Toni Keskinen

tonttu.keskinen@gmail.com

TIETOKONE JA TIETOVERKOT TYÖVÄLINEENÄ

3.11.2017

1. Salaus

Salaus viittaa kryptologiassa prosessiin, jolla koodataan viestejä tai tietoja niin, että vain valtuutetut osapuolet voivat lukea niitä.[1] [1]Salaus ei estä viestin sieppaamista, vain sen lukemisen.[2] Salausjärjestelmä muuttaa viestin tai tiedon selkotekstin (engl. plaintext) salatekstiksi (engl. ciphertext) salausalgoritmia käyttäen.[2] [2]Viestin tai tiedon voi tämän jälkeen lukea vain jos salatekstin salaus puretaan.[2] Teknisistä syistä salausjärjestelmä käyttää tyypillisesti algoritmin tuottamaa näennäisesti satunnaista salausavainta. On periaatteessa mahdollista purkaa salaus ilman avainta, mutta tähän tarvitaan hyvin paljon laskentatehoa, jos salausjärjestelmä on toteutettu hyvin. Valtuutettu vastaanottaja voi helposti purkaa viestin salauksen avaimella, jonka salatun viestin lähettäjä antoi hänelle.

2. Sanastoa

Salauksella tarkoitetaan prosessia, jossa selväkielinen teksti eli selkoteksti muutetaan sellaiseksi, ettei sitä pysty tulkitsemaan (salattu teksti, salateksti). Salauksen purkaminen on vastakkainen prosessi, jossa salattu teksti muutetaan selkotekstiksi. Salain on algoritmipari, jolla nämä muutokset tehdään. Algoritmien toimintaa säätelee salausavain, jonka vain viestin lähettäjä ja vastaanottaja tuntevat. Enkryptaus tarkoittaa kryptaamista (salaamista). Dekryptaus tarkoittaa kryptauksen purkamista (salauksen ratkaiseminen).

3. Yleistä

Jo antiikin aikana tunnettujen symmetristen salakirjoitusmenetelmien ideana oli se, että viestin lähettäjä ja vastaanottaja käyttivät viestin salaamiseen ja salakirjoitetun viestin

[1] Niihän se on että näinhän se on
[2] Yuuuuuuup

purkamiseen samaa avainta. Nykyisten, 1970-luvulta lähtien kehitettyjen epäsymmetristen salakirjoitusmenetelmien avulla voidaan kuitenkin toteuttaa aivan uudentyyppinen järjestelmä. Kuka tahansa voi salakirjoittaa viestin tietyn vastaanottajan julkisella salakirjoitusjärjestelmällä hänen ilmoittamaansa julkista avainta käyttäen. Kuitenkin ainoastaan viestin vastaanottaja voi purkaa viestin omalla salaisella avaimellaan.

Nykyisten tietoverkkojen, erityisesti Internetin, toiminta perustuu epäsymmetrisiin (julkisiin) salakirjoitusjärjestelmiin pohjautuviin PKI- (public key infrastructure) protokolliin. Jo klassisia esimerkkejä käytetyistä järjestelmistä ovat Diffie-Hellman-avaimenvaihtoprotokolla ja RSA- ja ElGamal-kryptosysteemit.

Protokollien tehtävä on määrittää, miten luonteeltaan matemaattisia salakirjoitusjärjestelmiä käytetään. Niiden tavoitteena on varmistaa tietoliikenteen turvallisuus. Varsin yleinen tietoturvaongelma on protokollasta poikkeaminen, jonka syynä voi olla vaikkapa ns. social engineering -tyyppinen tiedusteluyritys (ks. Kevin Mitnick). Protokollat on tarkoitettu sellaisiksi selkeiksi ohjesäännöiksi, että kuka tahansa tietoverkon käyttäjä voi niitä käyttäen varmistua oman tietoliikenteensä turvallisuudesta. Protokollien suunnittelu ja niiden syvällinen ymmärtäminen edellyttää kuitenkin pitkällistä matemaattista koulutusta. Protokolla-asiantuntijan tulee olla perehtynyt lukuteorian, algebran ja erityisesti algoritmiteorian viimeisimpiin tutkimustuloksiin.

Kryptologian keskeisimpänä maksiimina voidaan pitää ns. Kerchoffin periaatetta. Periaatteen mukaan järjestelmän tulee perustua avainten salassa pitämiseen. Vihollisen on oletettava tuntevan varsinaisen salakirjoitusjärjestelmän. Kerchoffin periaatteen seuraus on se, että kuka tahansa voi avoimesti kokeilla järjestelmän turvallisuutta. Järjestelmän turvallisuus joutuu näin todelliseen koetukseen (ruuvipenkkiin). Luotettavimmat julkisissa tietoverkoissa käytettävät salakirjoitusmenetelmät noudattavat Kerchoffin

periaatetta. Kuitenkin vielä nykyisin erityisesti mobiilin tietoliikenteen ja sotilassovellutusten puolella pyritään kehittämään järjestelmiä, jotka Kerchoffin periaatteen vastaisesti perustuvat itse salakirjoitusjärjestelmän salassapitämiseen.

4. Salakirjoitusten ja niiden murtamisen historiaa

4.1. Esihistoria

Aluksi kirjoitettujen viestien harvinaisuus suojasi viestejä. Kun useampi kuin yksi osasi kirjoittaa, sanoman salakirjoittaminen muuttui tarpeelliseksi.

Eräs vanhimmista tiedonsalaustavoista oli käytössä Egyptissä. Viesti kirjoitettiin viestinviejän kaljuksi ajettuun päähän. Tukan kasvettua viesti oli valmis lähetettäväksi. Tällä tavalla ymmärrettynä ensimmäiset salakirjoitukset olivat viestin peittämistä, eli steganografiaa.

5. Atbash-koodi ja Caesarin salakirjoitus

Yksi vanhimmista varsinaisista salakirjoituksista on Atbash-koodi. Siinä kirjaimistossa aakkosjärjestyksessä viimeinen kirjain vaihdetaan ensimmäiseen, toiseksi viimeinen toiseen, ja niin edelleen. Nimi atbash tulee heprean kirjaimista alef-tav-bet-shin. Suomalaisilla aakkosilla se toimisi siten, että A:sta tulisi Ö ja B:stä Ä. Atbash-koodausta käytettiin yleisesti tietyissä piireissä satoja vuosia ennen ajanlaskun alkua, ja onpa Raamatussakin Jeremian kirjassa Atbash-koodattuja nimiä.lähde? Koodia käyttävät vieläkin eräät salaseurat tai sen kaltaiset, jotka tahtovat ilmaista olevansa pitkän perinteen vaalijoita.lähde?

Suetonius kuvaa teoksessaan De vita Caesarum Julius Caesarin käyttäneen kenraaliensa kanssa viestiessään salakirjoitusta, jossa kirjain korvataan aakkosjärjestyksessä 3 kirjainta eteenpäin löytyvällä kirjaimella, ja aakkoston lopussa kierretään takaisin alkuun. Tällöin, A:sta tulee D, B:stä tulee E ja niin edespäin. Nykyisin Caesar-salauksella tarkoitetaankin tämän yleistystä, jossa aakkostossa siirrytään sovittu määrä kirjainta eteenpäin. Caesar-salauksen erästä muotoa, Rot13, jossa siirrytään 13 kirjainta eteenpäin, käytetään edelleen esimerkiksi Internet-keskusteluissa, koska koodaus toimii samalla purkuna englannin kielen aakkostolla, jossa on 26 merkkiä.

5.1. Atbash-koodin ja Caesar-salakirjoituksen murtaminen

Atbash-koodilla on vain yksi mahdollinen avain, joten se on hyvin heikko salakirjoitus.

Caesar-koodi ja sen muunnokset on murrettavissa kokeilemalla kaikki N siirrosta aakkosistossa (N = aakkosiston kirjainten määrä), siis esimerkiksi englannin kielessä (= 26 aakkosta) maksimissaan 26 kokeilulla.

Kehittyneempi versio eli sekoitettu Caesar, jossa selväkielistä A:ta vastaa mielivaltainen salakirjoitettu kirjain, B:tä mielivaltainen jäljellä olevista kirjaimista jne., sisältää periaatteessa A! (A-kertoma) määrän mahdollisia avaimia. Englantilaisella aakkosistolla (26 aakkosta) erilaisia sekoitettuja Caesar- avaimia on 26! eli 4,0329 * 1026 mahdollisuutta. Tällaista määrää on liki mahdotonta käydä yksitellen läpi.

Kuitenkin mikäli tiedetään, millä kielellä salattu viesti on kirjoitettu, on sekoitettu Caesar helppo murtaa yhden vähänkin pidemmän sanoman perusteella frekvenssianalyysillä. Eri kielille voidaan muodostaa tilastollinen jakauma eri kirjainten käytöstä. Esimerkiksi

englannin kielessä yleisin kirjain on E. Jos siis englanninkielisessä sekoitettua Caesaria käyttävässä koodatussa sanomassa on eniten W- kirjaimia, hyvä arvaus on, että W vastaa E-kirjainta. Vastaavasti suomen kielessä A on yleisin kirjain.

6. Kehittyneemmistä versioista

Seuraava kehittyneempi versio on muuttaa salakirjoitusaakkosistoa esimerkiksi viiden kirjaimen jälkeen, jolloin tilastollinen ratkaisumenetelmä vaikeutuu oleellisesti. Tätä versiota käytti esimerkiksi suomalainen salakirjoitusviivain eli ns. "matolaatikko"-menetelmä. Tämän menetelmän kehittyneempään muunnelmaan perustui myös saksalaisten toisen maailmansodan aikana käyttämä ENIGMA-salauslaite.

Edellä mainituista esimerkeistä selviää, että salakirjoituksen murtaminen on ainakin matematiikkaa, kielitiedettä ja tilastotiedettä, ja myös yleistä älykkyyttä.

7. Transpositiosalaus

Transpositiosalaus on menetelmä, jossa kirjainten järjestystä muutetaan sovitulla tavalla.

8. Satunnaisluvut

Salauksessa käytettyjen satunnaislukujen tulisi olla mahdollisimman aidosti satunnaisia. Aidosti satunnaisten lukujen tuottaminen on kuitenkin vaikeaa. Nykyään parhaina tapoina tuottaa todellisia satunnaislukuja pidetään luonnollisia systeemejä, kuten radioaktiivisten aineiden luonnollisen hajoamisen tuottamat säteilyhiukkaset, tai esimerkiksi laavalampun vahan liike. Useimmiten tietokoneissa käytetään näennäissatunnaislukugeneraattoreita, jotka eivät välttämättä kelpaa salauskäyttöön. Tietokoneiden salauksessa käytetty satunnaisuus perustuu yleensä käyttäjän tekemien

toimenpiteiden ja verkossa tapahtuvien tapahtumien satunnaisuuden keräämiseen.lähde? Käytännön esimerkkejä edellä mainitusta ovat esimerkiksi käyttäjän hiiren liikkeiden tai mikrofonin vastaanottaman kohinan käyttäminen salausavaimen luomiseen.

8.1. Salauksen käyttökohteita

Tietokoneiden myötä kryptografia sai uuden sovelluskohteen datan salauksen, allekirjoitusten ja eheyden varmistamisesta. Tästä esimerkkejä ovat erilaiset sovellukset ja protokollat etäyhteyksien (SSH) ja www-liikenteen (HTTPS) salaamiseen sekä sähköpostiviestien salaamiseen ja allekirjoittamiseen (PGP).

9. Salausalgoritmeja

9.1. Symmetrisiä salausalgoritmeja

- DES, Data Encryption Standard
- AES, Advanced Encryption Standard (Rijndael)
- IDEA
- Blowfish, Twofish
- 3-DES

9.2. Epäsymmetrisiä eli julkisen avaimen salausalgoritmeja

- Diffie-Hellman-avaimenvaihto
- RSA
- ElGamal
- Elliptiset käyrät

9.3. Yksisuuntaisia tiivisteitä

- MD5 (Message digest)
- SHA-1 (Secure Hash Algorithm)

9.4. Sähköisen allekirjoituksen menetelmiä

- DSA (Digital Signature Algorithm)
- X.509 Varmenteet

9.5. Kryptografiaa käyttäviä sovelluksia

- GPG
- HTTPS-protokolla
- Kerberos-tunnistusprotokolla
- PGP (Pretty Good Privacy)
- SSH-protokolla

10. Murtamaton koodi ja sen ongelmat

Toisin kuin yleensä luullaan on olemassa myös kryptografisesti murtamaton salausmenetelmä: kerta-avain (engl. one-time pad, OTP) -- kertakäyttöinen todellisista satunnaisluvuista koostuva avain, joka on yhtä pitkä kuin salattava viesti. Jokainen viestin merkki yhdistetään avaimen vastaavan merkin kanssa. Murtamattomuus perustuu siihen, että jokainen mahdollinen ratkaisu on yhtä todennäköinen, eikä oikeaa selvätekstiä voi erottaa muista vaihtoehdoista.

Historia on osoittanut, että kertakäyttöisiksi tarkoitettuja avainlistoja viitsitään käyttää harvoin vain yhden kerran. Jos "kertakäyttöistä" avainta käytetään useamman kerran, salateksti voidaan murtaa helposti.

Kertakäyttöisten avainlistojen käyttö on valitettavan epäkäytännöllistä suurien tietomäärien ja monien vastaanottajien kohdalla. Haasteina ovat avainlistojen turvallinen toimittaminen vastaanottajalle sekä niiden alkuperäisen valmistuksen vaatima työ. Avainlista, jonka joku on päässyt kopioimaan matkalla käyttäjälle, on täysin arvoton.

Mikäli avain on lyhyempi kuin viesti tai satunnaisluvut eivät ole aidosti satunnaisia, salaus ei voi olla täydellinen. Silti hyvin tehty salaus voi olla käytännössä äärimmäisen vaikea murtaa.

Kuva 1

Arkikielessä murtamattomalla salauksella voidaan tarkoittaa myös salausmenetelmää, jolla salatun viestin purkuun ei tunneta muuta menetelmää kuin kokeilla kaikkia salausmenetelmän sallimia avaimia. Kyseistä purkamismenetelmää kutsutaan raa'alla voimalla (engl. brute force) purkamiseksi. Esimerkiksi AES-salausta pidetään nykyään murtamattomana.

Kuva 2

Avainlista, 10-9

Caesar, 5-6

Historia, 10-9

mahdollisia, 5-6

salauslaite, 6-7