietomurto on tehty.

Tietovuoto vai tietomurto?

Tietomurto tarkoittaa sitä, että tietoihin on päästy käsiksi palveluksessa tai sovelluksessa olevaa tietoturva-aukkoa hyödyntäen. Tiedot on saatu murtautumalla palveluun, yleensä jo julkiseen tietoon tullutta mutta vielä paikkaamatonta haavoittuvuutta hyödyntäen. Tietomurron avulla saatuja tietoja ei välttämättä julkaista eli vuodeta esimerkiksi nettiin, vaan tietoja voidaan käyttää esimerkiksi identiteettivarkauksiin

Tietovuoto voi tapahtua joko tietomurron seurauksena tai ilman tietomurtoa. Tiedot voivat vuotaa julkisuuteen esimerkiksi yrityksen tai organisaation sisältä henkilöltä, jolla on ollut pääsy kyseisiin tietoihin. Tietovuoto voi olla tahallinen tai tapahtua vahingossa.

Tiedot vuotavat ilman tietomurtoakin

Eikä tietovuotoja varten tarvita aina edes tietomurtoa. Tiedot voivat vuotaa esimerkiksi yrityksen työntekijän kautta ilman että järjestelmiin murtaudutaan.

Uhria voidaan huijata lähettämään tiedot huijarille, tiedot voivat vuotaa vahingossa esimerkiksi väärin kirjoitetun sähköpostin vastaanottajan kautta tai työntekijä voi vuotaa tiedot tahallisesti, joko ilkivaltana tai taloudellisen hyödyn saamiseksi.

80 prosenttia tietovuodoista tulee yrityksen sisältä päin, arvioivat Tiedon johtaja **Jyrki Oksala** sekä Trusteqin kehitysjohtaja **Jukka Lauhia** Pilvipalvelut ja käytännön tietoturva -tapahtumassa marraskuun lopussa.

Tilastot eivät tue väitettä täysin, ainakaan kansainvälisesti: tietovuotoja tilastoivan datalossdb.org-palvelun mukaan tänä vuonna tapahtuneista tietovuodoista 49 prosenttia tapahtui yritysten ulkopuolisten tekijöiden toimesta ja 42 prosenttia yrityksen työntekijöiden kautta. Lopuille tietovuodoille ei löytynyt varmaa selitystä.

Etenkin yrityksen sisältä tapahtuvat tietovuodot eivät aina ole tarkoituksellisia, vaan johtuvat useammin työntekijän huolimattomuudesta kuin tahallisuudesta.

Kuka siis korvaa, jos tietoja vuodetaan? "Sieltähän ne sopimuksesta löytyy", Oksala toteaa. "Korvauksia voi olla hankala saada. Vastuu on rajattu aika vahvasti", Lauhia varoittaa. MPC

Tunti: 7 merkkiä

GRAFIIKKA: **KATJA REINA**

Tietomurron anatomia

1

PALVELUSTA LÖYDETÄÄN haavoittuvuus. Siitä kerrotaan tietoturva-asiantuntijoiden sähköpostilistoilla tai keskustelupalstoilla. Murtautuja saa tiedon haavoittuvuudesta samasta paikasta. Murtautujalla on yleensä tunteja tai päiviä aikaa ennen kuin tietoturva-aukko paikataan.

5 790

haavoittuvuutta sovelluksissa ja verkkopalveluissa vuonna 2011 (24.11. asti).

LÄHDE: SecurityFocus

3

HYÖKKÄÄJÄ

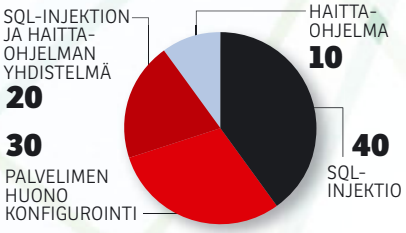
MURTAUTUJA EI HYÖKKÄÄ suoraan palvelimelle, vaan käyttää välissä tor-verkkoa tai Socks-välityspalvelinta. Tor-verkko kierrättää liikenteen useiden anonyymipalvelimien kautta. Uhri ei siis näe, mistä hyökkäys todellisuudessa tuli. Tekijää ei voida jäljittää.

Viikko: 8 merkkiä

TIETOMURROT, %

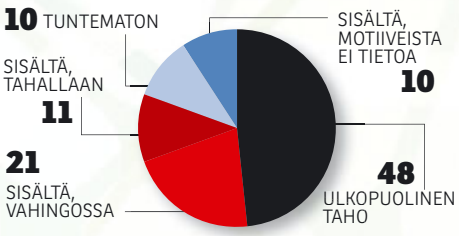
LÄHDE: The Web Application Security Consortium 2008

MITEN TIEDOT VUOTAVAT, %



LÄHDE: UK Security Breach Investigations Report 2010

NÄIN TIETOJA VARASTETAAN YRITYKSESSÄ, %



LÄHDE: Datalossdb.org

2

MURTAUTUJA TIETÄÄ, mikä ohjelmisto on haavoittuva, ja etsii Googlella sivustoja, joilla palvelu on käytössä.

4

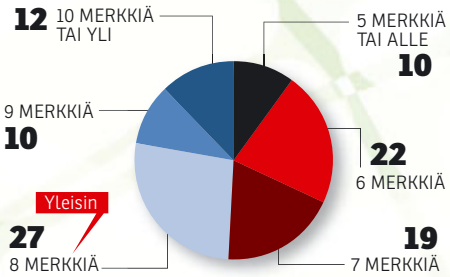
TIETOTURVA-AUKON HYÖDYNTÄMISTÄ varten hyökkääjän on syötettävä palvelimelle omaa koodiaan. Tämä onnistuu yleensä esimerkiksi www-sivuilla olevan lomakkeen kautta, sillä lomakkeen kenttiin voi syöttää mitä haluaa.

Kun lomakkeeseen syötetyt erikoismerkit aiheuttavat virhetilanteen, päädytään virheilmoitussivulle. Virheilmoitussivun osoitetta muokkaamalla järjestelmään voidaan syöttää koodia. Sopiva sovellus voi käydä automaattisesti läpi jopa satoja tuhansia variaatioita hyökkäyskoodista.

5

KUN SOPIVA haittakoodi löytyy, päästään antamaan käskyjä sivuston takana olevalle tietokantapalvelimelle. Tietokantaa voidaan pyytää listaamaan esimerkiksi käyttäjätiedot. Nämä tiedot näkyvät nyt www-sivulla tekstimuodossa. Riippuu palvelusta, mitä tietoja sinne tallennetaan. Tietoja voivat olla esimerkiksi käyttäjätunnus, nimi, sähköpostiosoite, osoite, puhelinnumero, henkilötunnus, luottokortin numero ja salasana tai sen tarkistussumma.

HELISTIN.FI-KÄYTTÄJIEN SALASANAN PITUUS, %
Salasanoja palvelussa yhteensä 73 173 kpl



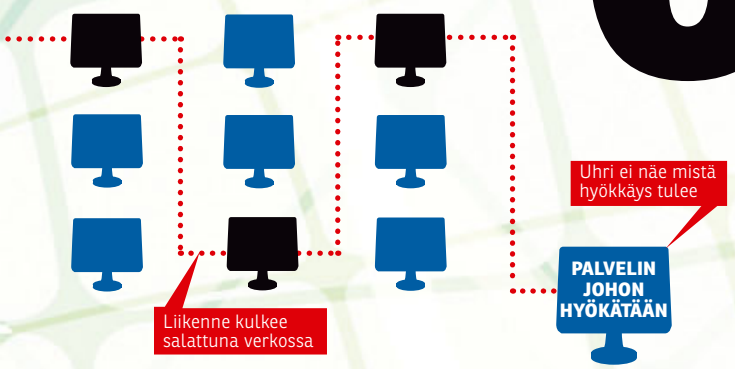
LÄHDE: Helistin.fi-palvelussa käytetyt salasanat

6

SALASANOJEN TARKISTUSSUMMIA voi etsiä Googlen avulla tai niitä voi verrata etukäteen muodostettuihin rainbow table -taulukoihin. Salasanoja ei siis varsinaisesti murreta, vaan yleisimpien salasanojen sekä lyhyiden merkkijonojen tarkistussummat on laskettu etukäteen.

Kun palvelusta on saatu liuta salasanojen tarkistussummia, katsotaan, löytyykö samoja tarkistussummia rainbow table -taulukoista. Jos löytyy, niin taulukosta saa selville selkokielisen salasanan.

TOR-VERKON TOIMINTA



TARKISTUSSUMMA	SELVÄKIELINEN SALASANA
e7e941b1f09f266540c6780db51d5f58	salasana
a33c882677b5a41625037f90ab30f4ea	aurinko
e10adc3949ba59abbe56e057f20f883e	123456

Vuosi: 9 merkkiä

Vuotivatko salasanat todella?

HAKTIVISTIRYHMÄ Anonymouksen "Suomen-osasto" Anonymous Finland väittää olevansa vastuussa sekä henkilötietovuodosta että 500 000 vuotaneesta sähköpostiosoitteesta. Netcar.fi- ja Helistin.fi-vuotojen taustalla taas olivat ilmeisesti yksittäiset henkilöt, jotka eivät ole osa Anonymousta.

MikroPC haastatteli hakkeriaktivistien puhemieheksi esittäytynyttä henkilöä. Hänen mukaansa ryhmä olisi saanut haltuunsa sähköpostivuodon yhteydessä myös noin 490 000 salasanaa, joista "20–30 prosenttia" olisi tallennettu niin sanottuina **suolattuina tarkistussummina**, osa suolaamattomina **sha-1**-tiivisteinä ja osa selväkielisinä.

Puhemiehen mukaan sähköpostiosoitteet olisi saatu "suurimmaksi osaksi" PHP-Fusion-, PhpBB3- ja vBulletin-järjestelmiä käyttäviltä sivustoilta. PhpBB3 ja vBulletin ovat keskustelupalsta-alustoja, PHP-Fusion laajempi sisällönhallintajärjestelmä, jossa on myös keskustelupalsta.

PhpBB3:ssa ja vBulletinissa salasanat tallennetaan käyttäjäkohtaisesti suolattuina **md5**-tarkistussummina, PHP-Fusion-järjestelmässä oletusarvoisesti käyttäjäkohtaisesti suolattuna **sha-2**-tiivisteenä.

ANONYMOUS-EDUSTAJAN puheista sekä alustojen teknisistä toteutuksista voi vetää sen johtopäätöksen, että salasanoja tai niiden tarkistussummia ei välttämättä ole saatu todellisuudessa haltuun: kyseiset järjestelmät eivät tallenna salasanoja siinä muodossa, missä Anonymous-edustaja väitti.

Ja vaikka salasanatiivisteet olisivat vuotaneet, niitä ei saa kovin helpolla selväkieliseksi. Vain jos salasanat olisi tallennettu suolaamatta tai staattisella, palvelukohtaisella suolalla, salasanat voisi selvittää järjellisessä ajassa.

SALASANOJEN tarkistussummat lasketaan nykyään nopeimmin näytönohjainten avulla. Esimerkiksi kahdeksalla tehokkaalla Radeon HD 6970 -näytönohjaimella varustettu reilun 3 000 euron hintainen teho-pc laskee oclHashcat-plus-sovelluksen avulla parhaimmillaan 26 miljardia md5-tiivistettä tai 12 miljardia sha-1-tiivistettä sekunnissa. Jos salasanassa on isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä (40 yleisintä erikoismerkkiä), kaikki kahdeksan merkkiä pitkät md5-tarkistussummina tallennetut salasanat on murrettu nopeimmillaan reilussa viikossa.

Yhdeksänmerkkisten salasanojen murtoon menee jo noin 2,5 vuotta, kymmenmerkkisten yli 250 vuotta. Toki tuhannen yhtä tehokkaan laitteiston hajautetulla rinnakkaislaskennalla 9-merkkiset murtuisivat jo päivässä. Näin järeitä murtofarmeja kotikäyttäjiltä tuskin kuitenkaan löytyy.

Ja koska salasanat ovat näissä järjestelmissä käyttäjäkohtaisesti suolattuja, sama urakka pitäisi käydä läpi yksitellen jokaiselle käyttäjätunnukselle.

SEN SIJAAN JOS TIEDOT ovat vuotaneet sellaisista järjestelmistä, jotka tallensivat salasanat yksinkertaisina md5-tarkistussummina, etenkin helpot ja lyhyet salasanat selviävät todella helposti esilaskettujen rainbow table -murtotaulukoiden avulla. Esimerkiksi Phpbb-keskustelupalstan vanhempi 2-versio tallentaa salasanat yksinkertaisina md5-tarkistussummina.

Yksinkertainen md5-tarkistussumma on kaikkein helpommin murrettavissa, mutta mitä pidempi salasana on, sitä kauemmin sen murtaminen kestää. Lyhyen mutta monimutkaisen salasanan sijaan käytettävä pidempi mutta helpommin muistettava salalause on todellisuudessa paljon turvallisempi.

Suola on merkkijono, jonka järjestelmä lisää salasanaan ennen tarkistussumman laskemista. Se voi olla palvelukohtainen eli kaikille käyttäjille sama tai käyttäjäkohtainen. Suolan avulla pystytään estämään valmiiden tarkistussummataulukoiden käyttö salasanan purkamisessa. Käyttäjä ei voi vaikuttaa suolaan, vaan suolan käyttö riippuu järjestelmästä.

Tiiviste tai **tarkistussumma** on salasanasta yksisuuntaisella matemaattisella menetelmällä muodostettava merkkijono. Sanan "kissa" tarkistussumma on 1ad99cbe9e425d4f-19c53a29d4f12597, ja tarkistussummasta ei voi laskea takaisin, mikä salasana todellisuudessa on.

Verkossa on kuitenkin lukuisia sivustoja, joille on laskettu valmiiksi lyhyiden merkkijonojen – siis huonojen salasanojen – tarkistussummat. Vertaamalla tietomurron avulla saatuja tarkistussummia netistä löytyviin on erittäin helppo saada salasanat selville, jos tiivisteissä ei ole käytetty suolaa.

Md5, **sha-1** ja **sha-2** ovat erilaisia tapoja laskea tarkistussumma. Md5 on näistä yksinkertaisin ja nopeimmin laskettavissa, sha-1 hitaammin laskettava eli turvallisempi ja sha-2 kolmikosta turvallisin. Salasanan pituus sekä suolaaminen ovat tietoturvan kannalta tarkistussummametodia tärkeämpiä tekijöitä.

100 vuotta: 10 merkkiä

	Salasanan pituus, merkkiä			
Salasana sisältää	8	9	10	11
a-ö	sekunteja	minuutteja	tunteja	päiviä
a-ö, A-Ö	tunteja	päiviä	kuukausia	kymmeniä vuosia
a-ö, A-Ö, 0-9	tunteja	päiviä	vuosia	satoja vuosia
a-ö, A-Ö, 0-9, erikoismerkit	tunteja	päiviä	satoja vuosia	kymmeniä tuhansia vuosia
	Murtoaika			

Käytännön esimerkki

SALASANAN "KISSA" md5-tarkistussumma on 1ad99cbe9e425d4f19c53a29d4f12597. Tarkistussumman googlaamalla salasana paljastuu.

Kun salasanaan lisätään suola, esimerkiksi #www.keskustelupalsta.fi$, suolattu salasana on #www.keskustelupalsta.fi$kissa ja sen md5-tiiviste a29258ac806f5f15433c5393c8c09b3e. Tätä tiivistettä ei löydä valmiista taulukoista tai netistä.

JOS SUOLA ON KAIKILLE käyttäjätunnuksille sama, murtotaulukko on helppo luoda laskemalla tarkistussummat kaikille merkkijonoille välillä #www.keskustelupalsta.fi$a – #www.keskustelupalsta.fi$ööööööööö. Aikaa tähän menee tehokkaalla laitteistolla vain reilu viikko. Tämän jälkeen kaikki palvelussa käytetyt 8-merkkiset salasanat olisi saatu selville, oli käyttäjiä sitten 2 tai 2 000.

JOS SUOLA ON KÄYTTÄJÄKOHTAINEN, tällöin käyttäjä1:n suola olisi esimerkiksi Zab+Oh1@, käyttäjä2:n 0oEa128# ja niin edelleen. Vaikka käyttäjät 1 ja 2 käyttäisivät samaa salasanaa, salasanan tarkistussumma olisi eri. Tällöin jokaisen käyttäjän salasana pitäisi murtaa erikseen, mikä on todella hidasta. Jos käyttäjiä on 2 000, kuluisi reilun viikon sijasta 2 000-kertainen aika eli lähes 50 vuotta kaikkien 8-merkkisten salasanojen murtamiseen.

USEIMMAT NYKYAIKAISET palvelut tallentavat salasanat juuri käyttäjätunnuskohtaisella suolauksella. Jos käyttäjäkohtaisesti suolattujen salasanojen tarkistussummat vuotavat verkkoon, niiden murtaminen on hankalaa; jos salasana on riittävän monimutkainen, salasanan murtaminen on käytännössä mahdotonta ilman supertietokonetta tai muuta laajaa rinnakkaislaskentaa.

Unohda salasana – käytä salalausetta!

"HYVÄSSÄ salasanassa on sekaisin isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Esimerkiksi #s5K!h0x on hyvä salasana."

Näin väitetään, mutta tämä ei pidä paikkaansa. Tällainen salasana on vaikea muistaa ja helppo murtaa!

Käytännössä salasanan pituus määrittelee sen turvallisuuden. Jos salasanassa käytetään isoja ja pieniä kirjaimia, numeroita ja yleisimpiä erikoismerkkejä, jokainen lisämerkki karkeasti ottaen satakertaistaa murtamiseen kuluvan ajan.

MITÄ PIDEMPI salasana, sitä todennäköisempää on, että sen tarkistussummaa ei löydy netistä. Myös isojen kirjaimien, numeroiden sekä erikoismerkkien käyttö tuo lisäturvaa. Salasanan pituus on kuitenkin enemmän turvaa tuova tekijä kuin salasanassa olevien erikoismerkkien määrä.

Pitkän ja hankalan salasanan sijaan voi käyttää erikoismerkeillä ja numeroilla terästettyä salalausetta. Lause on helpompi muistaa kuin epämääräinen merkkijono. Salalause voi olla selväkielinen tai lyhenteitä käyttävä; "KissaniNimiOnMisse<3" tai esimerkiksi jääkiekkofanilla "Mm1995&2011!".

SALALAUSETTA EI SAA käyttää sellaisenaan missään palvelussa, vaan siihen on aina lisättävä palvelukohtainen merkkijono, joka ei ole helposti arvattavissa.

Jos näin ei tehdä, ja yksikin palvelu tallentaa salasanan selväkielisenä, yhden paljastuneen salasanan avulla salalause paljastuu. Esimerkiksi "Mm1995&2011!-keskustelupalsta.fi"-salalauseen paljastuttua on helppo arvata, että Gmailin salasana on "Mm1995&2011!gmail.com"

SALALAUSEESEEN on siis lisättävä jokaiselle palvelulle yksilöllinen merkkijono, jota ei voi arvata palvelun nimen perusteella. Tämän merkkijonon voi huoletta kirjoittaa paperille, ja paperia voi huoletta kuljettaa mukaanaan vaikka lompakossa.

Näin yksikään vuotanut salasana ei paljasta muiden palveluiden salasanoja eikä lompakossa mukana kulkeva paperi paljasta minkään palvelun salasanaa kokonaisuudessaan. Ja jos palvelukohtainen tunnus on esimerkiksi neljän kirjaimen mittainen, sen muistaminen on kuitenkin huomattavasti helpompaa kuin niin sanotun hyvän salasanan kuten "#s5K!h0x":n muistaminen.

Ja siinä missä "#s5K!h0x" murtuu viikossa, 12-merkkisen salalauseen kuten"Mm1995&2011!":n murtamiseen kuluisi aikaa kolme miljoonaa vuotta tai miljoonalta tehokoneeltakin kolme vuotta.

10 000 vuotta: 11 merkkiä