# Salasanat talteen turvallisesti tiivistelmä

Salasanojen murto on ikävä tapahtuma. Liian monet ihmiset käyttävät samoja salasanoja kaikkiin palveluihin. Tämä altistaa heidät tietomurron uhreiksi. Web-palvelun ylläpitäjänä täytyy taata, että kaikki salasanat pysyvät mahdollisimman turvassa.

Ensimmäinen virhe on tallentaa ne selkokielisenä. Tämän voi hakkeri napata yhdellä SQL injektiohyökkäyksellä. Astetta parempi tapa on kryptata salasanat jollain salausalgoritmilla. Vaikka salasanat ovat suojassa yksinkertaisilta hyökkäyksiltä, on tässäkin tavassa ongelma. Mikäli salasanoilla halutaan tehdä jotain, palvelimen pitää pystyä myös avaamaan ne. Jos hakkerilla on pääsy palvelimelle, voi hän löytää myös avaimen ja salauksen hyöty kadotetaan.

Salasanojen tallentamisessa parasta on tallentaa salasanojen tiiviste, eli hash. Näistä tiivisteistä ei pysty laskemaan alkuperäistä lähdettä. Vaikka tämä on parempi, ei se takaa tarpeeksi turvaa. On valmiiksi laskettuja taulukoita, jotka laskevat yleisimpien salasanojen tiivisteet. On olemassa teknisiä ratkaisuja, eli kryptografista suolaa. Tämä on merkkijono, joka lisää salasanan pituutta. Jos salasana on riittävän pitkä, tekee se taulukoinnista mahdottoman. Yksinkertainen tapa tallentaa salasanatiiviste on: suola + hash.

Viimeinen heikko kohta, on tiivistefunktioiden nopea helppo laskeminen. Tämä uhka voidaan torjua vaihtamalla tiivistefunktion tilalle erityisesti salasanojen tiivistämiseen suunniteltu algoritmi. Nämä algoritmit ovat tahallaan suunniteltu hitaiksi. Oikealla algoritmilla tuotettu salasanatiiviste on siis hidas laskea, joten sanakirjahyökkäys ei ole tehokas. Se on suolattu, joten hakutaulukkohyökkäys on mahdoton. Ja tietysti, tiivistealgoritmi on valittu oikein, joten on äärimmäisen epätodennäköistä, että kaksi eri salasanaa tuottaisi saman tiivisteen.

Sanoja hieman yli: 212