Näkymättömät viestit

- **Salakirjoitus** estää ulkopuolista saamasta selville viestin **sisältöä. Näkymättömyys** pyrkii peittämään ulkopuolisilta viestin **olemassolon**.

  Salaiset viestit **kätketään** harmittomalta näyttävän datan joukkoon.

- Salauksen periaatteita:
  - Salakirjoitusalgoritmi on yleisesti tunnettu, mutta viestin sisällön saa selville vain oikean avaimen haltija.
  - Vastustaja on älykäs, rikas ja haluaa selvittää viestin sisällön.
  - Tunnetun salaamattoman tekstin hyökkäys, valitun salaamattoman tekstin hykkäys

- Näkymättömyyden periaatteita:
  - Kätkemisalgoritmi on yleisesti tunnettu, mutta viestin olemassaolon pystyy toteamaan vain oikean **avaimen** haltija.
  - Vastustaja on älykäs, rikas ja haluaa havaita tai osoittaa viestin olemassaolon.
  - Vastustaja epäilee kaiken näkemänsä datan sisältävän piilotettuja viestejä ja on valmis käyttämään kaikki resurssinsa yhden yksittäisen viestin paljastamiseen.
  - Tunnetun näkyvän tekstin hyökkäys, valitun näkyvän viestin hyökkäys
  - Vaikka vastustaja tietää viestin olemassaolosta, hän ei pysty todistamaan sen olemassaoloa ulkopuoliselle ilman avainta.
- Klassiset kätkemismenetelmät ovat teoreettisesti vahvoja, mutta kalliita ja tehottomia:
  - Subliminaaliset kanavat digitaalisissa allekirjoituksissa
- Halutaan kätkeä viestit massadataan:
  - digitoituihin kuviin
  - videoon
  - digitaaliseen ääneen

Käytännöllisiä kätkemisalgoritmeja

- **Korvausmenetelmä** (*substitutive steganography*):

  Osa kohinaa sisältävän digitaalisen viestin kohinasta korvataan pseudosatunnaisella datalla.

  1. Salainen viesti salakirjoitetaan tai pakataan, jolloin siitä tulee pseudosatunnainen.
  2. Tuotetaan uusi **peitesanoma** (*wrapper message*), esim. digitoitu valokuva, jossa on paljon kohinaa.
  3. Valitaan peitesanoma eniten kohinaa sisältävät bitit, esim. RGB-arvojen vähiten merkitsevät bitit.
  4. Valitaan **salaisen avaimen perusteella pseudosatunnaisesti pieni osa** kohinaa sisältävistä biteistä **kätköbiteiksi** (*hiding bits*).
  5. Korvataan kätköbitit salakirjoitetun sanoman biteillä.

- Peitesanoman bittien pitää olla sen verran satunnaisia, että korvaamisen aiheuttama satunnaisuuden lisäys ei ole havaittavissa.

  Hyviä kätköpaikkoja ovat yleensä mittaustulosten vähiten merkitsevät bitit. Digitoitu kuva on taulukko mittaustuloksia!

- **Valintamenetelmä** (*selective steganography*):

  Satunnaisen näköisilläkin biteillä tunnusomainen tilastolinen jakauma, joka korvausmenetelmässä muuttuu.

  Ei muuteta peitesanomia, vaan valitaan ne niin, että viesti on siellä jo valmiiksi.

  1. Generoidaan suuri määrä hiukan toisistaan poikkeavia peitesanomia, esim. digitoidaan sama kuva satoja kertoja.
  2. Lasketaan jokaisesta peitteestä sormenjälki, esim. CRC:n 8 ensimmäistä bittiä.
  3. Jatketaan kunnes sormenjälki on haluttu luku.

- Turvallista, mutta kallista ja hidasta. Voidaan kätkeä noin 1 tavu / peitesanoma.

- **Konstruktiomenetelmä** (*constructive steganography*):

  Mallinnetaan peitetiedoston bittien jakauma ja muutetaan kätkemisalgoritmia matkitaan niiden alkuperäisiä tilastollisia tunnuslukuja.

  Perinteinen steganografia käyttää konstruktiomenetelmää. Esim. luodaan fraktaalikuva salaisen sanoman perusteella tai valitaan kirjeen sanojen alkukirjaimet sopivasti.

- Mallin luominen vaatii paljon työtä ja taitoa. Vihollinen todennäköisesti tekee paremman mallin.

  Huono malli ennemmin paljastaa kuin kätkee.

  Malli on osa algoritmia, joten vihollinen tuntee sen ja voi kaikessa rauhassa etsiä siitä vikoja.

- **Vain korvausmenetelmä pystyy kätkemään suuria määriä dataa tehokkaasti.** Valintamenetelmä on luotettava, mutta tehoton. Konstruktiomenetelmä on heikko.

- **Tärkeää! Samaa käärettä ei koskaan saa käyttää kahta kertaa. Alkuperäinen kääretiedosto pitää hävittää.**

- Jos kätköbittien valinta riippuu vain avaimesta, ei samaa avainta saa käyttää uudelleeen.

  Tehdään avaimesta kääreen funktio, jolloin eri kääreillä voidaan huoletta käyttää samaa vainta.

  Esim. digitaalisessa kuvassa lasketaan 7 eniten merkitsevästä bitistä sormenjälki, jonka perusteella muutetaan käyttäjän avainta.

$$K = SHA(Ku, wrapper^7).$$

- **Viestin pitää olla lyhyt verattuna kääreeseen.** Kohinaa sisältävistä biteistä voidaan käyttää enintään muutama prosentti.

- Jos kääreessä on riittävästi kohinaa, vihollinen ei voi havaita viestiä tai sen olemassaoloa.

  Brute force -hyökkäys on mahdoton, koska kohinabiteistä löytyy mikä tahansa sanoma, jos luetaan sopivat bitit.

  Vihollinen voi poistaa kätketyn viestin lisäämällä omaa kohinaa.

Näkymättömyyden seurauksia

- Video- ja audiodata, juuri se tieto, jota rutiininomaisesti siirretään ja talennetaan suria määriä, soveltuu kaikkein parhaiten salaisten viestien kätkemiseen. Tekniikka on olemassa ja kadun miehen saatavilla.

- **Sotilasorganissatioissa** tietoturva perustuu salaisen tiedon pitämiseen fyysisesti rajoitetuilla alueilla. Edes luotettu henkilökunta ei ole pystynyt vuotamaan tietoa kuin muistinsa varassa.

  Näkymättömyys merkitsee, että minkä tahansa vaarattomalta näyttävään datan mukana voidaan salakuljettaa salaista tietoa.

  Silti äänen ja kuvien tehokas siirtäminen on välttämätöntä.

- **Tiedonsiirtopalveluja myyvät yritykset** haluaisivat hinnoitella eri tyyppisten tietojen siirron erikseen.
  - videoneuvottelun kilobittihinta alhainen
  - sähköpostin kilobittihinta korkea

  Videosignaaliin voidaan kätkeä kuinka paljon sähköpostia tahansa, joten erittely ei ole mahdollista.

- **Rikolliset** ja muut moraalittomasti käyttäytyvät voivat käyttää näkymättömyyttä hyödykseen.

  Näkymättömyyden kieltäminen on mahdotonta.

  Vaikka salauksen käyttö kiellettäisiin, rikolliset voivat kätkeä viestinsä.

  Salauksen kieltämisestä tai rajoittamisesta on vain haittaa lainkuuliaisille yrityksille ja kansalaisille. Sillä ei ole mitään vaikutusta rikollisiin.