TIETOTURVAN PERUSTEET, Luku 1: Yleistä tietoturvasta

T. Karvi

Tammikuu 2011

Turvallisuuskoulutus turvallisuusjohdolle I

Organisaatioiden turvallisuus on hyvin laaja alue, josta tietoturvallisuus muodostaa vain pienen osan. Erään kaupallisen turvallisuuskurssin asioita:

- Turvallisuus yrityksen tai organisaation toiminnassa ja turvallisuuden johtaminen.
- Turvallisuusriskien tunnistaminen ja hallintakeinot.
- Turvallisuustoiminnan lainsäädännöllinen viitekehys.
- Turvallisuusviestintä ja -tiedottaminen, turvallisuuskoulutus.
- Tuotannon ja toiminnan turvallisuus.
- Työturvallisuus.
- Pelastustoiminta.
- Ympäristöturvallisuus.
- Varautuminen ja jatkuvuussuunnittelu.
- Tietoturvallisuus.

Turvallisuuskoulutus turvallisuusjohdolle II

- Tietotekninen turvallisuus.
- Tilaturvallisuus- ja turvallisuusvalvonta.
- Taloushallinnon ja varainhoidon turvallisuus.
- Henkilöturvallisuus ja ulkomaantoimintojen turvallisuus.
- Security Management.
- Turvallisuussuunnitelmat ja -projektit.
- Turvallisuuden kehittäminen ja johtaminen.

Tietoturvan jaottelut I

Tietoturva on myös laaja alue. Seuraavassa listassa on lueteltu tietoturvan eri osa-alueita. Jaottelu on melko yleinen ja se esitetään yleisissä tietoturvan oppikirjoissa.

- Hallinnollinen turvallisuus kattaa ne toimenpiteet, joilla määrätään organisaatiossa noudatettavat periaatteet ja toimintalinjat: turva-, toipumis- ja valmiussuunnitelmat.
- Henkilöstöturvallisuus kattaa henkilöstöön liittyvien luotettavuusriskien hallinnan toimenkuvien, käyttöoikeuksien määrittelyjen sekä turvallisuuskoulutuksen ja valvonnan avulla.
- Fyysiseen turvallisuuteen sisältyy laitteisto-, käyttö- ja varastointitilojen, arkistojen sekä laitteiden ja materiaalien fyysinen suojaus sekä tietoverkon kaapeloinnin suojaus.
- Tietoliikenneturvallisuus kattaa ne toimenpiteet, joilla pyritään varmistamaan tietoverkossa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys.

Tietoturvan jaottelut II

- Laitteistoturvallisuuteen kuuluu laitteiden kokoonpanoon, kunnossapitoon ja laadunvarmistukseen liittyvät turvallisuusominaisuudet.
- Tietoaineistoturvallisuus sisältää asiakirjojen, tietueiden ja tiedostojen tunnistamisen ja turvallisuusluokituksen sekä tietovälineiden hallinnan ja säilytyksen kaikissa eri käsittelyvaiheissa luomisesta hävittämiseen saakka.
- Ohjelmistoturvallisuuteen kuuluu käyttöjärjestelmien, sovellusohjelmien ja tietoliikenneohjelmistojen turvallisuusominaisuudet.
- Käyttöturvallisuuteen kuuluu henkilöstön turvalliset käyttöperiaatteet, käyttöympäristöön ja varsinaisen tietojenkäsittelyn turvallisuuteen vaikuttavien tapahtumien valvonta sekä jatkuvuuden turvaamiseen liittyvien menettelyjen käyttö.

Erään kaupallisen tietoturvallisuuden koulutusohjelman sisältö I

- Tietoturvallisuus organisaation toiminnan osana.
- Tietoturvallisuutta koskeva lainsäädäntö ja viranomaistoiminta.
- Riskien tunnistaminen ja hallintakeinot.
- Tietoaineistojen luokitus ja valvonta.
- Järjestelmien kehittäminen ja ylläpidon turvallisuus.
- Laitteistojen ja ohjelmistojen turvallisuus.
- Salaustekniikat ja niiden hallinta.
- Tietoliikenneturvallisuus.
- Henkilöturvallisuus.
- Fyysinen turvallisuus.
- Käyttöturvallisuus ja tietojärjestelmien palveluiden hankinta.
- Liiketoiminnan jatkuvuuden hallinta.

Erään kaupallisen tietoturvallisuuden koulutusohjelman sisältö II

- Tietoturvallisuuden tarkastaminen ja kehittäminen.

Huomattakoon, että näillä kursseilla ei ole käsitelty turvallista ohjelmistosuunnittelua, ohjelmiston toteutusta ja testausta eikä turvaprotokollia.

Tietoturvaan liittyvä lainsäädäntö Suomessa I

Suomessa tietoturvaan liittyvää lainsäädäntöä on monissa laissa, jotka luetellaan seuraavassa listassa:

- perustuslain perusoikeussäännökset (731/1999)
- henkilötietolaki (523/1999)
- laki viranomaistoiminnan julkisuudesta (621/1999)
- laki sähköisestä asioinnista hallinnossa (12/2003)
- laki sähköisistä allekirjoituksista (14/2003)
- laki yksityisyyden suojasta työelämässä (759/2004)
- valtioneuvoston ohjesääntö (262/2003)
- arkistolaki (831/1994)
- asetus valtion talousarviosta (1243/1992)
- henkilökorttilaki (829/1999)
- väestötietolain muutos (527/1999)

Tietoturvaan liittyvä lainsäädäntö Suomessa II

- viestintämarkkinalaki (393/2003)
- valtion virkamieslaki (750/1994)
- rikoslaki ja laki rikoslain muuttamisesta (769/1990, 578/1995, 951/1999)
- valmiuslaki (1080/1991)
- laki puolustustaloudellisesta sunnittelukunnasta (238/1960)
- laki huoltovarmuuden turvaamisesta (1390/1992)
- pakkokeinolaki (450/1987, 403/1995, 1026/1995, 22/2001)
- laki turvallisuusselvityksistä (177/2002)
- sähköisen viestunnän tietosuojalaki (516/2004)
- laki kansainvälisistä tietoturvavelvoitteista (588/2004)

Keskeiset lait I

Keskeinen tietoturvallisuuteen vaikuttava lainsäädäntö löytyy rikoslaista ja pakkokeinolaista:

Rikoslaki:

- 38 luku, 3§, viestintäsalaisuuden loukkaus
- 38 luku, 4§, törkeä viestintäsalaisuuden loukkaus
- 38 luku, 5-7§, tietoliikenteen häirintä
- 38 luku, 8§, tietomurto
- 35 luku, 1.2§, vahingonteko
- 34 luku, 9a, vaaran aiheuttaminen tietojenkäsittelylle
- 34 luku, 9b, tietoverkkorikosvälineen hallussapito
- 28 luku, 7§, luvaton käyttö
- 28 luku, 8§, törkeä luvaton käyttö

Keskeiset lait II

Pakkokeinolaki(1026/1995):

- poliisiviranomaisen tiedonsaantioikeudet
- 2§, telekuuntelun edellytykset (viestin kuuntelu/tallettaminen salaa viestin sisällön selvittämiseksi)
- 3§, televalvonnan edellytykset (salassa pidettävien tunnistetietojen hankkiminen viesteistä)

Uutena lakina Lex Nokia (harjoitustehtävä).
Lisäksi on mainittava tekijänoikeussäädökset, jotka koskevat myös ohjelmistotuotteita. Usein lisäksi Sarbanes-Oxley -laki mainitaan kansainvälisten yhtiöiden turvapalaverien yhteydessä.

Viranomaiset I

Tietoturvallisuuden kannalta keskeisiä viranomaisia ovat

- Eduskunta
- Valtioneuvoston kanslia
- Kauppa- ja teollisuusministeriö
- Valtiovarainministeriö
- Liikenne- ja viestintäministeriö
- Arkistolaitos
- Oikeusministeriö
- Huoltovarmuuskeskus
- Puolustusministeriö
- Keskusrikospoliisi
- Sisäasiainministeriö
- Tietosuojavaltuutetun toimisto

Viranomaiset II

- Työministeriö
- Valtiontalouden tarkastusvirasto
- Ulkoministeriö
- Viestintävirasto

Eettiset ohjeet

Seuraavassa on ISSAn (The Information Systems Security Association) jäsenyysvaatimukset. Yhdistyksen tavoitteena on edistää käytäntöjä, jotka varmistavat organisaation tietojen luottamuksellisuuden, eheyden ja käytettävyyden. Jäsenten tulee näyttää korkeimman eettisen käytöksen esimerkkiä.

- Suorita kaikki ammatilliset toiminnot ja velvollisuudet lakeja ja korkeita eettisiä periaatteita noudattaen.
- Edistä yleisesti hyväksyttyjä ja tällä hetkellä parhaita turvakäytäntöjä ja standardeja.
- Älä levitä luottamuksellisia tietoja, joita olet saanut ammatillisissa tehtävissä toimiessasi.
- Suorita ammatilliset velvollisuudet ahkerasti ja rehellisesti.
- Vältä kaikkia toimintoja, jotka johtavat työntekijöiden, tietoturva-ammatin tai ISSAn eturistiriitoihin tai maineen menetykseen.
- Älä loukkaa tahallisesti kolleegoiden, asiakkaiden tai työntekijöiden ammatillista mainetta.

Patentit

- Tietoturvatuotteet, varsinkin erilaiset salausalgoritmit, ovat patentoituja. Suurin osa patenteista on myönnetty 1970-luvun lopulla tai 80-luvun alussa, joten osa patenteista on joko rauennut tai piakkoin raukeamassa.
- USA:n patentit ovat voimassa 17 vuotta myöntämispäivästä ja 20 vuotta siitä, kun ne on jätetty patenttivirastoon.
- Ensimmäinen tärkeä rauennut patentti on Diffien ja Hellmanin avaintenluontimenetelmä, joka vapautui 29. 4. 1997. Esimerkiksi S/MIME käytti nopeasti hyväksi tätä mahdollisuutta.
- Julkisen avaimen salausmenetelmä RSA vapautui 20. 9. 2000.
- Elliptisiin käyriin perustuvien julkisten avainten menetelmien leviämistä estää tehokkaasti kanadalaisen Certicom-yhtiön lisenssipolitiikka (yli 130 patenttia).

Tietoturvan sääntely I

- Kryptografiset tuotteet on aikaisemmin rinnastettu useimmissa länsimaissa aseisiin ja niihin on kohdistettu tiukkoja vientirajoituksia.
- Jossain määrin tämä herättää kummastusta, sillä vahvoja, tunnettuja salausmenetelmiä on suhteellisen helppo toteuttaa.
- Kansainvälinen Wassenaar-sopimus on käsitellyt kaksikäyttötuotteita, eli tuotteita, joita voidaan käyttää sekä siviili- että sotilaskäytössä.
- Wassenaar-sopimus korvasi aikaisemman COCOM-sopimuksen (lopetettu maaliskuussa 1994).
- Vuoden 1998 lopulla Wassenaar-järjestelyssä 33 keskeistä teollisuusmaata, mukana myös Suomi, päättivät yhteisestä vientivalvonnasta. Korostettakoon, ettei Wassenaar-vientilista ollut vientikielto, vaan lisensointia edellyttävä valvontaluettelo.

Tietoturvan sääntely II

- Tällä hetkellä Suomessa on voimassa kaksikäyttötuotteiden vientivalvontalainsäädäntö, joka koostuu EU:n neuvoston asetuksesta (EY) nro 1334/2000 sekä tätä täydentävästä kansallisesta lainsäädännöstä (laki kaksikäyttötuotteiden vientivalvonnasta 562/1996 ja valtioneuvoston asetus 924/2000).
- Kaksikäyttötuotteiden vientivalvonnasta Suomessa vastaa ulkoasiainministeriön kauppapoliittisen osaston vientivalvonta-asioiden yksikkö.
- Se on myös lupaviranomainen kaksikäyttötuotteiden viennissä (poislukien EU:n neuvoston asetuksen liitteen I kategorian 0 tuotteet eli ydinspesifiset tuotteet, joiden vientivalvonta tapahtuu ydinenergialain perusteella ja lupaviranomainen on KTM:n energiaosasto ja/tai Säteilyturvakeskus STUK).

Tietoturvan sääntely III

- EU-asetuksen liite I (luettelo kaksikäyttötuotteista ja -teknologiasta) löytyy UM:n nettisivuilta osoitteesta

  http://formin.finland.fi/palvelut/kauppa/vientivalvonta

  kohdasta "Vientivalvonnan alaisuuden selvittäminen".
- Salaustuottet mukaanlukien tiedon suojaus löytyvät ryhmän 5 osasta 2.
- Kohdassa "Tuotehakemisto"on luettelo kaikista vientivalvonnan piiriin kuuluvista tuotteista.
- Luettelo valvonnanalaisista tuotteista, ohjelmistoista ja teknologioista löytyy myös EU:n sivuilta osoitteesta

  http://ue.eu.int/pesc/ExportCTRL/fi/index.html

  ja sieltä kohdasta "Security-related export controls".

Tietoturvan sääntely IV

- Ulkoasiainministeriö on myös julkaissut julkaisusarjassaan kaksiosaisen käsikirjan Vientivalvonta I ja II (3/2004). Niitä voi tiedustella Edita-kirjakaupasta, Sanomatalosta.

EU-asetus

EU-asetuksen liite I on yhdistelmä kansainvälisten vientivalvontajärjestelyjen seuraavista tuoteluetteloista:

- Wassenaarin järjestely (WA): http://www.wassenaar.org/
- Australian ryhmä (AG): http://www.australiagroup.net/
- Ohjusteknologian valvontajärjestely MTCR: http://www.mtcr.info/
- Ydinalan valvontajärjestely (NSG): http://www.nuclearsuppliersgroup.org

Yksityiskohtana mainittakoon, että symmetrisen salauksen tuotteiden vienti oli pitkään sallittu kolmansiin maihin vain, jos avaimen pituus ei ylitä 56 bittiä. Tällaiset salaukset on suhteellisen helppo murtaa massiivisilla laitteistoilla. Nykytilanne?

Tietoturvaorganisaatioita ja tietoturvan ohjeistuksia sekä standardeja I

Erilaisia tietoturvaorganisaatioita on suuri määrä. On sekä kansallisia että kansainvälisiä tietoturvaan keskittyviä organisaatioita. Seuraavassa on lueteltu näistä muutamia:

- *CERT Coordination Center*: Perustettu 1988 (DARPA). Internetiin liittyviin tietoturvaongelmiin keskittyvä keskeinen koordinointielin.
- *SANS Institute*: Perustettu 1989. Instituutti järjestää tietoturvakoulutusta sekä tarjoaa GIAC-turvasertifikaattiohjelman (Global Information Assurance Certification).
- *Computer Security Institute, CSI*: Perustettu 1974. Tietoturvallisuuteen keskittyvä ammattilaisten organisaatio.
- *InfoSec*: Perustettu 1998. Tarjoaa yleistä tietoturvakoulutusta (CISSP) ja erikoiskursseja (esim. Windows Kernel Reverse Engineering).

Tietoturvaorganisaatioita ja tietoturvan ohjeistuksia sekä standardeja II

- *National Security Agency, NSA*: USA:n hallituksen alainen organisaatio, joka kehittää ja tutkii salausmenetelmiä ja harrastaa tietoteknistä tiedustelua. NSA on ollut aktiivinen myös julkisten salausmenetelmien standardoinnissa (DES, AES).
- *Tietoturva ry*: Perustettu 1997. Yli 900 jäsenen kotimainen tietoturvaorganisaatio, joka on Tietotekniikan liiton teemayhdistys.

Kaikki yllä mainitut organisaatiot järjestävät koulutusta ja julkaisevat tietoturvaan liittyvää materiaalia. Erityisen mielenkiintoisia ovat esimerkiksi SANS-instituutin julkaisema luettelo Top 20 Internet Security Problems ja saman instituutin Storm Center, jossa seurataan uusimpia haavoittuvuuksia ja hyökkäyksiä. Lisäksi Suomen tilannetta seuraa CERT-FI, joka toimii viestintävirastossa ja jonka internet-sivuilta voi seurata lähes reaaliajassa haavoittuvuuksia ja tietoturvauutisia.

Vahti-sarja I

- Valtiovarainministeriö julkaisee VAHTI-tietoturvaohjeistusta, jota kehitetään jatkuvasti. Ohjeiston tarkoitus kattaa kaikki alueet.
- VM on antanut ohjeistusta valtion organisaatioille jo yli 20 vuoden ajan ja toimintaa on tehostettu vuodesta 1999 alkaen.
- Ohjeista saa hyvät tietoturvakäytännöt ja tarkistuslistat. Ohjeistoa käytetään laajasti myös valtionhallinnon ulkopuolella: kunnissa, yrityksissä, järjestöissä ja kansainvälisessä yhteistoiminnassa.

Tällä hetkellä VAHTI-sarjaan kuuluu yli 30 laaja-alaista tietoturvaohjetta. Seuraavista Internet-osoitteista pääsee tutustumaan näihin (valisemalla alakohdan tietoturvallisuus):

- www.vm.fi/vahti
- www.finansministeriet.fi/datasakerhet
- www.financeministry.fi/security

Tietoturvastandardit

Tietoturvaan liittyy myös yleisiä standardeja. Tietojärjestelmien kehitystyössä voidaan varautua tietoturvauhkiin SSE-CMM -prosessimallin avulla. Tietojärjestelmiä voidaan luokitella niiden tietoturvallisuuden vahvuuden mukaan Common Criterian avulla. Organisaation tietohallintoa voidaan mitata sen tietoturvallisuuden johtamisjärjestelmän osalta BS7799-standardin avulla.

Yleistä tietoturvaohjelmistojen laatimisesta I

- Salausmenetelmien suunnittelu vaatii yllättävän paljon tietoja algebrasta (esim. äärellisten kuntien teoria) ja kryptoanalyysistä. Tästä syystä muiden kuin asiantuntijoiden suunnittelemat salaustekniikat ovat yleensä heikkoja.
- Suosituksena on mainittu usein myös periaate, että ennen kuin salausmenetelmä otetaan tuotantokäyttöön, se on julkaistu ja sitä on tutkittu 3-5 vuotta.
- On useita esimerkkejä salausmenetelmistä, jotka on suunniteltu salassa ja joiden toimintamekanismi on pyritty salaamaan. Kuitenkin ennen pitkään menetelmä on vuotanut julkisuuteen ja monessa tapauksessa nämä salaiset menetelmät ovat osoittautuneet heikoiksi.
- Valmiita salausprimitiivejä sisältävien turvaprotokollien suunnittelussa ja toteuttamisessa päästään hieman vähemmillä matemaattisilla perustiedoilla. Tällöin riittää, että osaa valita yllä olevia palveluja tarjoavat kunnolliset primitiivit.

Yleistä tietoturvaohjelmistojen laatimisesta II

- Näiden perusteella voi sitten alkaa suunnitella tietoturvaprotokollaa. Protokollan toteutuksessa on kuitenkin otettava huomioon niin monia yksityiskohtia, että luotettavien järjestelmien toteuttaminen on yleensä ryhmätyötä, jossa on mukana tietoturvan asiantuntijoita.
- Huonosti toteutetun turvaohjelmiston murto onnistuu usein ilman, että varsinaisia salaustekniikoita murretaan tai että salausavaimia paljastetaan ennakolta.
- Nykyään myös vaaditaan, että kryptografinen algoritmi (esimerkiksi yhteisen avaimen generoiva protokolla) todistetaan oikeaksi, ennenkuin se julkaistaan hyvissä tieteellisissä lehdissä tai konferensseissa.

Yleistä tietoturvaohjelmistojen laatimisesta III

- Ensimmäisiä todistustekniikoita esiteltiin Canettin ja Krawczykin artikkelissa An analysis of Key-Exchange Protocols and Their Use for Building Secure Channels ja nykyään käytetään paljon LaMacchian, Lauterin ja Mityaginin menetelmää (artikkelissa Stronger Security of Autenticated Key Exchange). Se perustuu peliteoreettiseen lähestymistapaan.
- Formaalien todistusmenetelmien kehittäminen on ollut eräs tärkeimpiä edistysaskeleita viimeaikaisessa kryptografiassa, joskin menetelmät ovat herättäneet myös paljon keskustelua (Koblitz, Menezes: Another Look at "Provable Security").

Turvallisen suunnittelun periaatteet

Seuraavassa esitellään kahdeksan yleistä periaatetta, joita tulisi soveltaa turvallisuuteen liittyvissä projekteissa. Nämä yleiset periaatteet on laadittu varhain, ja siitä johtuen jotkut niistä eivät enää ole niin ajankohtaisia kuin aikaisemmin.

Määritelmä

Pienimmän oikeuden periaatteen *mukaan subjektille tulee antaa vain ne oikeudet, joita hän välttämättä tarvitsee tehtävän suorittamiseen.*

Esimerkki.

- Postipalvelin ottaa vastaan postia internetistä ja kopioi viestit hakemistoon, josta paikallinen palvelin jakaa viestit eteenpäin.
- Postipalvelimella täytyy olla oikeudet, jotta se voi ottaa viestejä vastaan portista, luoda tiedostoja hakemistoon ja muuttaa niitä (uudelleen kirjoittaa tai muuttaa osoitetta, lisätä tarpeelliset rivit).
- Sen pitäisi luopua kaikista oikeuksista tiedostoon sen jälkeen, kun tiedostot on kirjoitettu hakemistoon, koska se ei toiminnassaan tarvitse niitä enää. □

Määritelmä

Oletuskiellon periaate *sanoo että subjektilta pitää kieltää pääsy objektiin, ellei subjektille ole eksplisiittisesti sallittu pääsyä siihen.*

Erityisesti objektiin pääsystä ei ole mitään oletusarvoja tai oletusoikeuksia. Jos subjekti ei onnistu viemään objektiin kohdistuvaa operaatiota loppuun, sen pitäisi purkaa tehdyt osaoperaatiot ennen lopettamistaan. Näin systeemi pysyy turvallisena vaikka ohjelma keskeytyisi.

Määritelmä

Taloudellisen mekanismin periaate *sanoo, että turvamekanismin tulisi olla niin yksinkertainen kuin mahdollista.*

Jos määrittelyt ja toteutukset ovat yksinkertaisia, virheitä on todennäköisesti vähemmän. Monimutkaiset mekanismit usein tekevät oletuksia systeemistä ja ympäristöstä. Jos nämä oletukset ovat virheellisiä, ilmaantuu turvaongelmia.

Esimerkki.

- Ident-protokolla lähettää TCP-yhteyttä käyttävään prosessiin liittyvän käyttäjänimen kaukaiselle koneelle.
- Koneella A oleva mekanismi, joka tekee pääsynvalvontapäätöksiä ident-protokollan avulla, olettaa nimen lähettävän koneen olevan luotettava.
- Jos kone B päättää hyökätä A:ta vastaan, se voi lähettää minkä tahansa nimen A:lle ident-protokollan vastaussanomassa. A:n oletus vastaavan koneen luotettavuudesta ei pidäkään paikkaansa. □

Rajapinnat toisiin moduuleihin vaativat huomiota, koska moduulit tekevät usein oletuksia syöte- tai tulostusparametreista tai systeemistä. Kommunikointi ulkoisten olioiden, kuten ohjelmien, systeemien ja ihmisten kanssa lisää ongelmia.

Määritelmä

Täydellisen välityksen periaate *vaatii, että kaikkien pääsyjen kohdalla tulee tarkistaa, että pääsy on todella sallittu.*

Aina kun subjekti yrittää lukea objektin, käyttöjärjestelmän tulisi toimia välittäjänä. Ensiksikin KJ päättää, onko subjektilla oikeus lukea objekti. Jos on, KJ tarjoaa resurssit lukemiseen. Jos subjekti yrittää lukea samaa objektia uudestaan, taas tulisi tehdä tarkistus. Useimmat systeemit eivät toista tarkistuksia. Ne tallentavat ensimmäisen tarkistuksen tuloksen ja nojautuvat tähän uuden pyynnön yhteydessä.

Esimerkki 1.
Kun UNIX-prosessi yrittää lukea tiedostoa, KJ tarkistaa, voiko prosessi tehdä niin. Jos voi, prosessi saa tiedostokuvaajan (file descriptor, kts kohta 2), johon pääsyoikeus on kirjattu. Aina kun prosessi haluaa lukea tiedoston, se esittää kuvaajan ytimelle, jolloin ydin sallii pääsyn.
Jos tiedoston omistaja kieltää prosessilta pääsyn tiedostoon sen jälkeen, kun tiedostokuvaaja on luotu, ydin kuitenkin sallii pääsyn kuvaajan perusteella. Tämä on ristiriidassa täydellisen välityksen periaatteen kanssa. □

Esimerkki 2.
Nimipalvelu (DNS) tallettaa (cache) nimi-IP-osoite -tiedot. Jos hyökkääjä onnistuu muuttamaan talletettuja tietoja, reititystiedot tulevat virheelliseksi.Tämä tarjoaa hyökkäysmahdollisuuksia, kts tarkemmin [**?**] ja [**?**]. □

Määritelmä

Avoimen suunnittelun periaate sanoo, että mekanismin turvallisuus ei saisi riippua salaisesta suunnittelusta tai toteutuksesta.

Esimerkki. I

- Content Scrambling System (CSS) on kryptografinen mekanismi, joka suojaa DVD-levyjä kopioimiselta.
- DVD-levyllä on todennusavain, levyavain ja otsikkoavain.
- Otsikkoavain salattu levyavaimen avulla. DVD:n eräs lohko sisältää useita kopioita levyavaimesta, joista jokainen on salattu eri soittimen avaimella. Lohkoon on viety myös avaimen tiivistearvo (hash).
- Kun DVD-levy viedään soittimeen, algoritmi lukee todennusavaimen. Sen jälkeen se avaa levyavaimet käyttäen DVD-soittimen avainta. Kun purun tulos vastaa tiivistearvoa (tiivisteen laskemisen jälkeen), oikea levyavain on löydetty. Sitä käytetään lopuksi otsikkoavaimen purkamiseen, jonka avulla elokuvan salaus voidaan purkaa.
- Vuonna 1999 ryhmä norjalaisia sai käsiinsä DVD-levyjä toistavan ohjelman, jossa oli salaamaton avain. He myös johtivat ohjelmasta algoritmin, joka oli sama kuin CSS. Tämä mahdollisti sen, että he saattoivat purkaa minkä tahansa DVD-elokuvan.

Esimerkki. II

- Pian internetissä alkoi levitä ohjelma, joka teki tämän kaiken nopeasti. Tämä taas aiheutti sen, että DVD Copyright Control Association vaati oikeusteitse, ettei koodia saanut levittää julkisesti. Korostaakseen algoritmin salaamisen tärkeyttä he liittivät CSS:n lähdekoodin kanteeseen. Huomattuaan virheensä asianajajat vaativat kanteen salaamista, mutta sitä oli jo levitetty useissa internet-palvelimissa, mukaanlukien yksi, josta kannetta oli ladattu yli 21 000 kertaa.
- Koko CSS on osoittautunut melko heikoksi ja sen salaus voidaan purkaa raa'alla voimalla. Osasyynä tähän on avaimen pituus, vain 40 bittiä. Se taas johtui USAn silloisista vientirajoituksista.
- Nykyiset HD- ja Blue Ray -levyt sisältävät vahvan salauksen.

□

Määritelmä

Oikeuksien erottamisen periaate *sanoo, että systeemin ei pitäisi antaa oikeuksia yhden ehdon perusteella.*

Esimerkiksi Berkeleyn UNIX:ssa käyttäjät eivät voi vaihtaa käyttäjätiliään juureksi, ellei kaksi ehtoa ole voimassa. Ensimmäinen ehto on, että käyttäjä tuntee juuren salasanan. Toinen ehto on, että käyttäjä kuuluu wheel-ryhmään (GID 0). Molempien ehtojen tulee olla voimassa.

Määritelmä

Pienimmän yhteisen mekanismin periaate *sanoo, ettei resursseihin pääsyä valvovia mekanismeja pidä jakaa muiden kanssa.*

Resurssien jakamisesta seuraa, että informaatiota voidaan välittää. Sääntö ei vaikuta yhtä tärkeältä kuin muut säännöt.

Määritelmä

Psykologisen hyväksyttävyyden periaate *sanoo, että turvamekanismin ei tule vaikeuttaa resurssien käyttöä verrattuna tilanteeseen, jossa mekanismia ei käytetä.*

Käytännössä turvamekanismit lisäävät jonkin verran vaivaa, mutta lisäyksen tulisi olla kohtuullista. Turvamekanismien toteutus vaatii myös laskentaresursseja, joita kaikissa sovelluksissa ei ole riittävästi. Siten turvallisuusvaatimuksista on tällaisissa tapauksissa tingittävä. Esimerkiksi verkkokerrokseen tarvittaisiin vahvoja todennusmenetelmiä, mutta raskaan liikenteen yhteydessä vahvat todennusmenetelmät eivät ole toistaiseksi olleet mahdollisia.