Salaustekniikoilla lisää turvallisuutta

Tuula Käpylä,
VTT Tietotekniikka

Tietoverkkojen kautta hoidetaan myös luottamuksellista ja salaista tiedonvaihtoa. Tieto voi kulkea kymmenien eri verkkopalveluntarjoajien järjestelmien kautta. Jotta tiedon säilytys ja siirto olisi mahdollisimman turvallista, tarvitaan sopivia suojausmenetelmiä.

Vahva salaus

Luotettava suojaus saadaan aikaan käyttämällä vahvoja salaustekniikoita. Vahvoilla salaustekniikoilla tarkoitetaan tekniikoita, jotka eivät tämän hetken tietämyksen perusteella ole murrettavissa järjellisessä ajassa ja järjellisillä resursseilla. Tiedon salaus ei ole kuitenkaan ratkaisu kaikkiin tietoturvaongelmiin. Vahva salaus on kuitenkin ainoa keino toteuttaa turvallisia tietojärjestelmiä, jos verkkoympäristö ei ole turvallinen.

Mitä salakirjoitus on?

Salakirjoitus eli salaus (encryption) on selväkielisen tekstin muuttamista salattuun muotoon sopivaa matemaattista menetelmää (algoritmi) ja avainta käyttäen. Salakirjoitus voidaan muuttaa takaisin ymmärrettävään muotoon purkamalla eli tulkitsemalla (decryption) salakirjoitettu teksti avaimella. Kryptografia (cryptography) on salausta, salausalgoritmeja ja myös tarkistussummia käsittelevä matematiikan haara. Termiä käytetään myös salaustekniikoista puhuttaessa.

Ehkä paras kirja kryptografiasta ja algoritmeista on “Bruce Schneier: Applied Cryptography” [Sch1].

Millainen on hyvä salausalgoritmi?

Hyvin toteutetuissa salausalgoritmeissa salauksen purku onnistuu vain oikealla avaimella. Julkinen algoritmi, jota on tutkittu pitkään ja todettu varmaksi, on yleensä turvallinen käyttää. Ei ole syytä luottaa järjestelmiin, jotka perustuvat salaiseen algoritmiin. Salassa kehitelty ja salassa pidetty algoritmi saattaa olla turvallinen, mutta se voi myös sisältää tarkoituksella siihen suunnitellun takaoven. Kaikkiin uusiin algoritmeihin kannattaa suhtautua varauksella, koska niitä ei ole ehditty tutkia ja testata riittävän pitkään. Yleisesti voidaan sanoa, että kannattaa luottaa algoritmeihin, jotka ovat tunnettuja, julkisesti tutkittu ja testattu sekä jo käytössä olevia. Lisäksi kannattaa muistaa, että yhdessä sovelluksessa turvalliseksi osoittautunut algoritmi ei välttämättä ole turvallinen jossakin toisenlaisessa sovelluksessa.

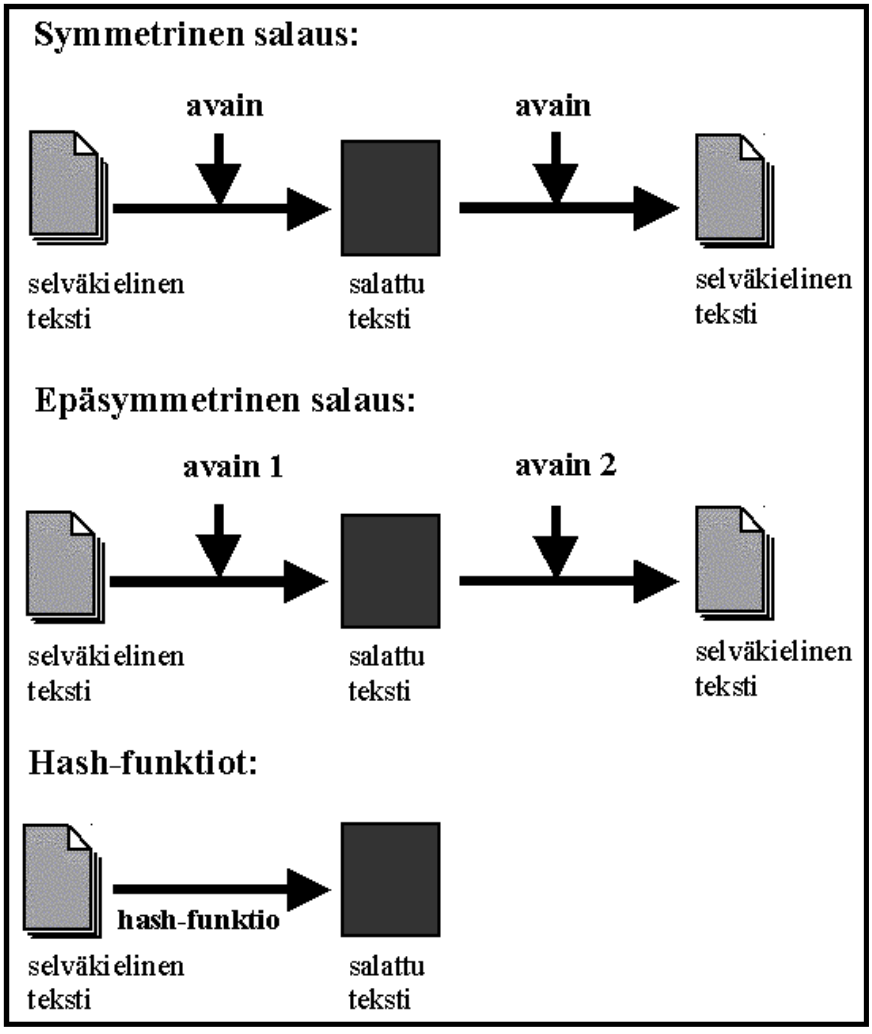
Algoritmin turvallisuuden lisäksi käyttäjän täytyy tarvittaessa ottaa vielä huomioon algoritmin lisenssi- ja patenttiasiat sekä eri maiden vienti- ja tuontisäännökset.

Lisätietoja algoritmeista löytyy mm. lähteistä [Stallings], [SSH1] ja [Kessler].

Salauksen päämenetelmät

Symmetrinen eli salaisen avaimen menetelmä

Symmetrisessä eli salaisen avaimen menetelmässä (secret key cryptography) salaus puretaan samalla avaimella, jolla se salakirjoitettiin. Jos menetelmää käy-



tetään tiedon välitykseen, ongelmana on avaimen turvallinen välitys toiselle osapuolelle. Turvallisen välityskanavan toteutus tulee yleensä maksamaan paljon. Symmetriset salaukset sopivat kuitenkin hyvin tapauksiin, joissa salausavainta ei tarvitse siirtää, esim. käyttäjän hakemistojen salaus.

Useimmat symmetriset salausalgoritmit salaavat tiedon määrätyn kokoisissa lohkoissa (block ciphers) ja toteuttavat usein useita kierroksia (8-32) jotakin yksinkertaista epälineaarista funktiota (esim. Feistel [Feistel]). Kukin lohko on yleensä 64 tai 128 bitin pituinen. Pienissä osissa toteutetun salauksen murtamista pidetään yleisesti vaikeampana, joten pieni lohkokoko on yleensä turvallisempi. Tietolohkot salataan yksitellen. Kunkin lohkon lopputulos on joko täysin itsenäinen tai siihen on vaikutusta muiden lohkojen tuloksilla. Jälkimmäisessä tapauksessa salattavan tiedon kaksi identtistä lohkoa antavat erilaisen tuloksen, ja se on käytännössä turvallisempi menetelmä. On olemassa useita vakiintuneita tapoja, joilla algoritmit käsittelevät lohkoja, esim. ECB (Electronic Code Book), CBC (Cipher Block Chaining), PCBC (Propagating Cipher Block Chaining), CFB (Cipher Feedback) ja OFB (Output Feedback). Näistä lohkojen käsittelytavoista löytyy enemmän tietoja mm. lähteestä [RSA2]. Symmetriset salausalgoritmit voivat myös lohkojen sijaan operoida suoraan esim. yksittäisillä biteillä tai tavuilla (stream chiphers).

Symmetriset algoritmit ovat laskennallisesti nopeita. Symmetristen algoritmien nopeuksista löytyy tietoja mm. lähteistä [Brown] ja [Sch2].

Symmetristä salausta pidetään yleisesti varmana, jos avaimen pituus on enemmän kuin 90 bittiä (mm. M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson ja M. Weiner [Blaze]). Varmana pidettyjä symmetrisiä algoritmeja ovat mm. Blowfish [Blowfish] ja IDEA [IDEA].

Epäsymmetrinen eli julkisen avaimen menetelmä

Epäsymmetrinen eli julkisen avaimen menetelmä (public key cryptography) perustuu kahden avaimen käyttöön. Toista avainta käytetään tiedon salaamiseen, ja toista käytetään salauksen purkamiseen. Avaimen välitysongelma on näin vältetty. Avaimet ovat toistensa vastakappaleita. Kumpikaan avaimista ei kerro toisesta avaimesta mitään, vaikkakin niillä on tietty matemaattinen yhteys. Kun tieto salataan avaimella, niin salattu tieto voidaan purkaa vain ja ainoastaan ko. avaimen vastakappaleella. Toinen avain on julkinen, ja käyttäjä voi luovuttaa sen haluamilleen tahoille. Toinen avain on salainen, ja se on vain käyttäjän tiedossa. Salaus etenee nyt suoraviivaisesti niin, että lähettäjä salaa tiedon vastaanottajan julkisella avaimella ja lähettää salatun tiedon vastaanottajalle. Vastaanottaja purkaa salatun tiedon omalla salaisella avaimellaan.

Menetelmää voidaan käyttää myös niin, että lähettäjä liittää mukaan **digitaalisen allekirjoituksen** ja salaa sen omalla salaisella avaimellaan. Vastaanottaja tulkitsee tämän allekirjoituksen lähettäjän julkisella avaimella. Tätä tapausta käytetään silloin, jos halutaan, että lähettäjä ei voi jälkikäteen kieltää lähettäneensä tietoa (kiistämättömyys) tai halutaan varmentaa, että tieto tuli oikealta henkilöltä. Lisäksi tiedosta voidaan sopivalla yksisuuntaisella hash-funktiolla laskea hash-koodi eli nk. tiiviste, joka liitetään digitaaliseen allekirjoitukseen. Pienikin muutos tiedon sisällössä aiheuttaa sen, että tämä tiiviste muuttuu. Digitaalinen allekirjoitus todistaa tiedon alkuperän ja samalla takaa sen eheyden. Digitaalinen allekirjoitus koostuu käytännössä otsikkokentästä, käyttäjän tunnisteesta ja tiivisteestä. Tiivisteitä voidaan käyttää aineiston eheyden varmistamiseen myös ilman digitaalista allekirjoitusta.

Epäsymmetrinen salaus sopii hyvin tiedon välitykseen. Sitä voidaan käyttää esim. todennukseen, allekirjoituksiin ja avaintenhallintaan. Epäsymmetrinen salaus on kuitenkin hidasta, koska se edellyttää hyvin pitkiä avaimia riittävän turvallisuuden takaamiseksi. Lisäksi salatun tiedon koko saattaa olla huomattavasti suurempi kuin alkuperäisen selväkielisen tiedon. Myös julkisten avainten käsittelyyn liittyy ongelmia. Käyttäjän tulee voida varmistua mm. siitä, että hän sai oikean henkilön julkisen avaimen ja että saatu avain on voimassa. Yleisesti varmenne eli sertifikaatti on jonkin luotetun ja tunnetun tahon (varmenneviranomainen, Certification Authority, CA) digitaalinen allekirjoitus julkiselle avaimelle.

Yleensä epäsymmetrisen salauksen turvallisuus perustuu modulaariseen aritmetiikkaan ja johonkin vaikeaksi oletettuun matemaattiseen ongelmaan. RSA (Rivest, Shamir, Adleman) [RSA] on tällä hetkellä yleisin käytössä oleva epäsymmetrinen salausalgoritmi, ja sen turvallisuus pohjautuu olettamukseen, että suurten lukujen tekijöihin jakaminen (faktorointi) on vaikeaa. Asiaa ei ole todistettu, mutta käytäntö ei ainakaan toistaiseksi ole osoittanut muuta. Matemaatikot ovat jo yli kaksituhatta vuotta yrittäneet keksiä nopean menetelmän jakaa luku tekijöihinsä siinä onnistumatta.

Jos arvioi RSA-avaimen turvallisuutta tulevaisuudessa, niin täytyy ottaa huomioon sekä kehitysaskeleet faktoroinnissa että tietokoneiden ja verkkojen nopeuksien kehittyminen. Algoritminä RSA on yleisesti hyväksytty ja sitä pidetään turvallisena, jos käytetään riittävän pitkää avainta. Alle 1.5K bitin salausavaimia kannattaa tällä hetkellä käyttää vain lyhytaikaiseen salaukseen.

Hybridijärjestelmät

Epäsymmetriset salaukset ovat hitaita. Symmetrinen salaus on noin 1000 kertaa nopeampaa kuin epäsymmetrinen salaus. Käytännössä tämä on usein johtanut symmetrisen ja epäsymmetrisen tekniikan yhdistämiseen hybridijärjestelmiksi. Siirrettävä tieto salataan ensin symmetrisellä algoritmilla, ja käytetty salausavain salataan epäsymmetrisellä salauksella, ja se liitetään salattuun tietoon.

Elliptiset käyrät

Yleisellä tasolla elliptisten käyrien salaus (elliptic curve cryptosystem, ECC) vastaa epäsymmetristä menetelmää, mutta siinä modulaarinen aritmetiikka on korvattu operaatioilla, jotka määritellään elliptisillä käyrillä. Elliptisten käyrien salaus saattaa yleistyä, koska siinä saavutetaan turvallisuus pienemmällä avaimen bittimäärällä kuin epäsymmetrisellä

menetelmällä. Elliptisten käyrien salausta ei ole tutkittu kovin pitkään, joten sen heikkouksia saattaa vielä tulla esiin. Lisätietoja elliptisistä käyristä löytyy mm. lähteistä [Certi], [UCL] ja [IsI].

Hash-funktiot

Hash-funktiot eli tiivistefunktiot (hash fuction tai message digest/fingerprint/compression function) ovat yksisuuntaisia funktioita. Hash-funktiolla voi laskea/tiivistää tiedolle nopeasti niin sanotun hash-koodin eli tiivisteen. Hash-koodin pituus on tyypillisesti 128 tai 160 bittiä, kun itse lähtötieto voi olla mielivaltaisen pituinen. Turvallisen hash-koodin minimipituus onkin nykyään vähintään 128 bittiä. On käytännössä mahdotonta löytää kahta erilaista tietoa, joilla olisi sama hash-koodi. Hash-funktio on siis törmäyksetön (ns. collision resistant). Pienikin muutos lähtötiedossa aiheuttaa suuren muutoksen hash-koodiin (ns. avalanche effect). Hash-fuktiot ovat julkisia ja niiden turvallisuus perustuu yksisuuntaisuuteen. Lisätietoja hash-funktioista löytyy mm. lähteistä [RSA3] ja [Jenkins].

Steganografia

Steganografia on vanha tieteenhaara, joka käsittelee tiedon piilottamista toiseen tietoon. Perinteisen kryptografian tavoitteena on salata tiedon sisältö, kun taas steganografian tavoitteena on salata myös tiedon olemassaolo. Steganografia merkitsee salaisen tiedon välittämistä viattomalta näyttävän tiedon mukana, esim. kuvassa tai musiikkiäänitteessä. Yleensä tämä salainen tieto on vielä salattu, jotta sitä ei löydettäessäkään pystytä tulkitsemaan. Viime vuosina on ollut tavoitteena mm. kehittää steganografialla käyttökelpoisia menetelmiä, joilla copyright-teksti tai sarjanumero voidaan piilottaa esim. elokuviin, kirjoihin ja musiikkiäänitteisiin. Lisätietoja steganografiasta löytyy mm. lähteestä [Johnson1]. Tietoja työvälineistä ja ohjelmista löytyy lähteestä [Johnson2].

Salaustuotteiden saatavuus

Salaustuotteiden saatavuutta maailmalla rajoittavat vientivalvontasäännökset. Vientivalvontaa koskevaa niin sanottua Wassenaar-sopimusta laajennettiin joulukuussa 1998, jolloin 33 maata (myös Suomi) hyväksyivät sen. Sopimuksen mukaan vientivalvonnan piiriin kuuluvat mm. yli 64 bittiset massajakeluun tarkoitetut salausohjelmistot, jotka eivät ole julkisia. Julkisia ovat ohjelmistot, jotka ovat saatavilla ilman edelleenlevitystä koskevia rajoituksia. Lisätietoja Wassenaar-sopimuksesta löytyy lähteestä [Wass].

USA on ollut vientirajoitusten johtava kannattaja ja on myös painostanut muita maita rajoituksiin. USA ilmoitti kuitenkin syyskuussa 1999 löysäävänsä merkittävästi vahvojen salaustuotteiden vientikieltoa [White]. Muutos tuli voimaan tammikuussa 2000. Jokainen maasta lähtevä salausohjelma joutuu kuitenkin tekniseen tarkastukseen ennen vientiluvan saamista. Vientikelpoisten ohjelmien kriteereistä ei saa tietoja. Heinäkuussa 2000 USA helpotti säännöksiä tiettyjen maiden osalta (mm. EU-maat) lähinnä vastauksena EU:n vastaaville muutoksille. Lisätietoja USA:n vientisäännöksistä löytyy lähteestä [BXA].

Liikeyritykset ja kansalaisoikeuksien puolustajat kannattavat vahvaa salausta, kun taas lainvalvojat ovat olleet rajoitusten kannalla. Tietoja vientivalvontasäännösten soveltamisesta eri maissa löytyy lähteestä [Koops].

Suomessa erilaisten salaustuotteiden kehittäminen on ollut tehokasta, ja hyviä salaustuotteita on ollut saatavilla omasta takaa.

Salaustuotteiden käyttö

On todennäköistä, että tulevaisuudessa kaikki tietoliikenne yritysten ja muiden vastaavien yksiköiden välillä kulkee salattuna. Jo tällä hetkellä salaustekniikoita ja salaustuotteita käytetään laajasti, ja monille aloille niiden käyttö on perusedellytys, esim. sähköisen kaupankäynnin ja sähköisen rahan onnistuneen toteutuksen edellytys on salaustekniikoiden tehokas hyödyntäminen. SSH-ohjelmistoa (Secure Shell) [SSH2] käytetään turvaamaan TCP/IP-yhteydet vahvalla salauksella (esim. etäyhteydet, asiakas-palvelin -yhteydet, tiedostojen siirrot). SSH:lla voidaan toteuttaa myös VPN (Virtual Private Network). VPN-ratkaisuilla salataan lähiverkon ja/tai julkisen verkon (esim. Internet) välinen liikenne, jolloin julkisen verkon yli operointi onnistuu vastaavalla tavalla kuin yrityksen omassa verkossa.

Sähköposti

Sähköpostissa salaustekniikoita on käytetty jo pitkään. Sähköpostin salaus onkin tehokas keino estää eri koneiden kautta kulkevien viestien väärinkäyttö. Digitaalisella allekirjoituksella voidaan varmentaa, että viesti tuli oikealta henkilöltä. Hash-funktiolla voidaan varmentaa viestin muuttumattomuus.

Tällä hetkellä on käytännössä kaksi eri protokollaa sähköpostin salaamiseen: S/MIME (Secure/Multipurpose Internet Mail Extensions) ja PGP (Pretty Good Privacy). Myös muita protokollia on ehdotettu aikaisemmin, esim. PEM (Privacy Enhanced Mail) ja MOSS (MIME Object Security Service), mutta niiden käyttö on jäänyt vähäiseksi. S/MIME on toteutettu useissa yleisesti käytössä olevissa sovelluksissa. Salauksen vahvuus kannattaa tarkistaa sovelluskohtaisesti, koska S/MIME (v2) on käyttänyt oletusarvoisesti heikkoa salausta (40 bittiä). PGP on hyvä esimerkki hybridijärjestelmästä, ja se on tällä hetkellä eniten käytössä oleva sähköpostin salaamiseen käytetty menetelmä. PGP on ainakin toistaiseksi toteuttanut vain vahvaa salausta. Lisätietoja sähköpostin salauksesta löytyy mm. lähteistä [PGP], [IMC] ja [IETF1-2].

Tiedostot ja hakemistot

Yhdysvaltalaisen vakuutusyhtiön selvityksen mukaan joka kymmenes kannettava tietokone varastetaan lentokentällä [Safeware]. Toinen otollinen paikka varkauksille on hotelli tai auto. Varastetun kannettavan tietosisältö on helppo hyödyntää, jos tietoa ei ole vahvasti salattu. Luottamukselliset tiedot eivät aina ole turvassa käyttäjän työhuoneessa käyttäjän omalla työasemallakaan ilman vahvaa salausta.

Tiedostojen, hakemistojen ja levyalueiden salaukseen löytyy helppo-

Tuotenimi	Omistaja/kehittäjä	Alusta[1]	Hinta[2]	Lisätietoja
BestCrypt	Jetico, Tampere	DOS, Win 3.xx /95/98/NT/ 2000, Linux	$89.95 (Win 95/98 /NT/2000)	http://www.jetico.sci.fi/
CodedDrag	Linzin yliopisto, Itävalta	Win 95/NT	$30	http://www.fim.uni-linz.ac.at/codeddrag/codedrag.htm
Cryptext	Nick Payne	Win 95/98/NT	freeware	http://www.pcug.org.au/~njpayne/index.html
Crypto	Gregory Braun	Win 95/98/NT/ 2000	$20	http://www.gregorybraun.com/Crypto.html
DataGuard	Secure Link Services (SLS), Sveitsi	Win 95/NT	$49	http://www.sls.net/dataguard_v15.html
ECBackup	SoftLab, Ukraina	Win 95/98/NT	$30	http://softlab.od.ua/
ECD, EHD	'Id Est'	Linux	freeware	http://members.home.net/id-est/
Encrypt Easy	BaltSoft, Liettua	Win 95/98/NT	$19	http://www.baltsoft.com/
Enigma 98	CryptoSoft, Saksa	Win 95/98/NT	$69	http://www.cryptosoft.com/
FileCrypto	F-Secure, Espoo	Win 95/98/NT	$119	http://www.f-secure.fi/products/filecrypto/
FileGuard	Highware, Belgia	Mac	$159	http://www.Highware.com/
Interscope BlackBox	Interscope, Romania	Win 95/98/NT/ 2000	$35	http://www.essentialdetails.com/blackbox/
JumBlo	Siskin Software, Irlanti	Win 95/NT	$15	http://homepage.tinet.ie/~siskin/products.html
Protect!	Protect Data, Ruotsi	Win 95/98/NT	1200 mk	http://www.protectdata.fi/index.htm
Protect	Decros, Tsekki	Win 95/98/NT	$99	http://www.decros.com/
SAFE Folder	GlobeTech Catana, Ruotsi	Win 95/98	$57.95	http://www.globetech.se/
Scramdisk	'Sam Simpson', Iso-Britannia	Win 95/98	freeware	http://www.scramdisk.clara.net/
S-Crypto	Ascit, Hollanti	Win 95/98/NT	38.23 euroa	http://www.ascit.com/info13.htm
StrongCrypt	Waqas Shafiq, Pakistan	Win 95/98/NT	$20	http://wshafiq.webjump.com/StrongCrypt.html
StrongDisk	PhysTechSoft, Venäjä	Win 95/98/NT/ 2000	$79.95	http://www.PhysTechSoft.com/en/StrongDisk/
Tresor	Warlord, Sveitsi	Mac	25 euroa	http://www.warlord.li/english/products.html
WinCrypt 95	F.I.S. Group, Latvia	Win 95/98/NT	$70	http://www.fis.lv/navigator/aboutframeset.html
WinSafe	Patrik Nilsson, Ruotsi	Win 95/98/NT	$25	http://www.pbnsoft.com/winsafe/information.htm
Y3K S-CRYPT 2000	Y3K Software, Iso-Britannia	Win 95/98/NT	$20	http://www.y3k-software.com/crypt.html

1) Windows 2000 -tuki oli tekeillä useille tuotteille. Taulukon tiedot vastaavat tietojen keruuhetken (2.10.2000) tilannetta.
2) Hinta on yhden käyttäjän lisenssin hinta. Hinta on USA:n dollareissa ellei toisin ole mainittu.

Taulukko 1: Tiedostojen/hakemistojen/levyalueiden salaustuotteita

käyttöisiä ja edullisia tuotteita (Taulukko 1). Salaustuotteesta on syytä tarkistaa aina erikseen salauksen voimakkuus. Maahantuotujen tuotteiden salausta on saatettu heikentää kyseisen maan vientisäännösten edellyttämällä tavalla.

Java-ohjelmistokehitys

JCE (Java Cryptography Extension) [Sun1-2] toi Java JDK Security API:iin vahvan salauksen. Sunin JCE-pakettia ei ole sellaisenaan saanut tuoda USA:n ja Kanadan ulkopuolelle. Tänä vuonna Sun alkoi toimittaa erilliset paketit koti- ja ulkomarkkinoille. Ulkomarkkinoiden versiossa on rajoituksia avaimien pituuksille. Symmetrisen salauksen algoritmien avaimen pituus rajoitettiin 64 bittiin ja epäsymmetrisen salauksen (RSA) 512 bittiin.

Myös korvaavia ja/tai täydentäviä tuotteita Sunin JCE:lle löytyy, ja ilman turvallisuutta vähentäviä rajoituksia. Cryptix JCE on todennäköisesti eniten käytetty näistä tuotteista. Jos salauskirjaston käyttäjä haluaa varmistua tuotteen turvallisuudesta, niin kannattaa varmistaa lähdekoodin saatavuus. Ainakin Taulukon 2 tuotteista lähdekoodi on tarvittaessa saatavissa.

Toteutus ratkaisee

Algoritmin vahvuus ja avaimen riittävä pituus eivät vielä takaa turvallista salausta. Melko harvoin hyökkäykset kohdistuvat itse salausalgoritmia vastaan, koska vahva salausalgoritmi ei ole purettavissa järjellisessä ajassa. Vahva salaus on tehokas, jos se on toteutettu oikein. On mahdollista suunnitella heikko salausjärjestelmä käyttämällä vahvoja algoritmeja ja protokollia.

Vahva salausalgoritmi ei auta, jos järjestelmä on toteutettu huonosti, ja käyttöliittymä, avaintenhallinta tai salasanojen

Tuotenimi	Omistaja/kehittäjä	Hinta/lisenssi	Lisätietoja
Cryptix JCE	The Cryptix Foundation Limited	Cryptix General License (Open Source)	http://se.cryptix.org/index.html
IAIK-JCE	IAIK (Institute for Applied Information Processing and Communications), Itävalta	alkaen 500 euroa	http://jcewww.iaik.tu-graz.ac.at/jce/jce.htm
JCSI	DSTC, Australia	kaupall. käytössä maksullinen	http://security.dstc.edu.au/projects/java/jcsi.html
Open JCE	eSec Limited, Australia	eSec Public Licence (Open Source)	http://www.openjce.org/
Forge Security Provider	Forge Information Technology, Australia	freeware	http://www.forge.com.au/

Tauluko 2: Java-salauskirjastoja

hallinta ei ole kunnossa. Järjestelmä ei esimerkiksi huolehdi, että salaamaton selväkielinen tieto (ja myös kaikki sen väliaikaiset esiintymät) hävitetään turvallisesti salauksen jälkeen tai järjestelmä ei huolehdi, että avain/salasana on kaikissa käyttökohteissa vahva tai järjestelmä mahdollistaa vanhojen avainten palauttamisen ja samalla antaa myös mahdollisille väärinkäyttäjille enemmän mahdollisuuksia. Puute avaintietokannassa voi mahdollistaa tietokannan väärinkäytön.

Jos on mahdollista, että salasana voi joutua väärän henkilön käsiin, niin salainen avain on syytä tallettaa paikkaan, josta ei edes salasanan haltuunsa saanut henkilö voi sitä lukea. Salasanat, joiden takana on arvokkaita tietoja, kannattaa arkistoida turvalliseen paikkaan. Jos salasana unohtuu, vahvalla salauksella salattu tieto ei ole purettavissa ja siten käyttökelvoton. Yrityksen pitää järjestää salasanojen ja salausavainten hallinta niin, että tieto on purettavissa myös silloin, kun tiedon vakituinen haltija on lomalla, sairas tms.

Usein salausjärjestelmän heikoin kohta on sen satunnaislukugeneraattori. Satunnaislukugeneraattoreilla luodaan salausjärjestelmän avaimet, ja joissakin tapauksissa niitä käytetään myös itse salakirjoituksessa tai digitaalisessa allekirjoituksessa. Satunnaislukugeneraattori saattaa tuottaa heikkoja avaimia. Satunnaislukugeneraattorien ongelmista löytyy enemmän tietoja lähteestä [Kelsey].

Jos salausjärjestelmä perustuu laitteiston turvallisuuteen, niin on syytä suunnitella aina laitteistoa täydentävä turvallisuusmekanismi. Laitteiston viat ja häiriöt voivat olla riski salausjärjestelmälle, ja joku voi yrittää tuottaa niitä tahallisesti saadakseen selville esim. salaisen avaimen. On myös toteutettu hyökkäyksiä salausta vastaan, jotka perustuvat esim. laitteiston virrankulutuksen tai säteilyn mittaamiseen [Timing].

Viime kädessä salausjärjestelmänkin turvallisuus perustuu luottamukseen, esim. luottamukseen järjestelmän käyttäjään, luottamukseen työaseman turvallisuuteen, luottamukseen verkkoprotokollan turvallisuuteen, luottamukseen julkisen avaimen lähteeseen jne. Olisikin aina syytä selvittää tarkemmin keneen tai mihin salausjärjestelmä luottaa, millä tavalla ja missä laajuudessa, ja pyrkiä vahvistamaan tämä luottamus luottamuksen arvoiseksi.

Monissa tavanomaisissa järjestelmissä riittää, että ohjelma toimii. Salausjärjestelmissä asia ei ole näin yksinkertainen. Jos salausohjelma toimii, se ei vielä kerro mitään salauksen turvallisuudesta. Hyväkään suunnittelu ja toteutus ei voi estää kaikkia inhimillisiä erehdyksiä mutta voi välttää useita, esim. järjestelmässä on oletusarvoisesti vahva salaus, ja käyttäjä ei voi vahingossa käyttää heikkoa salausta.

On tietysti hyvä toimia sillä periaatteella, että kaikki salausjärjestelmät voidaan murtaa ennemmin tai myöhemmin, ja varautua tällaiseen tilanteeseen jo etukäteen mahdollisten vahinkojen minimoimiseksi. Jos kvanttitietokoneista tulee joskus todellisuutta, silloin kaikki nykyiset salakirjoitukset olisivat hyödyttömiä ja olisi pakko siirtyä uusiin salaustekniikoihin (esim. kvanttikryptografia). Kilpajuoksu jatkunee.

Tuula Käpylä,
VTT Tietotekniikka,
Tekniikantie 4 B, Espoo
PL 1201, 02044 VTT
Puh: (90) 456 6054
Email: Tuula.Kapyla@vtt.fi
Fax: (90) 456 6027

Lähdeluettelo

[Blaze] Blaze, M., Diffie, W., Rivest, R., Schneier, B., Shimomura, T., Thompson, E., Wiener, M., Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, January 1996.

[Blowfish] The Blowfish Encryption Algorithm: http://www.counterpane.com/blowfish.html

[Brown] Lawrie Brown, A Current Perspective on Encryption Algorithms: http://www.adfa.oz.au/~lpb/papers/unz99.html

[BXA] Bureau of Export Administration (BXA) in the U.S. Regulations governing exports of encryption: http://www.bxa.doc.gov/Encryption/

[Certi] Certicom's Web site, Elliptic curves: http://www.certicom.com/research.html

[Feistel] Horst Feistel, Cryptography and Computer Privacy, Scientific American, May 1973. http://www.rsasecurity.com/rsalabs/faq/2-1-4-1.html

[IDEA] IDEA algorithm: http://www.it-sec.com/idea.html

[IETF1] The Internet Engineering Task Force, S/MIME Working Group: http://www.imc.org/ietf-smime/

[IETF2] The Internet Engineering Task Force, OpenPGP Working Group: http://www.imc.org/ietf-open-pgp/

[IMC] Internet Mail Consortium, S/MIME and PGP/MIME -- Information on the two leading end-to-end mail security solutions: http://www.imc.org/smime-pgpmime.html

[IsI] Integrity Sciences, Elliptic curves: http://world.std.com/~dpj/elliptic.html

[Jenkins] Bob Jenkins, Hash Functions and Block Ciphers: http://burtleburtle.net/bob/hash/index.html

[Johnson1] Neil F. Johnson, Steganography & Digital Watermarking: http://isse.gmu.edu/~njohnson/Steganography/

[Johnson2] Neil F. Johnson, Steganography Tools: http://www.jjtc.com/Security/stegtools.htm

[Kelsey] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, Cryptanalytic Attacks on Pseudorandom Number Generators: http://www.counterpane.com/pseudorandom_number.html

[Kessler] Gary C. Kessler, An Overview of Cryptography: http://www.hill.com/library/staffpubs/crypto.html

[Koops] Bert-Jaap Koops, Crypto Law Survey: http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm

[PGP] The International PGP Home Page: http://www.pgpi.org/

[RSA] RSA Security FAQ: What is RSA? http://www.rsasecurity.com/rsalabs/faq/3-1.html

[RSA2] RSA Security FAQ: What is a block cipher?: http://www.rsasecurity.com/rsalabs/faq/2-1-4.html

[RSA3] RSA Security FAQ: What is a hash function?: http://www.rsasecurity.com/rsalabs/faq/2-1-6.html

[Safeware] Safeware, The Insurance Agency Inc.: http://www.safeware.com/

[Sch1] Bruce Schneier, Applied Cryptography, Second Edition: protocols, algorithms, and source code in C, John Wiley & Sons, 1996.

[Sch2] Speed Comparisons of Block Ciphers on a Pentium: http://www.counterpane.com/speed.html

[SSH1] SSH Communications Security, Introduction to Cryptography: http://www.ipsec.com/tech/crypto/intro.html

[SSH2] SSH Communications Security: SSH Secure Shell: http://www.ipsec.com/products/ssh/

[Stallings] William Stallings, Lecture Notes for Use with Cryptography and Network Security: http://williamstallings.com/Extras/Security-Notes/

[Sun1] Java Cryptography Extension: http://java.sun.com/products/jce/

[Sun2] Java Cryptography Extension 1.2, API Specification & Reference: http://spectral.mscs.mu.edu/javadev/security/jce1.2/doc/guide/API_users_guide.html

[Timing] Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems: http://www.cryptography.com/timingattack/

[UCL] Microelectronics Laboratory, Some references on elliptic curves: http://www.dice.ucl.ac.be/crypto/joye/biblio_ell.html

[Wass] Wassenaar Arrangement: http://www.wassenaar.org/

[White] The White House, Administration Updates Encryption Export Policy: http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1999/9/16/15.text.1

Muita salaukseen liittyviä lähteitä

CERT, The CERT Coordination Center provides information about the security of networked computing systems: http://www.cert.org/
Cipher, The newsletter of the IEEE Computer Society's Technical Committee on Security and Privacy. http://www.ieee-security.org/cipher.html
CRYPTO-GRAM: A free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography (Bruce Schneier): http://www.counterpane.com/crypto-gram.html
Cryptology ePrint Archive, recent research in cryptology: http://eprint.iacr.org/
Cryptome, Recent cryptography news and announcements: http://cryptome.org/
David Wagner, A list of cryptography researchers with Web pages: http://www.cs.berkeley.edu/~daw/people/crypto.html
EPIC's Cryptography Policy Archives: http://www.epic.org/crypto/
Francis Litterio, The Study of Encryption: http://world.std.com/~franl/crypto.html
Index of cryptography papers available online, Counterpane Internet Security: http://www.counterpane.com/biblio/
International Crytology Conference (CRYPTO): http://joinus.comeng.chungnam.ac.kr/~dolphin/db/conf/crypto/index.html
Java Security Features: http://java.sun.com/docs/books/tutorial/security1.2/overview/index.html
Java security Q&A archive: http://java.sun.com/security/hypermail/java-security-archive-3/index.html
Lawrence E. Widman, Privacy and Security on the Internet: http://www.med-edu.com/internet-security.html
M. Silvestri, Standards, references, guidelines: http://www.wowarea.com/english/help/crystd.htm
Peter Gutmann, Encryption and Security-related Resources: http://www.cs.auckland.ac.nz/~pgut001/links.html
Peter Gutmann, Secure Deletion of Data from Magnetic and Solid-State Memory: http://www.cs.auckland.ac.nz/~pgut001/secure_del.html
Pointers to cryptographic software, Computer Network Lab: http://netwk.hannam.ac.kr/link/crypto/software.html
Pointers to cryptography and information security pages, Dis.Org: http://www.dis.org/erehwon/crypto.html
Rohit Khare and Adam Rifkin, Weaving a Web of Trust: http://www.cs.caltech.edu/~adam/papers/trust.html
Ron Rivest's list: http://theory.lcs.mit.edu/~rivest/crypto-security.html
Sci.crypt URLs: http://www.ar.com/ger/sci.crypt.html
SIRENE's security and cryptography list: http://www.semper.org/sirene/outsideworld/security.html#spec
Terry Ritter, Learning About Cryptography: http://www.io.com/~ritter/LEARNING.HTM
The FUNET crypto archive: ftp.funet.fi:/pub/crypt
The IETF Security Area: http://web.mit.edu/network/ietf/sa/
Tom Dunigan's security pointers: http://www.epm.ornl.gov/~dunigan/security.html
Yahoo on security and encryption: http://dir.yahoo.com/computers_and_internet/security_and_encryption/
Zedz Consultants, Freedom Tools for Citizen Units: http://www.zedz.net/

FAQ (Frequently Asked Questions) -lähteitä

Alt.2600/#hack FAQ: http://linuxsavvy.com/staff/jgotts/hack-faq/
Anonymous remailer FAQ by André Bacard: http://www.andrebacard.com/remail.html
Computer Security FAQ: http://www.faqs.org/faqs/computer-security/
Computer Virus FAQ: http://www.faqs.org/faqs/computer-virus/
Cryptography FAQ: http://www.faqs.org/faqs/cryptography-faq/
Elliptic Curve Crypto FAQ by George Barwood: http://cryptoman.com/elliptic.htm
Hash Function FAQ by Bob Jenkins: http://burtleburtle.net/bob/hash/hashfaq.html
Internet Firewalls FAQ by Matt Curtin and Marcus J. Ranum: http://www.interhack.net/pubs/fwfaq/
Locksmithing FAQ: http://www.indra.com/archives/alt-locksmithing/
PGP DH vs. RSA FAQ: http://www.scramdisk.clara.net/pgpfaq.html
PGP FAQ: http://www.faqs.org/faqs/pgp-faq/
RSA Laboratories' Cryptography FAQ: http://www.rsasecurity.com/rsalabs/faq/
SSH FAQ by Thomas König: http://www.uni-karlsruhe.de/~ig25/ssh-faq/
The comp.security.pgp FAQ by Arnoud Engelfriet: http://www.dk.pgp.net/pgpnet/pgp-faq/
The passphrase FAQ for PGP: http://www.stack.nl/~galactus/remailers/passphrase-faq.html#101
The PGP Attack FAQ by infiNity: http://www.stack.nl/~galactus/remailers/attack-faq.html
The World Wide Web Security FAQ: http://www.w3.org/Security/Faq/