8. joulukuuta 2022

Tiivisteiden käyttö salasanojen tallennuksessa

Valtteri Varvikko (015107406)

Historialliseti ihmisyhteisöissä materian suojaaminen on ollut keskiössä. Tieteen kehittyminen on luonut mahdollisuuksia myös tiedon roolin kasvamiselle. Arvokkaina pidettyn tiedon suojaamisen vaatii uudenlaisen suunnan perinteisten lukkojen rinnalle. Nykyaikana tiedon rooli on korostunut ennennäkemättömän suureksi, ja arvokkaana pidetyn materian tavoin myös arvokkaana pidetyn tiedon edellyttää vahvoja suojausmenetelmiä. Digitaalisessa maailmassa tiedon suojaamisen käytetään laajalti salasanoja, joiden käytössä kryptografisilla menetelmillä on merkittävä rooli.

Salasanat voidaan tallettaa tietokantaan sellaisenaan. Nykykonsensuksen mukaan näin ei tule enää menetellä. Pääsyä tietokantaan voidaan rajata, mutta onnistuneen hyökkäyksen mahdollisuus on tästä huolimatta olemassa. Nykyisin vallitseva menetelmä on tallettaa salasanan sijaan tiiviste, joka vääriin käsiin päätyessään ei vaaranna suojattua dataa. Kyse ei ole niinkään salauksesta, joka mahdollistaa alkuperäisen syötteen palauttamisen salausta datasta. Salasanoista pyritään tiivistämään arvoja, joita ei missään olosuhteissa ole mahdollista palauttaa rajallisella laskentakapasiteetilla. Salasanojen tiivistykseen käytetään tästä syystä laajalti kryptografisia tiivisteitä, jotka yksisuuntaisuudestaan johtuen estävät alkuperäisen syötteen johtamisen tiivisteestä.

Salasanojen oikeellisuuden tarkistamisessa keskitytään tiedon palauttamisen sijaan selvittämään, onko kyseistä salasanaa käytetty jonkin tiivisteen luomisessa. Ihanteellisesti tietokantaan talletetaan salasanan sijaan siitä johdettu avain, josta ei ole mahdollista johtaa itse salasanaa. Huolellisesti laaditussa järjestelmässä tiivisteitä vertaillaan ohjelmakoodissa, eikä hyökkääjän ole mahdollista injekoida haltuunsa saamian tiivisteitä tiivistysvaiheen ohi. Salansanatiiviste on ulkopuolisen haltuun päätyessään hyödytön, ja siten riskitön tallettaa tietokantaan.

Kryptografiset tiivistefunktiot ovat deterministisiä ja tuottavat tietylle syötteelle aina saman tiivisteen. Siten mitkä tahansa kaksi yhtäläistä tiivistettä on suurella todennäköisyydellä tiivistetty samasta. Yhtä salasanaa vastaavan tiivisteen paljastuminen takaa vaivattoman pääsyn kaikkiin samaa salasanaa käyttäneiden identiteettiin, koska nämä voidaan tunnistaa etsimällä tiivisteiden joukosta identtisiä tiivisteitä. Laajempaan hyökkäykseen voidaan pyrkiä tiivistämällä suuri määrä tunnetusti yleisimpiin kuuluvia salasanoja, ja verrata niitä tietokantojen tiivisteisiin.

Salasanojen identiteetin takaamiseksi salasanaa tiivistäessä käytetään salt-arvoa, eli satunnaisesti generoitua merkkijonoa. Tiiviste luodaan syötteestä ja sen perään listätystä salt-arvosta. Kryprotgrafisen tiivistefunktion generoima tiiviste muuttuu tunnistamattomaksi mistä tahansa muutoksesta syötteeseen, joten satunnainen salt-arvo tuottaa samoillekin syötteille

erilaisen tiivisteen. Näin tiivistettyjä salasanoja ei voida yhdistää toisiinsa tiivisteitä vertaamalla - sama salasana tiivistetään aina aiemmista tunnistamattomaan muotoon.

Salt-arvoa tarvitaan, kun salasanan oikeellisuus halutaan tarkistaa. Salt-arvo talletetaankin yhdessä salasanan kanssa. Tarkistettava salasana tiivistetään käyttäen samaa mmenetelmää kuin talletetun tiivisteen luomisessa. Poikkeuksena salt-arvoa ei luonnollisesti generoida uudelleen, vaan tiivistyksessä käytetään talletettua salt-arvoa. Salt-arvon tallettaminen yhdessä salasanan kanssa ei vaikuta tietoturvaan lainkaan.

Tiivistefunktioiden laskennallinen vaativuus kasvaa laskentakapasiteetin kehittyessä. Mitä enemmän tiivisteitä aikayksikössä on mahdollista generoida, sitä useampaa erilaista salasanaa ehditään raa'an voiman menetelmällä koettaa. Salasanojen tiivistyksessä on huomioitava senhetkiseen laskentakykyyn suhteutettuna riittävä vaativuus. Nopea tiivistefunktio nopeuttaa raakaan voimaan perustuvia hyökkäyksiä, tarpeettoman vaativa taas kuluttaa järjestelmän resursseja ja hidastaa kirjautumista.