



VALTIOVARAINMINISTERIÖ

VALTIONHALLINNON TIETOTURVAKÄSITTEISTÖ

4/2003



VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

VALTIONHALLINNON TIETOTURVAKÄSITTEISTÖ

4/2003

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ

Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin

(09) 160 01

Telefaksi

(09) 160 33123

Internet

www.vm.fi

Julkaisun tilaukset

Puh. (09) 160 33 222

Sähköposti: vahtijulkaisut@vm.fi

ISSN 1455-2566

ISBN 951-804-404-8

Edita Prima Oy
HELSINKI 2003



Ministeriöille, virastoille ja laitoksille

VALTIONHALLINNON TIETOTURVAKÄSITTEISTÖ

Valtiovarainministeriö antaa oheisen suosituksen (jäljempänä käsitteistö), joka on laadittu valtiovarainministeriön asettaman ja johtaman Valtionhallinnon tietoturvasuuden johtoryhmän VAHTI toimesta. Käsitteistö korvaa aiemman valtionhallinnon tietoturvakäsitteistön (VAHTI 1/2000) ja yhtenäistää valtionhallinnon tietoturvatерminologiaa.

Käsitteistö on tarkoitettu käytettäväksi laajasti valtionhallinnon yksiköissä tehtävässä tietoturvatyössä. On suositeltavaa, että johdon, tietoturva-, tietohallinto-, tietopalvelu- ja turvallisuusvastaavien lisäksi myös virastojen muu henkilökunta perehtyy käsitteistöön. Valtion organisaatioissa tulee huolehtia siitä, että henkilöstö on riittävän hyvin perillä tietoturvasuudesta ja siihen liittyvistä käsitteistä. Käsitteistö sisältää noin tuhat tietoturvakäsitteen määritelmää ja englanti-suomi-sanakirjan.

Valtioneuvoston periaatepäätöksissä valtion tietoturvasuudesta 11.11.1999 ja kansallisesta tietoturvastrategiasta 4.9.2003 korostetaan tietoturvaosaamisen kehittämisen tärkeyttä. Osaamisen ja hyvän tietoturvayhteistyön edellytys on, että henkilöstö tuntee tietoturvasuuden keskeiset käsitteet.

Käsitteistö tulee VAHTIn Internet-sivuille (osoitteet: www.vm.fi/tietoturvasuus ja www.vm.fi/vahti). Käsitteistöä kehitetään tarvittaessa mm. saatavan palautteen pohjalta, jonka voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi). Käsitteistöä, jonka laantumiseen on osallistunut myös yksityinen sektori, voi käyttää hyväksi myös valtionhallinnon ulkopuolella.

Lisätietoja antavat neuvotteleva virkamies Mikael Kiviniemi ja projektipäällikkö Olli-Pekka Rissanen (etunimi.sukunimi@vm.fi).

Alivaltiosihteeri

Juhani Turunen

Ylijohtaja

Jorma Karjalainen*Liite Valtionhallinnon tietoturvakäsitteistö (VAHTI 4/2003)*

VALTIONHALLINNON TIETOTURVAKÄSITTEISTÖ 2003

Esipuhe

Tämä on kolmas kerta, kun valtiovarainministeriö julkaisee Valtionhallinnon tietoturvakäsitteistön. Käsitteistön edelliseen painokseen (Vahti 1/2000) verrattuna tässä on kaksinkertainen määrä hakusanoja. Nyt hakusanoja on noin tuhat. Kolmen vuoden aikana tietoturvallisuus on kehittynyt ja sen merkitys kasvanut erityisesti uusien tietoturvauhkien myötä. Samaan aikaan on uusia käsitteitä tullut käyttöön. Uutta aineistoa on tuotu erityisesti seuraavilta aloilta:

- tietoturvallisuuden suoranaisesti tai välillisesti liittyvät säädökset
- virukset ja muut haittaohjelmat
- sähköinen sodankäynti.

Käsitteistö julkaistaan tietoturvatyössä käytettävän terminologian yhtenäistämiseksi sekä tulevan tietoturvallisuutta koskevan lainsäädäntö-, ohjeistus-, suunnittelu- sekä käytännön toteutustyön tueksi. Tietoturvallisuus koskee yhä enenevässä määrin kaikkia käyttäjiä. Suomenkielinen termistö auttaa ymmärtämään minkä tyyppisistä ongelmista ja riskeistä on kyse. Tietoturva-asiantuntijoiden lisäksi käsitteistön on tarkoitus hyödyttää myös kaikkia käyttäjiä.

Muutosten ja lisäysten pääasiallisina lähteinä on käytetty ATK-sanakirjaa, valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) 2000-luvulla julkaisemia ohjeita, suosituksia ja raportteja, eräitä muita julkishallinnon tietoturva-aiheisia julkaisuja sekä viimeaikaista koti- ja ulkomaista sekä kansainvälistä tietoturva-alan aineistoa. Lainsäädännön kautta käyttöönotettuja käsitteitä on myös tuotu käsitteistöön. Käsitteistön kokoamisesta on vastannut Ph.D. Ilmari Pietarinen tukenaan VAHTIn alainen työryhmä.

Käsitteistöön on sijoitettu kaavioita, joiden tarkoitus on auttaa hahmottamaan termien välisiä suhteita. Termi, johon liittyy kaavio, on merkitty symbolilla ♣. Termien välisiä viittauksia on runsaasti. Viitteissä käytetyt symbolit tarkoittavat:

- nuoli ylöspäin (▲): viittaus yleisempään käsitteeseen tai yleiskielen sanaan
- nuoli oikealle (►): vertaa
- nuoli alaspäin (▼): viittaus rajatumpaan käsitteeseen.

Koska suomenkielinen termi on monelle käsitteelle vielä vakiintumaton, joissakin tapauksissa on hyväksytty rinnakkaisia nimityksiä. Joistain termivalinnoista on keskusteltu laajasti käsitteistön valmistelleessa työryhmässä ja näin pyritty löytämään mahdollisimman yleinen termi. Yleisenä pyrkimyksenä on ollut käyttää suomen kielen mukaisia sanontoja.

Keskeisestä käsitteestä "tietoturvallisuus" työryhmä suosittelee yksinkertaisuuden vuoksi käytettäväksi muotoa "tietoturva" silloin, kun se on yhdyssanan alkuosana. Esimerkiksi suositellaan käytettäväksi tietoturvapoliitiikka ja tietoturvariski. Kannattaa myös huomata, että yleiskieleen ovat vakiintuneet käsitteet turvallisuuspolitiikka ja turvallisuusriski.

Käsitteistön käyttö kaupalliseen käyttöön ja jäljentäminen ansaitsemistarkoituksessa on kielletty. Muussa hyödyntämisessä tulee mainita tämä käsitteistö lähteenä.

Sisällysluettelo

1	Käsitteistö.....	1
2	Englanti–suomi -sanasto.....	74

0 – 9

3DES

DES-salakirjoitusmenetelmän versio, jossa viesti salakirjoitetaan kolme kertaa peräkkäin

Käytetyistä avaimista riippuen tehollinen avaimen pituus on näin ollen 56, 112 tai 168 bittiä.

▲ *DES, symmetrinen lohkosalaus* ▶ *AES*

A

AES

Advanced Encryption Standard

standardoitu symmetrisen lohkosalauksen menetelmä, jossa avaimen pituus on 128, 192 tai 256 bittiä; standardi FIPS 197 (2002)

Huom. Menetelmää kutsutaan myös Rijndael-menetelmäksi tekijänsä mukaan.

▲ *salausalgoritmi, symmetrinen lohkosalaus*
▶ *3DES, Blowfish, DES, Twofish*

aikakatkaisu

en time-out

erityistomien käynnistyminen automaattisesti, jos odotettua toimintaa ei määräjassa esiinny
Esim. siirtoyhteyden purkautuminen tietyn ajan kuluttua viimeisen jakson lähettämisestä.

▲ *käyttö (2)* ▶ *vahtiajastin*

aikaleima

en time stamp

tapahtumatietoon tai viestiin liitetty tieto lähetyksen, saapumis- tai käsittelyajankohdasta ja mahdollisesti tapahtuman osapuolista

Aikaleimalla saadaan aikaan viestin lähettämisen tai vastaanottamisen kiistämättömyys.

▲ *leima, notarointi* ▶ *kiistämättömyys*

aikaleimapalvelin

en time stamp server

palvelin, joka tiettyssä ympäristössä toteuttaa aikaleimapalvelun

▲ *notaaripalvelin, palvelin*

aikaleimapalvelu

en time stamp service

verkossa luotetun osapuolen tarjoama palvelu, joka liittyy aikaleiman viestiin

▲ *julkisen avaimen järjestelmä, luotettu taho, palvelu, verkkopalvelu* ▶ *verkkonotaari*

aikapommi

en time bomb

tuholaisohjelma, joka on kohdekoneessa aluksi piilevänä ja käynnistyy myöhemmin, esimerkiksi määrätyn kuukauden määrättyinä päivinä

▲ *haittaohjelma ♣, pommi, tuholaisohjelma ♣*
▶ *vahtiajastin*

aineisto

en material; data

johonkin tarkoitukseen käytettävissä tai saatavilla oleva, yleensä suuri määrä eri tavoin ryhmiteltyjä tietoja, esimerkiksi asiakirjoja, tiedostoja tai arkistoja

▲ *tieto* ▶ *aineistoturvallisuus, arkisto, laitton kopio*
▼ *testiaineisto, turvaluokitettava tieto*

aineistoturvallisuus

en data security

tietoturvaluuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen

▲ *tietoturvallisuus ♣, turvallisuus* ▶ *aineisto, hallinnollinen tietoturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus* ▼ *arkistolaki, tietojen luokitus*

aitous

en authenticity

tietoverkossa tiedon alkuperän tai viestin lähettäjän luotettava tunnistettavuus

▲ *ominaisuus* ▶ *eheys, haastemenetelmä, kelpoisuus, kiistämättömyys, tunnistus, valtuustieto, varmenne*

ajantasaisuus

en currency

kohdetta esittävien tietojen säilyminen kohteen ominaisuuksissa tapahtuvien muutosten mukaisina

Esim. Yrityksen henkilöstön ja sen palkkauksen jatkuvasti muuttuessa henkilöstötietojen ajantasaisuus on tärkeä.

▲ *ominaisuus* ▶ *käytettävyyden (1), luotettavuus*

akkreditointi

en accreditation

pätevyyden tai kelpoisuuden toteaminen tähän oikeutetun tai muuten luotetun tahon toimesta

Akkreditointi ei välttämättä merkitse virallista luvan antoa tai valtuuttamista johonkin tehtävään.

Suomessa akkreditoitintoimintaa harjoittaa Mittatekniikan keskus.

▲ *luotettu taho* ▶ *arviointi, hyväksymistarkastus, kelpuutus, valtuutus, varmentaminen*

akkreditointijärjestelmä

en accreditation scheme

järjestelmä, jonka puitteissa määritellään aukottomasti eri varmentajien roolit, valtuudet ja keskinäiset suhteet

- ▲ *julkisen avaimen järjestelmä, varmentaja*
- ▶ *varmennusorganisaatio*

aktiivinen hyökkäys

en active attack

hyökkäys, jonka tarkoituksena on muuttaa, poistaa tai lisätä tietoa tai häiritä järjestelmän toimintaa

- ▲ *hyökkäys* ▶ *passiivinen hyökkäys* ▼ *datapohjainen hyökkäys, koukkaus, murtautua, palvelunestohyökkäys, tekeytyminen, tietomurto, välistä-vetohyökkäys*

algoritmi

en algorithm

joukko toimintaohjeita, jotka esittävät sarjan toimia tehtävän suorittamiseksi tai ratkaisemiseksi. Suoritettava tehtävä voi olla esimerkiksi viestin salakirjoitus tai salakirjoituksen avaaminen.

- ▼ *salausalgoritmi, tiivistysfunktio*

alhaalla

suositellaan: kaatunut, ei toiminnassa

kts. *kaatua*.

allekirjoitus

en signature (1)

asiakirjaan, viestiin tai muuhun tekstiin liitetty henkilön omakätinen nimikirjoitus tai muu tieto, jonka vain kyseinen henkilö on voinut tuottaa, osoituksena siitä, että teksti vastaa hänen tahtoaan tai aikomustaan

- ▲ *todennus* ▶ *tunniste, tunnus* ▼ *digitaalinen allekirjoitus, sähköinen allekirjoitus*

allekirjoituslaki

en Electronic Signatures Act

laki sähköisistä allekirjoituksista (14/2003)

- ▲ *laki, tietotekniikkaoikeus, tietoturva-oikeus*
- ▶ *luotettu taho, sähköinen allekirjoitus*

altistus

en exposure

riskille alttiina oleminen

- ▶ *haavoittuvuus, riski*

ammattietiikka

en professional ethics

kts. *eettiset ohjeet*

analyysi

- ▶ *arviointi* ▼ *riskianalyysi, salauksen ratkonta, uhka-analyysi, verkkoanalysointori*

anonyymi FTP

en anonymous FTP

yhteyskäytäntö, joka toteuttaa anonyymien tiedostoniirron

anonyymi tiedostonsiirto

en anonymous file transfer

tiedostonsiirto palvelimesta työasemaan käyttäjätunnusta ilmoittamatta, käyttäen tähän varattua yleistä tunnusta

Käyttäjätunnukseksi on tällöin esimerkiksi sana "anonymous" ja salasanaan käyttäjän sähköpostiosoite.

anonyymiasiointi

en anonymous transactions

asiointi, jossa asiakkaan tunnistamista ei vaadita

- ▲ *anonyymikäyttö, asiointi, verkkoasiointi*

anonyymikäyttö

en anonymous use

tietoverkon käyttö, jossa käyttäjän henkilöllisyyttä ei tunnisteta, mutta häneltä voidaan kysyä käytötapahtumaan liittyviä tietoja

- ▲ *käyttö (1), tunnistus* ▶ *nimimerkki, tunnistetun käyttö* ▼ *anonyymiasiointi, anonyymitunnus*

anonyymipalvelin

en anonymity server

1) tietoverkossa palvelin, joka lähettää viestin edelleen ilman lähettäjän tunnistetta

2) palvelin, joka suorittaa anonyymipalveluja

- ▲ *anonyymipalvelu, palvelin* ▶ *tunnisteeton käyttö*

anonyymipalvelu

en anonymous service

tietoverkossa palvelu, joka toteuttaa anonyymikäytön tai anonyymiasiointin

- ▲ *palvelu* ▼ *anonyymipalvelin*

anonyymitunnus

en anonymous user ID

palvelun anonyymikäyttöön varattu tunnus

- ▲ *anonyymikäyttö, tunnus* ▶ *peitenimi*

ansa

en trap (s)

ohjelma, joka tekeytyy palvelimeksi pyydystääseen murtautujia

- ▲ *turvaohjelma ♣* ▶ *eristää, murtautuja, tietomurtohälytin* ▼ *ansoittaa, houkutuslintu, roska-postiansa*

ansoittaa

en entrap

sijoittaa ohjelmaan valvottuja salaovia tunkeutujien ilmisaamiseksi

- ▲ *ansa* ▶ *salaovi, takaportti*

apletti

yleensä Java-kielinen sovellus tai ohjelma, joka suoritetaan web-selaimen käynnistämänä tulkiten; suomeksi *sovelma*

arkaluonteinen tieto

en sensitive data

yksilöä tai organisaatiota koskeva tieto, jonka rekisteröintiä ja käyttöä on rajoitettu lain tai asianomaisen vaatimuksesta

Suomen henkilötietolain mukaan arkaluonteisia ovat henkilötiedot, jotka kuvaavat tai on tarkoitettu kuvaamaan

- rotua tai etnistä alkuperää
- uskontoa, yhteiskunnallista vakaumusta tai ammattiliittoon kuulumista
- rikollista tekoa ja rangaistusta tai muuta rikoksen seuraamusta
- terveydentilaa ja vammaisuutta tai hoitotoimia
- seksuaalista suuntautumista tai käyttäytymistä
- sosiaalihuollon tarvetta tai saatuja sosiaalihuollon palveluja tai etuuksia.

▲ *henkilötietolaki, tieto* ▶ *luottamuksellinen, salainen, salassa pidettävä tieto, tietovalkama, vaatimus, yksityisyyden loukkaus, yksityisyys*

arkisto

en archive (s)

säilytettävien dokumenttien tai tallenteiden kokoelma, tai paikka, jossa niitä on tarkoitus säilyttää

▶ *aineisto, asiakirja* ▼ *käyttöarkisto, turva-arkisto, varmuusarkisto*

arkistolaki

en Archives Act

arkistolaki (831/1994) velvoittaa julkishallinnon yksiköt arkistotoiminnassaan huolehtimaan yksityisten ja yhteisöjen oikeusturvasta ja tietosuojasta sekä säilyttämään asiakirjat niin, että ne ovat turvassa tuholta ja asiattomalta käytöltä

▲ *aineistoturvallisuus, laki*

arviointi

en evaluation (1); assessment

sen seikan selvittäminen, täyttääkö tietty kohde sille asetetut vaatimukset eri osiltaan

Esim. tietotuotteen standardinmukaisuuden arviointi, tietojärjestelmän arviointi tietoturva-vaatimuksia vastaan.

▶ *akkreditointi, analyysi, hyväksymistarkastus, katselmus, laatu, tarkastus (2), tietoturvanormi* ▼ *ITSEC, sertifioida*

asiakirja

en document

kirjallinen tai kuvallinen esitys tai yhteen kuuluvista tai tarkoitetuista merkeistä muodostuva tiettyä kohdetta tai asiaa koskeva viesti, joka on saatavissa selville teknisen apuvälineen avulla

▶ *arkisto, loki, tietokoneavusteinen väärennys*
▼ *sähköinen asiakirja, viranomaisen asiakirja*

asiakirjajulkisuuslaki

en sunshine law

kts. *julkisuuslaki*

asiakirjaluokitus

kts. *tietojen luokitus*

asiankäsittely

en case processing; workflow

1) palveluorganisaatiossa tai viranomaisessa viereille pantuun tiettyä asiakasta tai asiakasryhmää koskevaan asiaan ja siihen liittyviin dokumentteihin kohdistuva hallinnollisten tai kaupallisten toimenpiteiden sarja, joka päättyy asian ratkaisuun tai muuhun tiettyyn lopputulokseen

2) tietotekniikkaa hyväksikäyttävä asiankäsittely (1)

▶ *asiointi*

ASIM

automated security incident measurement

verkkoliikenteen seurannan ja tietomurtohälytyksen järjestelmä

▲ *seurain, tietomurtohälytin* ▶ *IDS*

asiointi

en client transaction; client interaction

toiminta, jonka sisältönä on vuorovaikutus asiakkaiden ja palveluntuottajien välillä kaupallisen tai hallinnollisen palvelun saamiseksi tai velvollisuuden täyttämiseksi

Silloin kun asiointilla on oikeusvaikutus, esimerkiksi asia tulee virallisesti vireille, asiointissa vaaditaan osapuolten luotettavaa tunnistamista.

▶ *asiankäsittely, palvelu* ▼ *anonymiasiointi, sähköinen asiointi, sähköinen asiointitunnus, verkkoasiointi*

asiointipalvelu

en online service

jatkuvasti saatavilla oleva hallinnollisen tai kaupalliseen asiointiin verkkopalvelu

▲ *palvelu, sähköinen asiointi, verkkoasiointi, verkkopalvelu* ▶ *tiedotuspalvelu*

asymmetrinen salaus

kts. *epäsymmetrinen salaus*

atk-oikeus

kts. *tietotekniikkaoikeus*

atk-rikos

kts. *tietotekniikkarikos*

atk-sabotaasi

en computer sabotage

atk-laitteen tai laitteiston fyysinen vahingoittaminen

▲ tietotekniikkarikos, uhka, vahinko

atk-tarkastaja

en systems auditor

tietojärjestelmiin perehtynyt tarkastaja

▲ tarkastaja ▶ tietojärjestelmä

atk-vakoilu

kts. yritysvakoilu

atk-virus

kts. virus ♣

auditointi

kts. tarkastus

autentikointi

kts. aidonnus, todennus

autenttisuus

kts. aitous

avaimen palautus

en key recovery

kadonneen salausavaimen uudelleen konstruointi tai vara-avaimen saanti

▲ salausavain ♣ ▶ turvatalletus, vara-avainjärjestelmä

avaimenhaltija

en keyholder

yksilö tai yhteisö, jolla on hallussaan tai valvonnassaan salausavaimia

▲ salausavain ♣ ▶ avaintenhallinta

avain

en key

tieto, jonka avulla tai jonka kautta pääsee toiseen tietoon, esimerkiksi salausavain

▲ tieto ▶ laskennallisesti murtovarma, tunnus ▼ julkinen avain, kaksikäyttöavain, kerta-avain, salainen avain, salausavain ♣, todennusavain, toimiavain, USB-avain, yksityinen avain

avainpiiri

en key chip

ohjelman luvattoman kopion käytön estämiseen tarkoitettu laiteosa tai mikropiiri, joka on kytkettävä tietokoneeseen ohjelmaa käytettäessä

▲ turvamoduuli ▶ laiton kopio, tonkeli

avainten jakelukeskus

en key distribution center

taho, joka jakelee ja rekisteröi julkisen avaimen järjestelmässä julkisen ja yksityisen avaimen muodostamia avainpareja

Toiminto voi olla yhdistettynä varmentajan tehtäviin, kuten Suomessa väestörekisterikeskuksen.

▲ avaintenhallinta ▶ varmentaja

avaintenhallinta

en key management

salausavainten tuottaminen, talletus, jakelu, rekisteröinti, peruuttaminen, poistaminen, arkistointi ja varmentaminen

▲ hallinta, salausavain ♣ ▶ avaimenhaltija ▼ avainten jakelukeskus

avaintenhallintajärjestelmä

en key management system

avaintenhallintaan tarkoitettu järjestelmä tai organisaatio

avaintenvaihtokäytäntö

en key agreement protocol

sarja toimenpiteitä, jotka mahdollistavat viestijöille turvallisen tavan lähettää toisilleen salausavaimet symmetristä salausta käyttävässä järjestelmässä

▲ käytäntö, symmetrinen salaus ♣, turvakäytäntö ▼ ISAKMP

avata (1)

en decode

saattaa kooditettu tieto siihen muotoon, jossa se oli ennen koodittamista

avata (2)

en decipher; decrypt

saattaa salakirjoitettu tieto selväkieliseen muotoon, yleensä avainta käyttäen

▲ salakirjoittaa ▶ murtaa ▼ koodin avaaminen, salauksen ratkonta, yksisuuntainen salausalgoritmi

avoin verkko

en open network

1) tietoverkko, joka on kenen tahansa käytettävissä, esimerkiksi Internet

2) tietoverkko, jonka liikenne noudattaa yleisesti standardoituja valmistajasta riippumattomia yhteyskäytäntöjä, esimerkiksi Internet

▲ tietoverkko ♣, verkko ♣ ▶ palveluverkko, suljettu verkko, yhteyskäytäntö, yksityisverkko

B

bakteeri

en bacterium (pl bacteria)

virus tai mato, joka kiinnittyy käyttöjärjestelmään ja kuluttaa tietokoneen resursseja mutta ei yleensä tee muuta vahinkoa

▲ *haittaohjelma* ♣, *monistuva ohjelma* ▶ *hukuttaminen*, *loisohjelma*, *mato* ♣, *muistivuoto*, *virus* ♣

biotunnistus

en biometric identification

ihmisen tunnistaminen fyysisten tuntomerkkien kuten sormenjäljen, äänen tai käden, kasvojen tai silmänpohjan piirteiden perusteella

▲ *tunnistaa (2)*, *tunnistus* ▶ *salasanatunnistus*, *sähköinen tunnistus*, *tuntomerkki* ▼ *puhujan tunnistus*, *äänentunnistus*

Blowfish

eräs symmetrisen lohkosalausmenetelmä

▲ *symmetrinen lohkosalaus*, *vahva salausalgoritmi* ▶ *AES*, *IDEA*, *Twofish*

BS 7799

Code of Practice for Information Security

Britannian standardointi-instituutin julkaisema suositus yrityksen tietoturvapoliitikasta ja turvallisuustodistuksen myöntämisperusteista

▲ *eettiset ohjeet*, *tietoturvastandardi* ▶ *ISO 17799*, *tietoturvapoliittikka*, *turvallisuustodistus*

BSI

Bundesamt für Sicherheit in der Informationstechnik

Saksan tietoturvavirasto

▶ *ENISA*

C

C-tason turvallisuus

en level C security

NCSC:n luokituksen mukainen perusturvallisuus, jonka esimerkiksi nykyaikaiset käyttöjärjestelmät toteuttavat

▲ *NCSC*, *perusturvallisuus*, *turvaluokitus*

C2W

command and control warfare

johtamissodankäynti

▲ *EW*

CA

certificate authority

varmentaja; varmenneviranomainen

Carnivore

FBI:n hallinnoima sähköisen viestinnän seurantajärjestelmä Yhdysvalloissa

▲ *nuuskia*, *urkintatekniikka* ▶ *Echelon*

CC

kts. *Common Criteria*

CEN

Comité Européen de Normalisation

Euroopan standardointikomitea, jonka toimialaan kuuluvat kaikki tekniikan alat paitsi sähkötekniikka ja teletekniikka

▲ *järjestö*, *standardointielin* ▶ *CENELEC*, *ETSI*, *SFS* ▼ *CEN/ISSS*

CEN/ISSS

CEN Information Society Standardization System

CEN-komitean alikomitea, joka käsittelee tietotekniikan alan standardeja

▲ *CEN*, *tietoturvastandardi*

CENELEC

Comité Européen de Normalisation Electrotechnique

Euroopan tason sähkötekniikan standardointikomitea

▲ *järjestö*, *standardointielin* ▶ *CEN*, *ETSI*

CERT

Computer Emergency Response Team

tietoturvallisuutta edistävien organisaatioiden maailmanlaajuinen verkosto, joka välittää tietoa tietoverkkoihin kohdistuvista tietoturvariskeistä ja järjestää asiantuntija-apua ja koulutusta niiden torjumiseksi

Suomessa verkostoon kuuluvat Viestintävirasto ja yliopistojen yhteinen Funet CERT

▶ *FIRST*, *Viestintävirasto*, *virusvaroitus*

CIAO

Critical Infrastructure Assurance Office

Yhdysvaltain valtionhallinnon virasto, joka kehittää ja koordinoi politiikkaa yhteiskunnan elintärkeiden perusrakenteiden turvaamiseksi

▲ *valmiussuunnittelu* ▶ *DII*, *NIPC*, *NISCC*, *NSA*, *PTS*

CISA

Certified Information Systems Auditor

kansainvälisen tutkinnon suorittanut atk-tarkastaja

▲ *eettiset ohjeet*, *tarkastaja*, *tietojenkäsittelyn tarkastus*, *tietoturvatarkastus* ▶ *CISSP*, *GIAC*, *SANS*

CISSP

Certified Information Systems Security Professional

tietoturvallisuuden ammattipätevyyden todistus, jonka myöntää ISC2-järjestö

▲ *eettiset ohjeet, tietoturvatarkastus* ▶ *CISA, GIAC, ISC2, SANS*

Clipper chip

Yhdysvaltain viranomaisten hanke salaisen Skipjack-salakirjoitusmenetelmän sisältävän Clipper chip-nimisen mikropiirin tekemiseksi pakolliseksi kaikkiin salausta käyttäviin laitteisiin, jolloin USA:n viranomaiset olisivat halutessaan voineet avata salauksen käyttäjän tietämättä

Elinkeinoelämän vastustuksen takia hankkeesta luovuttiin.

▲ *salausalgoritmi, viranomaispääsy* ▶ *takaportti*

Common Criteria

ISO/IEC standardi 15408, Evaluation Criteria for Information Technology Security, joka määrittelee tietoturvallisuuden arvioinnin kriteerit ja yhdistää USA:ssa (TCSEC, FC), EU:ssa (ITSEC) ja Kanadassa (CTCPEC) kehitetyt arviointikriteeristöt

▲ *tietoturvastandardi* ▶ *ITSEC, Orange Book*

cookie

kts. *eväste*

CRC-varmistus

en cyclic redundancy checking

kts. *syklinen ylimäärävarmistus*

CSP

certificate service provider

varmennuspalvelujen tuottaja

D

datapohjainen hyökkäys

en data driven attack

hyökkäys, jossa tuhoa tuottava aines on kätketty vaarattomalta näyttävään dataan

▲ *aktiivinen hyökkäys, hyökkäys* ▶ *haittaohjelma ♣, makrovirus*

dataverkko

en data network

▲ *verkko ♣* ▶ *esto, tietoverkko ♣* ▼ *tunnelointi*

DDoS

distributed denial of service

hajautettu palvelunestohyökkäys

▲ *DoS*

debuggaus

kts. *perkaus*

demilitarisoitu alue

kts. *harmaa vyöhyke*

DES

Data Encryption Standard

standardoitu 56-bittiseen avaimen perustuva symmetrisen lohkosalauksen menetelmä, jota käytetään laajasti henkilökohtaisten tunnistaiden salaukseen.

▲ *lohkosalaus, salausalgoritmi* ▶ *AES, IDEA*
▼ *3DES*

DEW

directed-energy weapon

suunnattua energiaa käyttävä ase

▼ *HPM*

digitaalinen allekirjoitus

en digital signature

sähköinen allekirjoitus, jonka tuottamiseen on käytetty varmennetta

Viestiin tai asiakirjaan liitetty digitaalinen allekirjoitus yksilöi lähettäjän ja on todiste viestin ja lähettäjän aitoudesta, ja yleensä myös viestin eheydestä.

▲ *allekirjoitus, varmenne* ▶ *laatuvarmenne, S/MIME, sinetti, sähköinen allekirjoitus, turvapisti* ▼ *DSS, EESSI*

DII

Defense Information Infrastructure

Yhdysvaltain puolustusvoimain maailmanlaajuisen tietojärjestelmä

▶ *CIAO, tietosodankäynti ♣*

disinformaatio

en disinformation

tarkoituksellisesti vääristelty tieto tai tiedottaminen, esimerkiksi osana psykologista tietosodankäyntiä

▲ *tietosodankäynti ♣* ▶ *tekeytyminen, virusvalhe*

DMZ

demilitarized zone

harmaa vyöhyke

DoD

Department of Defense

Yhdysvaltain puolustusministeriö

domain

kts. *verkkoalue*

DoS

denial of service

palvelunestohyökkäys

▼ *DDoS*

DSA

Digital Signature Algorithm

DSS-standardin perustana oleva epäsymmetrinen salakirjoitusalgoritmi

► *DSS*

DSS

Digital Signature Standard

Yhdysvaltain hallinnossa digitaalisen allekirjoituksen standardi (FIPS 186)

▲ *digitaalinen allekirjoitus, vahva salausalgoritmi*

► *DSA*

dynaaminen salasana

en dynamic password

sama kuin *kertatunnus*

▲ *salasana*

E**e-hallinto**

kts. *verkkoasiointi*

e-pommi

kts. *sähkömagneettinen pulssi, EMP*

Echelon

Yhdysvaltain, Britannian, Kanadan ja Australian yhteistoiminta sähköisen viestinnän järjestelmien tiedustelemiseksi

▲ *signaalitiedustelu ♣, urkintatekniikka, viestitiedustelu* ► *Carnivore, NSA, yritysvakoilu*

edustajärjestelmä

sama kuin *palvelujärjestelmä*

EESSI

European Electronic Signature Standardization Initiative

Euroopan Komission asettama työryhmä digitaalista allekirjoitusta koskevien vaatimusten määrittelemiseksi

▲ *digitaalinen allekirjoitus* ► *WP 29*

eettinen koodi

kts. *eettiset ohjeet*

eettiset ohjeet

en code of conduct; code of ethics

tietyn ammattialan, esimerkiksi tietojenkäsittelyn piirissä hyväksytyt periaatteet ammatissa toimimisesta

▲ *ohje, sääntö* ► *laki, normi, säädökset, tietotekniikan väärinkäyttö* ▼ *BS 7799, CISA, CISSP, hyvä tiedonhallintatapa, hyvä tietojenkäsittelytapa*

EFQM

European Foundation for Quality Management

Euroopan laatusäätiö, joka on julkaissut organisaation toiminnan laatukriteerejä, jotka puolestaan sisältävät myös tietoturvanäkökohtia

▲ *järjestö*

ehdollinen pommi

en logic bomb

tuholaisohjelma, joka toimii määrättyjen ehtojen toteutuessa, esimerkiksi tuhoten levyn tiedot vasta kun levyille on kertynyt tietty määrä tietoa

▲ *pommi, tuholaisohjelma ♣* ▼ *liipaisin*

eheys

en integrity

1) (tietojen tai tietojärjestelmän) aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus

2) ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta

▲ *laatu, ominaisuus* ► *aitous, kelpoisuus, kiistämättömyys, kirjausketju, käyttökelpoisuus, luotettavuus, luottamuksellisuus, oikeellisuus, tiedon peukalointi, tietoturvallisuus ♣, ylläpito* ▼ *ehyt tieto, pirstoutuminen, tarkastaa (1), turmeltua, turmeltuminen*

eheyttää

en defragment

järjestää pirstoutunut muisti uudelleen niin, että kukin tiedosto on tallennettuna yhtenä jatkumona

► *muistivuoto, pirstoutuminen*

ehtoilmoitus

en legal notice

sivustoon sijoitettu ilmoitus, jolla asetetaan ehtoja sivuston käytölle tai rajataan sivuston tarjoajan vastuita

ehyt tieto

en integral data

tieto, joka on säilyttänyt eheyden

▲ *eheys, tieto*

ei-julkinen tieto

en non-public information

tieto, jonka antamiseen ei ole velvollisuutta, mutta viranomainen voi harkintansa mukaan sen tehdä Ei-julkisia ovat muun muassa valmisteltavana olevat asiakirjat ja sisäiset viranomaispalvelut.

▲ *julkinen, julkisuuslaki, tieto, tietojen luokitus* ► *pääsy, salainen*

ekstranet

kts. *vierasverkko*

elektromagneettinen pulssi

mts. *sähkömagneettinen pulssi*

elektroninen sodankäynti

mts. *sähköinen sodankäynti*

▲ *sodankäynti*

elintärkeä sovellus

en vital application

tietojärjestelmän omistajan osoittama sovellus, jonka se katsoo välttämättömäksi keskeisten toimintojensa ylläpitämiseksi

▲ *tärkeysluokitus* ▶ *jatkuvuussuunnitelma, valmiusraportti*

elliptinen salaustekniikka

en elliptical curve cryptography

epäsymmetrisen salauksen avainten tuottamisen matemaattinen menetelmä, jossa käytetään hyväksi elliptisten käyrien ominaisuuksia

▲ *epäsymmetrinen salaus, salaustekniikka*

elpymissuunnitelma

mts. *toipumissuunnitelma*

elvytys

mts. *toipuminen*

EMP

electromagnetic pulse

sähkömagneettinen pulssi

▶ *HPM*

ENISA

European Network and Information Security Agency

Euroopan tietoturvavirasto

▲ *viranomainen* ▶ *BSI, FICORA, NCSC, NIPC*

ennakoiva tietoturvallisuus

en proactive information security

tietoturvapoliittika, jonka pääpaino on etukäteissuunnittelussa ja organisaation toimintamahdollisuuksien turvaamisessa

▲ *tietoturvallisuus* ♣, *tietoturvapoliittika* ▶ *puolustautuva tietoturvallisuus, turvallisuusjohtaminen* ▼ *ennaltaehkäisy, SMART*

ennaltaehkäisy

en preventive measures

ennakoiva toiminta tai menettely, joka vähentää järjestelmän haavoittuvuutta

▲ *ennakoiva tietoturvallisuus* ▶ *haavoittuvuus*

EP

electronic protection

suojautuminen sähköisessä sodankäynnissä

▲ *sähköinen sodankäynti*

epidemia

en epidemic

haittaohjelman tai vääristyneen tiedon leviäminen verkossa satunnaisesti

▲ *haittaohjelma* ♣, *tuholaisohjelma* ♣ ▶ *tartunta, virus* ♣

epäsymmetrinen salaus

en asymmetric encryption

salaus, jossa viestin avaaminen tapahtuu eri avaimella kuin sen salakirjoitus

▲ *salaus* ▶ *symmetrinen salaus* ♣, *yhdistelmäsalauk* ▼ *elliptinen salaustekniikka, julkinen avain, julkisen avaimen menetelmä* ♣, *RSA, yksityinen avain*

eristää

en quarantine (v)

viedä (virus tai muu haittaohjelma tai sen saastuttama tiedosto) paikkaan, jossa vahingonteko ei ole enää mahdollista

▲ *suojaus* ▶ *ansa, haittaohjelma* ♣, *saastua, virus* ♣

erittäin salainen

en top secret

valtionhallinnon turvaluokituksen mukaan I turvaluokkaan kuuluva äärimmäisen arkaluonteinen, salassa pidettävä tieto

▲ *salainen, turvaluokitus* ▶ *viranomaisen asiakirja*

erityissuojattava tieto

en especially protected information

viranomaisen asiakirja tai tieto, jonka käsittelylle on asetettu erityisiä tietoturva vaatimuksia luotamuksellisuuden (salassapito, tietosuoj), eheyden tai käytettävyyden suhteen

Eryityssuojattavat tiedot voidaan periaatteessa jakaa kolmeen luokkaan:

I - tiedon oikeudeton paljastuminen vaarantaisi keskeisiä yleisiä etuja

II - tiedon oikeudeton paljastuminen ja käyttö loukkaisi merkittävästi niitä etuja, joiden vuoksi rajoitukset on määrätty

III - tiedon oikeudeton paljastuminen ja käyttö vaarantaisi viranomaisen toimintaedellytyksiä taikka liike- ja ammattisalaisuuksia tai henkilötietojen suojaa.

▲ *suojaus, tieto, turvaluokitus* ▶ *salainen, vaatimus*

erityistilanne

en exceptional situation

normaaliolojen häiriötilanne, joka vaatii viranomaisten erityistoimia ja yhteistoiminnan tehostamista normaaliin toimintavaltuuksien puitteissa, esimerkiksi laajavaikutteinen rikos tai terrorismi tai tietotekniikkaan tai tietoliikenteeseen kohdistuva laajavaikutteinen häiriö

Tarkempi määrittely on annettu valtioneuvoston tiedotusohjeessa 10.3.1994.

▲ *tilanne* ► *katastrofi*, *poikkeusolot*, *poikkeustilanne*

escrow

kts. *vara-avainjärjestelmä*

esittäytyminen

en introduction

käyttäjän ilmoitus sisäänkirjauksen yhteydessä järjestelmälle tai tietoverkon palvelulle, kuka hän on, sekä mahdollisesti palvelun esittely käyttäjälle

▲ *käyttäjä*, *sisäänkirjaus* ► *todennus*, *tunnistus*

esto

en congestion

1) tilanne, jossa toimitus tai toiminto on estetty
2) dataverkossa tilanne, jossa käyttäjä ei saa yhteyttä verkon liikenteen ruuhkautumisen takia

▲ *yhteys* ► *dataverkko*, *estää*, *pimittää*, *vika*
▼ *palvelun esto*, *palvelunestohyökkäys*

estää

en inhibit; deny

1) keskeyttää toimitus tai toiminto toisen toimituksen tai toiminnon ajaksi

2) häiritä tai pysäyttää toiminto, heikentää käytettävyyttä tai aiheuttaa esto

▲ *käytettävyys (1)* ► *esto*, *palvelun esto*, *pimittää*

ETSI

European Telecommunications Standards Institute

Euroopan alueen teletekninen standardointilaitos

▲ *standardointielin* ► *CEN*, *CENELEC*, *SFS*
▼ *TETRA*

etähuolto

en telemaintenance

tietoverkkoon kytketyn laitteen huolto, jossa laite lähettää tiedot tilastaan automaattisesti verkon välityksellä huoltopisteeseen ja saa sieltä ohjeet huoltotoimenpiteiksi tai vian korjaamiseksi

▲ *huolto (1)* ► *monitori*, *seurain*, *televalvonta*, *verkkopalvelu*, *vika*

etäkutsu

en remote procedure call

aliohjelman kutsu verkon välityksellä toisesta tietokoneesta

etäkäyttö

en remote access; remote login

tietokoneen tai lähiverkon palvelujen käyttö lähiverkon ulkopuolelta

▲ *käyttö (1)*, *tietoverkko* ♣ ► *etätyö* ▼ *rlogin*, *töiden etäsyöttö*, *vastakutsu*

etätyö

en telework

työnteko oman organisaation lähiverkon ulkopuolella mutta käyttäen organisaation tietotekniikkapalveluja ja -resursseja

► *etäkäyttö*, *etäyhteys*, *lähiverkko*, *verkkopalvelu*

etäyhteys

en remote connection; remote access

datayhteys organisaation lähiverkkoon ja sen palveluihin organisaation tilojen ulkopuolelta, esimerkiksi matkalla olon tai etätyön takia

▲ *yhteys* ► *etätyö*, *lähiverkko*

eväste

en cookie

web-palvelimesta verkkoaseman web-selaimeen palvelimen lähettämä tietue, jonka avulla palvelin ja selain voivat pysyä yhteydessä toisiinsa, vaikka fyysinen yhteys välillä katkeaisikin

▲ *yhteys* ► *verkkojäljite*

EW

electronic warfare

sähköinen sodankäynti

▼ *C2W*

EWOS

European Workshop for Open Systems

Eurooppalaisten tietotekniikkayritysten järjestö avoimien tietotekniikkastandardien kehittämiseksi ja soveltamiseksi useita standardeja sisältävinä standardiprofiileina

EWOSilla on tietoturvasuutta käsittelevä ryhmä nimeltä EG-SEC.

▲ *järjestö*, *standardointielin*

extranet

kts. *vierasverkko*

F**fi-juuri**

en fi root

tietokanta, johon on merkitty Suomessa myönneetyt eli fi-maatunnuksen alaiset Internet-verkkotunnukset

▲ *Internet*, *maatunnus*, *verkkotunnus* ► *tunnus-hallintokeskus*, *verkkotunnuslaki*

FICORA

Finnish Communications Regulatory Authority

Viestintävirasto

▶ *ENISA*

FINEID

Finnish Electronic Identification

Suomessa sähköisessä asiointinnassa käytettävä henkilön tai organisaation tunnus

Huom. FINEID ei ole sama kuin henkilö- tai LY-tunnus.

▲ *tunnus* ▶ *HST*

FIPS

Federal Information Processing Standard

Yhdysvaltain liittovaltion hallinnon tietotekniikkastandardi

▶ *JHS*

FIRST

Forum of Incident Response and Security Teams kansainvälinen yksityisoikeudellinen järjestö, jonka toimenkuvaan kuuluu tietoturvaluukista tiedottaminen sen jäsenille ja tietoturvaloukkausten ehkäisyyn, havaintaan ja niistä toipumiseen tähtäävä yhteistyö

Jäsenistö käsittää kansallisia CERT-organisaatioita sekä yrityksiä, yhdistyksiä ja viranomaisia.

▲ *järjestö* ▶ *CERT*

FTPS

FTP- ja SSL-käytännöt yhdistämällä toteutettu suojattu tiedostonsiirtokäytäntö

▲ *SSL, yhteyskäytäntö*

fyysinen turvallisuus

en physical security

henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan

Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartiointin, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan sekä kuriirin ja tietoaineistoja sisältävien lähetysten turvallisuuden.

▲ *tietoturvallisuus* ♣, *turvallisuus* ▶ *käyttöturvallisuus, tietotekniikan turvallisuus, vahinko* ▼ *kulunvalvonta, laitteistoturvallisuus, toimitilaturvallisuus*

G

GIAC

Global Information Assurance Certification

tietoturvallisuuden ammattipätevyyden todistus, jonka myöntää SANS-instituutti

▲ *SANS* ▶ *CISA, CISSP*

H

haastemenetelmä

en challenge-response method

todennuksen menetelmä, jossa kutsuttu palvelin tai viestin saaja pyrkii varmistumaan kutsujan tai lähettäjän aitoudesta ottamalla tähän uuden yhteyden tai esittämällä tälle kysymyksen, johon vain oikea taho voi vastata oikein

Esim. pankkien Suomessa käyttämässä todennusmenetelmässä verkkopankin käyttäjän on annettava joka kerta muuttuva tunnusluku, joka on vain hänen tiedossaan.

▲ *menetelmä, todennus* ▶ *aitous, salalause, salasanatunnistus, todennustiedot, vastakutsu*

haavoittuvuus

en vulnerability

alttius tietoturvallisuutta uhkaaville tekijöille

▲ *ominaisuus* ▶ *altistus, ennaltaehkäisy, riski, riskienhallinta, sitkeys, tietosodankäynti* ♣, *tietoturvallisuus* ♣, *turvaohjelma* ♣, *uhka, verkkolinake* ▼ *tietoturva-aukko*

haavoittuvuusskannaus

en vulnerability scan

tietoverkossa kohdejärjestelmän palveluissa olevien tunnettujen haavoittuvuuksien automaattinen haku, esimerkiksi murtokokeilla tai tutkimalla palvelimen ohjelmistoversiota

▲ *luotaus, skannaus* ▶ *porttiskannaus*

haavoittuvuustutkimus

en vulnerability analysis

tietojärjestelmän haavoittuvuuden ja riskien sekä turvatoimien riittävyyden systemaattinen selvittäminen

▶ *riskianalyysi, uhka-analyysi*

haittaohjelma ♣

en rogue program

järjestelmään kuulumaton ohjelma, joka on yleensä liitetty siihen salaa ja joka haittaa järjestelmän toimintaa

Haitan aste voi vaihdella vähäisestä ajanhukasta aina tietojen tai ohjelmien tuhoutumiseen, vääristymiseen tai vääriin käsiin joutumiseen saakka.

▲ ohjelma ▶ datapohjainen hyökkäys, eristää, monistuva ohjelma, murto-ohjelma, tekeytyminen, tuholaisohjelma ♣, virusvaroitus ▼ aikapommi, bakteeri, epidemia, kameleontti, lataus, loisohjelma, mato ♣, palvelunestohyökkäys, papukaija, pommi, troijanhevonon, virus ♣

hajasäteily

en scattered electromagnetic radiation

elektronisesta laitteesta dataa siirrettäessä, tallennettaessa tai näytettäessä lähtevä sähkömagneettinen säteily

Säteilyn perusteella on mahdollista siepata laitteessa käsiteltävää tai näytettävää dataa.

▲ tietoturvariski ▶ näppäinloki, siepata, signaalitiedustelu ♣, sähkömagneettinen pulssi, Tempest

hajautettu palvelunestohyökkäys

en distributed denial of service attack

palvelunestohyökkäys samanaikaisesti useista työasemista, jotka yleensä on kaapattu tähän tarkoitukseen

▲ palvelun esto, palvelunestohyökkäys ▶ kaapata, koukkaus, orja

hakemistopalvelu

en directory service

julkisen avaimen järjestelmässä palvelu, joka hallitsee käyttäjien varmenteita ja sulkulistoja sisältäviä hakemistoja

Huom. 1) Hakemisto voi olla yksi valtakunnallinen tietokanta tai hajautettu, jolloin sen osat muodostavat hierarkkisen järjestelmän.

Huom. 2) Palvelu toteutetaan hakemistopalveluilla (DSA, Directory System Agent). Hakemistopalvelimet käyttävät keskenään hakemistopalvelukäytäntöä (DSP, directory system protocol). Käyttäjät (ihmiset tai ohjelmat) käyttävät hakemistoa käyttäjäagentin (DUA, directory user agent) avulla. Käyttäjäagentti on yhteydessä hakemistopalvelimeen hakemistokäytännön (DAP, directory access protocol) avulla.

▲ palvelu, verkkopalvelu ▶ julkisen avaimen järjestelmä, varmennehakemisto ▼ LDAP, sulkulista

hakkeri

en hacker

innokas tietokoneharrastaja

Sana on myös saanut kielteisen lisämerkityksen murtautuja

▲ käyttäjä ▶ hakkerointi, haktivisti, krakkeri, murtautuja, skriptari, valkolakki

hakkerointi

en hacking

1) tietokoneen innokas, harrastuksenomainen käyttö

2) tietojärjestelmiin murtautuminen

▲ käyttö (1) ▶ hakkeri, tietomurto, verkkosodankäynti ♣

haktivisti

en hactivist

henkilö, joka osoittaa mieltään tietoverkossa aiheuttamalla haittaa vastustamansa tahon toiminnalle verkossa

▶ hakkeri

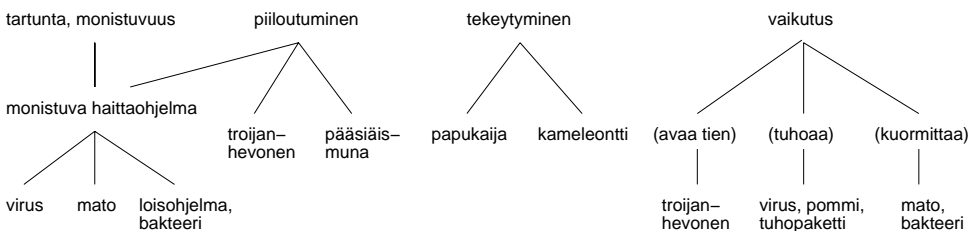
hallinnollinen tietoturvallisuus

en administrative and organizational information security

tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta

▲ tieto, tietoturvallisuus ♣, turvallisuus ▶ aineistoturvallisuus, ohjelmistoturvallisuus

Haitta- ja tuholaisohjelmia jonkin ominaispiirteensä mukaan



hallinnon sähköinen asiointi

en online government; electronic government
verkkواسointi hallinto- tai oikeusasioissa

▲ sähköinen asiointi, viranomainen ▶ varmenne, verkkoasiointilaki ▼ sähköinen asiointitunnus, sähköinen henkilökortti

hallinta

en management

1) monitahaisen kokonaisuuden hoito niin, että kokonaisuus ja sen eri osat voivat toimia tarkoitetulla tavalla

2) varusohjelmiston toiminto, joka huolehtii tietoteknisten välineiden ja voimavarojen tai tietojen saattamisesta käytettäväksi

▶ hallinto, järjestelmän omistaja, käytettävyys (1), ohjaus ▼ avaintenhallinta, käyttövaltuuksien hallinta, laadunhallinta, riskienhallinta, verkonhallinta, verkonhallintajohjelmisto, web-vastaava

hallinto

en management

voimavarojen, välineiden tai tietojen organisoinnista ja käytöstä määrääminen

▶ hallinta, Viestintävirasto ▼ tietohallinto, tunnus-hallintokeskus, varmennehallinto

harkinnanvaraisesti julkinen asiakirja

kts. ei-julkinen tieto

harmaa vyöhyke

en demilitarized zone

palomuurin ulkopuolinen, mutta palomuuria käyttävän organisaation hallinnassa oleva verkkolohko, johon voidaan sijoittaa esimerkiksi organisaation web-palvelin

▶ palomuuuri ♣, vierasverkko

hash-arvo

kts. tiiviste

heikko salaus

kts. kevyt salaus

▲ salaus

heikko tunnistus

kts. kevyt tunnistus

▲ tunnistus

HEL

high energy laser
suurenergialaser

henkilökortti

en identification card

kortti, jota käytetään haltijansa tunnistamiseen, esimerkiksi osoituksena henkilöllisyydestä tai valtuudesta

Suomessa käytettävistä henkilökorteista säädetään henkilökorttilaissa (829/1999).

▲ kortti, tunnistus ▶ henkilökorttilaki ▼ sähköinen henkilökortti

henkilökorttilaki

en Identity Card Act

perinteisen ja sähköisen henkilökortin sisältöä, myöntämistä ja käyttöä koskeva laki (829/1999)

▲ laki, tietotekniikkaoikeus, tietoturva-oikeus ▶ henkilökortti

henkilörekisteri

en person register

käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuva henkilötietoja sisältävä tietojoukko, jota käsitellään osin tai kokonaan atk:lla tai joka on teknisesti järjestetty niin, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia

▶ henkilötielaki, rekisterinpitäjä ▼ kielto-oikeus, rekisteriseloste, rekisteröity

henkilörekisteririkkomus

en misdemeanor in processing of personal data
henkilötietolain vastainen toiminta, josta tässä laissa on rangaistusseuraamus

Henkilörekisteririkkomuksia ovat henkilötietojen käsittelyä koskevien säädösten noudattamisen laiminlyönti, väärin tietojen antaminen tietosuojaviranomaiselle, henkilötietojen suojaamista ja hävittämistä koskevien säännösten rikkominen ja tietosuojalautakunnan määräyksen rikkominen, ellei muualla laissa ole säädetty ankarampaa rangaistusta. Rikoslaisissa on lisäksi määrättyjä rangaistukset henkilörekisteririkoksista.

▲ henkilötielaki, rikkomus ▶ henkilörekisteririkos, tietosuojarikos

henkilörekisteririkos

en crime in processing of personal data

vakava henkilötielain vastainen toiminta, josta rikoslaisissa on rangaistusseuraamus

Henkilörekisteririkoksia ovat mm.

- henkilötietojen käsittely vastoin lain säännöksiä, jotka koskevat käyttötarkoituksen mukaisuutta, tietojen tarpeellisuutta ja virheettömyyttä, arkaluonteisia tietoja ja henkilötunnusta

- rekisteröidyn tarkastusoikeuden estäminen

- henkilötietojen siirto EU:n tai ETA:n ulkopuolelle vastoin henkilötielain säännöksiä.

▲ henkilötielaki, rikos, tietotekniikkarikos ▶ henkilörekisteririkkomus, tietosuojarikos

henkilöstöturvallisuus

en personnel security

henkilöstöön liittyvien tietoturvariskien hallinta henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta

▲ tietoturvallisuus ♣, turvallisuus

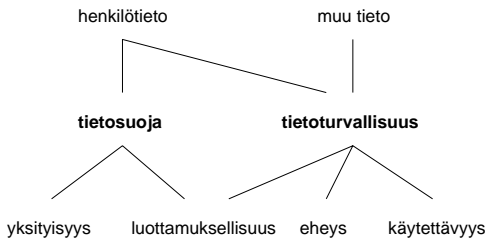
henkilötieto ♣

en personal data

luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolojaan kuvaava merkintä, joka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa elävää koskevaksi

▲ tieto ▼ tietosuoja ♣

Tietosuoja ja tietoturvallisuus: kohteita ja painopisteitä



henkilötietolaki

en Personal Data Act

luonnollisia henkilöitä kuvaavien tietojen keruuta, tallentamista ja käyttöä Suomessa säätelevä laki (523/1999)

Henkilötietolakia on sovellettava tietojenkäsittelyyn, joka tapahtuu atk:illa tai kun käsiteltävät henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri.

▲ laki, tietosuoja ♣, tietotekniikkaoikeus, tietoturva-oikeus, yksityisyyden suoja ▶ henkilörekisteri, tietosuojalautakunta, tietosuojavaltuutettu, työelämän tietosuojalaki ▼ arkaluonteinen tieto, henkilörekisteririkkomus, henkilörekisteririkos, rekisterimerkintärikos, rekisterinpitäjä, rekisteriseloste

henkilötunnus

en personal identification number

luonnollisen henkilön pysyvästi yksilöivä tunnus. Tunnus voi olla pysyvä, jos se ei sisällä muuttuvaa tietoa henkilöstä. Suomen henkilötunnus sisältää tiedon syntymäajasta ja sukupuolesta, jolloin, jos sukupuoli vaihtuu, henkilötunnus joudutaan vaihtamaan.

▲ tunnistus, tunnus, yksilöidä ▶ käyttäjätunnus, PIN, yksityisyys

henkilövarmenne

en personal certificate

varmenne, jota käytetään henkilön tunnistamiseen ja sähköisen allekirjoituksen tuottamiseen

▲ varmenne ▶ roolivarmenne, sähköinen allekirjoitus ▼ kansalaisvarmenne

HETU

henkilötunnus

▶ SATU

houkutuslintu

en honeypot

turvaohjelma tai -palvelin, joka pyrkii herättämään tunkelijan mielenkiinnon tekeytymällä huonosti suojatuksi palvelimeksi

▲ ansa, turvaohjelma ♣ ▶ papukaija, tekeytyminen

HPM

high power microwave

suuritehoinen mikroaalto

HPM:n taajuus on yleensä 1 -300 gigahertsiä, teho yli 100 MW ja sitä voidaan käyttää mm. tietoteknisten laitteiden tuhoamiseen.

▲ DEW ▶ EMP

HST

henkilön sähköinen tunnistaminen

fyysisen tai juridisen henkilön tunnistaminen sähköisen henkilökortin avulla

▶ FINEID, sähköinen henkilökortti

HTTPS

Secure Hypertext Transfer Protocol

HTTP- ja SSL-käytännöt yhdistämällä toteutettu suojattu yhteyskäytäntö

▲ SSL, turvakäytäntö ▶ S-HTTP

huijausvirus

sama kuin valevirus

hukuttaminen

en flooding

tauoton kuormittavan liikenteen lähettäminen palvelimelle tarkoituksena palvelimen ylikuormittaminen ja saattaminen toimintakyvyttömäksi

▶ bakteeri, palvelunestohyökkäys ▼ sähköpostipommitus

hunajapurkki

kts. houkutuslintu

huolto (1)

en maintenance; service

toiminta, jonka tarkoituksena on pitää järjestelmä tai laite käyttökunnossa

▲ käytettävyys (1) ▶ käyttö (2), toimintahäiriö, ylläpito ▼ etähuolto, puhdistus

huolto (2)

en service

yhteiskunnan, yrityksen tai muun organisaation tuottama palvelu yhteiskunnan tai talouselämän toimintojen ylläpitämiseksi tai laajasti koetun tarpeen tyydyttämiseksi

Esim. energiahuolto, tietohuolto, varaosahuolto.

▲ palvelu ▼ huoltovarmuus

huolto- ja laitevalmiussopimus

sopimus, joka määrittelee ajan, jonka kuluessa tuhon jälkeen huolletut laitteet ovat jälleen normaalissa käyttökunnossa

▲ huoltovarmuus, käytettävyys (1)

huoltovarmuus

en security of supply

väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömien toimintojen turvaaminen poikkeusolojen varalta

Laki huoltovarmuuden turvaamisesta 1390/1992.

▲ huolto (2), käytettävyys (1) ► jatkuvuussuunnitelma, poikkeusolot ▼ huolto- ja laitevalmiussopimus, Huoltovarmuuskeskus, huoltovarmuuspäätös

Huoltovarmuuskeskus

en National Emergency Supply Agency

kauppa- ja teollisuusministeriön hallinnonalaan kuuluva erityisviranomainen, jonka tehtävänä on Suomen taloudellisen huoltovarmuuden ylläpito ja kehittäminen

▲ huoltovarmuus, viranomainen ▼ VAVK

huoltovarmuuspäätös

en Government Resolution on Security of Supply
valtioneuvoston päätös huoltovarmuuden tavoitteista 8.5.2002

▲ huoltovarmuus, päätös, varautuminen

hyvä tiedonhallintatapa

en good data management practice

huolehtiminen asiakirjain ja tietojärjestelmien sekä niihin sisältyvien tietojen saatavuudesta, käytettävyydestä, suojaamisesta, eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä

Julkisuuslain mukaan hyvään tiedonhallintatapaan sisältyy diaarin ja rekisteriselosteiden huolellinen ylläpito, asiakirjajulkisuuden vaatimat järjestelyt, asianmukainen tietosuojajärjestelyt, henkilökunnan koulutus ja informointi näistä seikoista, niitä koskevien ohjeiden noudattamisen valvonta, sekä varautuminen suunniteltujen hallintouudistusten vaikutuksiin asiakirjain julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun.

▲ eettiset ohjeet, julkisuuslaki, laatu ► hyvä tietojenkäsittelytapa

hyvä tietojenkäsittelytapa

en good data processing practice

tietojenkäsittelyä koskevaa lainsäädäntöä ja sen soveltamisohjeita noudattavat menettelyt

▲ eettiset ohjeet ► hyvä tiedonhallintatapa, tietoturvallisuus ♣

hyväksymisjärjestelmä

kts. akkreditointijärjestelmä

hyväksymistarkastus

en acceptance test

toimet, joilla todetaan, täyttääkö tuote tai työn tulokset vaatimukset

▲ tarkastus (1) ► akkreditointi, arviointi, vaatimus

hyökkäys

en attack

yritys vahingoittaa tai rajoittaa tietojärjestelmän tai tietoverkon toimintaa, esimerkiksi tunkeutumalla suojattuun tietojärjestelmään

▲ tietojärjestelmä, tietotekniikan väärinkäyttö, tietotekniikkarikos ► hyökkääjä, tunkeutuminen, turmeltuminen, urkintatekniikka, verkkolinnake ▼ aktiivinen hyökkäys, datapohjainen hyökkäys, loiskäyttö, modeemihyökkäys, palvelunestohyökkäys, passiivinen hyökkäys, sanakirjahyökkäys, tekeytyminen, verkko-osoitteen väärentäminen, väsytyshyökkäys

hyökkääjä

en perpetrator

taho, jonka katsotaan aiheuttavan tai aiheuttaneen uhan tai hyökkäyksen

► hyökkäys, murtautuja, uhka

häirintä

en interference

vihamielisen tahon tai fyysisen ympäristön jatkuva epäsuotuisa vaikutus esimerkiksi toimivuuteen tai tietoturvallisuuteen

▲ käytettävyys (1), tietosodankäynti ♣ ► palvelunestohyökkäys, suojaus, vika ▼ tietoliikenteen häirintä

häiriö

en failure; malfunction

1) tilanne tai tapahtuma, jonka vuoksi järjestelmä ei toimi normaalisti

2) toiminnan jonkin osatekijän haitallinen vaihtelu, jonka puitteissa toiminta voi silti pääosin jatkua

▲ käytettävyys (1), luotettavuus ► jatkuvuussuunnitelma, varajärjestelmä, varautuminen, vika ▼ katastrofi, toimintahäiriö, turvallisuushäiriö, varallaolo

häiriöaika

en downtime

aika, jona laite tai järjestelmä ei ole käyttökunnossa

▲ *käytettävyys (1)*

hälytysviesti

en security alert

välikohtausta tai mahdollista tieturvaloukkausta koskeva määrämuotoinen viesti

► *tietomurtohälytin, turvallisuushäiriö*

I**IANA**

Internet Assigned Numbers Authority

Internetin yleisiä teknisiä hallintotehtäviä, kuten tunnushallintoa hoitava taho, nykyisin *ICANN*

▲ *Internet, tunnushallintokeskus* ► *ICANN*

ICANN

Internet Corporation of Assigned Names and Numbers

Internet-verkon tunnusjärjestelmiä hallinnoiva amerikkalainen yritys

USA:n valtion kanssa tehdyn sopimuksen mukaan ICANN:in tehtäviin kuuluu ylimmän tason juuritunnusten hallinnointi, IPv4- ja IPv6- osoitelohkojen myöntäminen ja eräiden teknisten määrittelyjen vahvistaminen

▲ *Internet, tunnushallintokeskus* ► *IANA, nimenvaltaus*

ICT

information and communication technologies
tieto- ja viestintätekniikat

ID

identifier; identification; identity document
tunniste, henkilöllisyys, henkilökortti

IDAP

Interdomain Access Protocol

Internetissä toimiva hajautettujen tietokantojen käytön valtuutus- ja todennuskäytäntö

▲ *Internet, todennus, yhteyskäytäntö*

IDEA

International Data Encryption Algorithm

patentoitu symmetrisen lohkosalausmenetelmä, jossa avaimen pituus on 128 bittiä

▲ *lohkosalaus, symmetrinen lohkosalaus, vahva salausalgoritmi* ► *Blowfish, DES*

identiteettivarkaus

en theft of identity

tilanne, jossa yksityinen avain tai jokin muu tunnistuksen väline kaapataan jonkun muun kuin sen laillisen haltijan käyttöön

▲ *tietorikos, tietotekniikkarikos* ► *kaapata, (käyttäjän) manipulointi, salasana*

IDS

intrusion detection system

tietomurtohälytin

► *ASIM*

IETF-standardi

Internet Engineering Task Force'n hyväksymä Internet-standardi

▲ *Internet, standardi* ▼ *IPSec, ISAKMP, Kerberos, NAT, OpenPGP, TLS*

informaationsodankäynti

kts. *tietosodankäynti* ♣

infrastrukturi

kts. *perusrakenne*

infrastruktuurisodankäynti

en infrastructure warfare

yhteiskunnan perusrakenteisiin kohdistuva tietosodankäynti

▲ *perusrakenne, sodankäynti, tietosodankäynti* ♣
► *NIPC, NISCC, OCIPEP*

Internet

tutkimus- ja yliopistopiireistä 1990-luvulla yleiseen käyttöön levinnyt kaikille avoin pakettivälitteinen TCP/IP-käytäntöjä noudattavien tietoverkkojen ja yhdyskäytävien muodostama maailmanlaajuinen verkosto

▲ *tietoverkko* ♣ ► *omaverkko* ▼ *fi-juuri, IANA, ICANN, IDAP, IETF-standardi, P3, TACACS+, TCP/IP, tunnushallintokeskus, verkko-tunnus, verkkotunnuslaki, vierasverkko, VPDN*

IPSec

Internet Protocol Security

IETF-standardi IP-verkon liikenteen suojaamiseksi pakettitasolla käyttämällä salaustekniikkaa

▲ *IETF-standardi, tietoturvastandardi* ► *turvareititin*

ISAC

Information Sharing Analysis Center

Yhdysvalloissa hallinnon ja elinkeinoelämän yhteiselin perusrakenteiden turvaamiseen liittyvissä asioissa

▲ *järjestö* ► *NIPC*

ISAKMP

Internet Security Association and Key Exchange Protocol

Internet-standardi osapuolten väliseen avaintenvaihtoon

▲ *avaintenvaihtokäytäntö, IETF-standardi*

ISC2

Internat'l Information Systems Security Certification Consortium

kansainvälinen yksityisoikeudellinen järjestö, joka laatii tietoturvallisuuden ammattipätevyysvaatimuksia ja myöntää todistuksia

▲ *järjestö* ▶ *CISSP, SANS*

ISO 17799

tietoturvallisuuden eri alat kattava kansainvälinen standardi

▲ *tietoturvastandardi* ▶ *BS 7799, tietoturvapoliitikka, turvallisuustodistus*

ISO 9000

laadunhallintaa koskeva standardiperhe

▲ *laatu* ▶ *laadunhallinta*

ISO/IEC JTC 1

ISO/IEC Joint Technical Committee 1

ISO:n ja IEC:n yhteinen komitea, jonka tehtävänä on tietotekniikan yleisten menetelmien ja teknikkoiden standardointi

Tietoturvastandardeja laaditaan ensisijaisesti komitean alikomiteassa (SC) 27 ja sen työryhmissä.

▲ *standardointielin*

istunnon kaappaus

en session hijacking

istunnon kestäessä tapahtuva tietoturvallisuuden loukkaus, jossa tekeytyjä syrjäyttää oikean käyttäjän ja jatkaa tämän aloittamaa istuntoa

▲ *kaappaus, tietoverkkorikos* ▶ *oikeudenloukkaus, osoitteen kaappaus, tekeytyminen*

ITSEC

Information Technology Security Evaluation Criteria

EU:n laatimat tietoturvallisuuden arviointiperusteet, joiden soveltamista käsittelee käsikirja ITSEM - Information Technology Security Evaluation Manual

▲ *arviointi, tietoturvastandardi* ▶ *Common Criteria*

itsekoodaava virus

en self-garbling virus; self-encrypting virus

virus, joka tarttuessaan salakirjoittaa itsensä, jotta turvaohjelma ei havaitsisi sen ominaispiirteitä, ja käynnistyessään avaa salakirjoituksen

Torjunnan vaikeuttamiseksi virus saattaa vaihtaa salausavainta kunkin tartunnan yhteydessä.

▲ *virus* ♣ ▶ *kameleontti, piilovirus*

itsekorjaava koodi

en error-correcting code

koodi (1), jonka avulla esitetty tieto voidaan entistää tietoon tulleista virheistä huolimatta, kun virheiden lukumäärä on tietyissä rajoissa

▲ *tarkistaa (1)* ▶ *itsevarmistava koodi* ▼ *Reed-Solomon koodi*

itsetahdistava jonosalaus

en asynchronous stream cipher

jonosalauksen menetelmä, jossa uusi avain määräytyy edellisen avaimen ja edeltävän salatekstin funktiona

Menetelmä on haavoittuva, sillä siirtovirheiden sattua vastaantottava pää saattaa menettää avaimen hallinnan.

▲ *jonosalaus* ▶ *tahdistettu jonosalaus*

itsevarmistava koodi

en error-checking code; error-detecting code

koodi (1), jossa virheellinen merkki poikkeaa kaikista kelpaavista merkeistä, kun virheiden lukumäärän oletetaan pysyvän tietyissä rajoissa

▲ *varmistus (2)* ▶ *itsekorjaava koodi*

IW

information warfare

tietosodankäynti ♣

J

jakojäännösvarmistus

en residue checking; modulo N checking

numerosarjan, esimerkiksi koodin oikeellisuuden varmistaminen siten, että numerosarja käsitetään kokonaisluvuksi ja sen yhteydessä käytetään varmisteena tämä luku tietyllä vakiolla jaettaessa muodostuvaa jakojäännöstä

▲ *varmistus (2)* ▶ *kaikuvarmistus, oikeellisuus, ylimäärävarmistus*

jatkoaloitus

en checkpoint restart

keskeytyneen ajon jatkaminen varmistuskohdasta

▲ *käyttö (2)* ▶ *uudelleenaloitus, uusinta-ajo, virhelopetus, välivedos*

jatkuvuussuunnitelma

en continuity plan

suunnitelma siitä, miten tietojenkäsittely ja tiedon siirto tulee turvata niin, että ne voivat jatkua häiriöiden aikana ja niiden jälkeen myös poikkeusoloissa

▲ *käytettävyys (1), suunnitelma* ▶ *elintärkeä sovellus, huoltovarmuus, häiriö, tietoturvasuunnitelma, varautumissuunnitelma* ▼ *toipumissuunnitelma, valmiussuunnitelma*

JHS

julkisen hallinnon suositus

organisaatio ja järjestelmä suositusten tuottamiseksi menettelyiksi, joilla pyritään edistämään hallinnon tietojärjestelmien yhteentoimivuutta

▶ *FIPS*

johtamissodankäynti

en command-and-control warfare

omien sodanjohdon järjestelmien kehittäminen ja suojaaminen, ja konfliktitilanteessa eri keinoin tapahtuva vastustajan järjestelmien tuhoaminen, häirintä ja harhauttaminen

▲ *sodankäynti, tietosodankäynti* ♣ ▶ *sähköinen sodankäynti*

jonosalaus

en stream cipher

salakirjoitus muuntamalla tieto tietoaalkioittain, yleensä biteittäin

▲ *salakirjoitus* ♣, *salaus, salaustekniikka* ▶ *lohkosalaus* ▼ *itsetahdistava jonosalaus, kertasalain, tahdistettu jonosalaus*

JTC 1

ISO/IEC JTC

julkinen

en public; (in the) public domain

yleisesti tiedossa oleva tai tiedoksi saatavissa

▲ *ominaisuus* ▶ *luottamuksellinen, pääsy, salainen, tietojen luokitus, viranomaiskäyttö* ▼ *ei-julkinen tieto*

julkinen avain

en public key

julkisen avaimen menetelmässä käyttäjälle kuuluvasta avainparista se avain, joka on julkisesti saatavilla

▲ *avain, epäsymmetrinen salaus, salausavain* ♣ ▶ *salainen avain, yksityinen avain* ▼ *julkisen avaimen järjestelmä*

julkisen avaimen järjestelmä

en public key infrastructure

julkisen avaimen menetelmän käytön mahdollistava järjestely, jossa nimetyt varmentajat tuottavat käyttäjille avainparit, varmentavat ne digitaalisella allekirjoituksellaan ja jakavat ne käyttäjille, ylläpitävät julkisten avainten hakemistoja ja sulkulistoja sekä mahdollisesti antavat muita järjestelmän käyttöön liittyviä palveluja

▲ *julkinen avain, tietoturvallisuus* ♣ ▶ *hakemistopalvelu, luotettu taho, verkkoasiointi* ▼ *aikaleimäpalvelu, akkreditoitijärjestelmä, langaton julkisen avaimen järjestelmä, PGP, sulkulista, varmenne, varmennehallinto, varmentaja, X.509*

julkisen avaimen menetelmä ♣

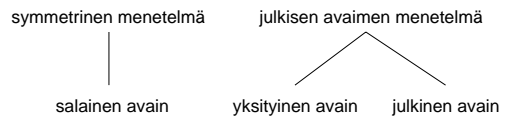
en public key method

epäsymmetrinen salausmenetelmä, jossa kullakin salakirjoituksen käyttäjällä on kaksi matemaattisesti toisiinsa liittyvää avainta: julkisessa hakemistossa julkaistava julkinen avain ja vain käyttäjän hallussa oleva yksityinen avain

Yksityisellä avaimella salakirjoitettu tieto voidaan avata vain vastaavalla julkisella avaimella, ja päin vastoin.

▲ *epäsymmetrinen salaus, menetelmä* ▶ *sähköinen tunnistus, vahva tunnistus* ▼ *PKCS, yksityinen avain*

Salausavaimia



julkisen avaimen varmenne

en public key certificate

julkisen avaimen järjestelmässä varmentajan omalla yksityisellä avaimellaan allekirjoittama tieto, joka sisältää käyttäjän julkista avainta ja käyttäjää itseään koskevaa informaatiota

▲ *varmenne* ▶ *juurivarmenne*

julkisuuslaki

en Act on the Openness of Government Activities
laki viranomaisten toiminnan julkisuudesta (621/1999)

▲ *laki, tietotekniikkaoikeus* ▶ *sananvapauslaki, tietosuojalaki, verkkokauppalaki, viranomaisen* ▼ *ei-julkinen tieto, hyvä tiedonhallintatapa, salassa pidettävä tieto, turvaluokiteltava tieto*

juurivarmenne

en root certificate

tietyn varmenneorganisaation ylimmän varmentajan varmenne, jonka se on itse allekirjoittanut

▲ *varmenne, varmennusorganisaatio* ▶ *julkisen avaimen varmenne, ylin varmentaja*

jäljitettävyys

en traceability

mahdollisuus jälkeen päin saada yksityiskohtaisesti selville, mitä toiminnassa, esimerkiksi tietojenkäsittelyprosessissa tapahtui

▲ *ominaisuus* ▶ *jäljituspaketti, kirjausketju, tarkastettavuus, uusittavuus*

jäljitysketju

kts. *kirjausketju*

jäljituspaketti

en trace packet

paketti, jonka käynti verkon kussakin solmussa aiheuttaa ilmoituksen solmusta verkonhallintaan

▲ *paketti, verkonhallinta* ▶ *jäljitettävyys, verkko-jälki*

järjestelmän omistaja

en system owner

nimetty taho, jolla on valta tai valtuudet päättää järjestelmästä

▶ *hallinta, ohjaus, rekisterinpitäjä, valtuus*

järjestelmäseloste

en system description

asiakirja, josta ilmenevät organisaation ylläpitämien tietojärjestelmien käyttötarkoitus ja niihin tallennettavat tietotyypit

▲ *seloste, tietojärjestelmä* ▶ *tietosuojaseloste*
▼ *rekisteriseloste*

järjestelmävastaava

en system administrator

henkilö, joka vastaa tietyn tietojärjestelmän toiminnasta

▲ *tietojärjestelmä, vastaava*

järjestelmävastuu

en system responsibility

tietoteknisen järjestelmän omistajan vastuut käyttäjille ja ulkopuolisille, kuten vahingonkorvausvelvollisuus ja todistustaakka järjestelmän asianmukaisesta toiminnasta

▲ *tietotekniikkaoikeus, tietoturvallisuus* ♣

järjestö

▼ *CEN, CENELEC, EFQM, EWOS, FIRST, ISAC, ISC2, WP 29, WPISP*

jäännöstieto

en residual data; residue

tietovälineeseen tai muistiin käsittelyn jälkeen jäänyt tieto, jota ei ole tarkoitus säilyttää

▲ *tieto, tietoriski* ▶ *ohjelmajäte, pengonta, puhdistus* ▼ *silppuri*

K

kaapata

en hijack; commandeer

ottaa valtuudetta ja oikeudetta haltuun tai hallintaan

▶ *hajautettu palvelunestohyökkäys, identiteettivarkaus, siepata, tekeytyminen, välistävetohyökkäys* ▼ *nimenvaltaus, orja*

kaappaus

en hijacking

kts. *kaapata*

▲ *rikos* ▼ *istunnon kaappaus, osoitteen kaappaus, verkkotunnuksen kaappaus*

kaatua

en crash

pysähtyä odottamatta

Tietokoneen tai ohjelman kaatumisesta seuraa usein merkittävää haittaa, kuten tietojen tai niiden eheyden menetys.

▲ *käytettävyys (1), luotettavuus* ▶ *pommi, virhe-lopetus*

kahdentaa

en duplex (v)

varmistustoimenpiteenä ylläpitää tai pitää käytössä rinnan kaksi identtistä tiedostoa, laitetta tai järjestelmää, yleensä toistensa yhteydessä

▲ *varmistaa* ▶ *toisintaa, vedostaa*

kaikuvarmistus

en echo checking; feedback error control

datansiirron virheiden paljastaminen lähettämällä vastaanotettu data takaisin lähetyspaikkaan, jossa sitä verrataan lähetettyyn dataan

▲ *varmistus (2)* ▶ *jakojäännösvarmistus, toistin, ylimäärävarmistus*

kaistanrajoitus

kts. *kuormanrajoitus*

kaksikäyttöavain

en dual use key

avain, jota voidaan käyttää sekä salausavaimena että aidonnusavaimena

▲ *avain* ▶ *salasavain* ♣, *todennusavain*

kaksikäyttötuote

en dual use product

tuote, tekniikka tai palvelu, jolla voi olla sekä siviiliuonteinen että sotilaallinen käyttötarkoitus

Useat salaustekniikan tuotteet on luokiteltu vienvälivonnassa kaksikäyttötuotteiksi.

▲ *salaustuote* ► *salausalgoritmi, salaustekniikka, Wassenaar-järjestely*

kameleontti

en chameleon

tunnettu hyötyohjelma, johon on lisätty tuholaisohjelman ominaisuuksia

▲ *haittaohjelma* ♣, *tuholaisohjelma* ♣ ► *itsekoodaava virus*

kansainvälinen yhteistoiminta

ks. *järjestö*

kansalaisvarmenne

en citizen's PKI certificate

väestörekisterikeskuksen tuotteistama ja ylläpitämä varmenne

Kansalaisvarmenne sisältää mm.

- varmentajan nimen
- varmenteen haltijan nimen
- haltijan sähköisen asiointitunnuksen (SATU)
- varmenteen voimassaoloajan
- varmenteen käyttötarkoituksen, sekä
- muita tietoja, kuten tietoja varmentajan käyttämistä laskentamenetelmistä ja varmennepoliitikasta.

▲ *henkilövarmenne, varmenne, VRK*

kansallinen tietoturvastrategia

en Government Resolution on National Information Security Strategy

valtioneuvoston periaatepäätös 4.9.2003 kansallisesta tietoturvallisuusstrategiasta

▲ *päätös, tietoturvapoliittikka, tietoturvastrategia*
► *turvallisuustietoisuus*

katastrofi

en disaster; catastrophe

erittäin vakava häiriö, jossa normaali toiminta lakkaa kokonaan tai sen jatkuvuus on uhattuna ja joka ei ole voitettavissa normaalein toipumistoinenpitein ja normaalein voimavaroin

▲ *häiriö* ► *erityistilanne, poikkeusolot, poikkeustilanne, toipumissuunnitelma* ▼ *katastrofisetiinen*

katastrofisetiinen

en disaster resistant

(järjestelmä) jonka perustoiminnot jatkuvat suurronnettomuudesta huolimatta

▲ *katastrofi* ► *vastustuskykyinen, vikasetiinen*

katkoton tehonsyöttö

en uninterrupted power supply; no-break power supply

jatkuvan ja riittävän laadukkaan sähkövirran tuottaminen, esimerkiksi tietokoneeseen, syöttötehon vaihteluista ja katkoksista huolimatta

▲ *käytettävyys (1), käytöturvallisuus*

katselmus

en review (s)

hankkeen tai työvaiheen päätyttyä pidettävä työn tulosten arviointi

Katsemukseen osallistuvat yleensä hankkeen osapuolet mutta usein myös ulkopuolisia. Katselmuksen tuloksia käytetään usein päätöksentekoon työn jatkamisesta.

► *arviointi, tarkastus (2)*

KBM

Krisberedskapsmyndigheten

Ruotsin valmiussuunnitteluviranomainen, jolla on myös perusrakenteiden turvallisuuteen liittyviä tehtäviä

▲ *valmiussuunnittelu* ► *NISCC, OCIPER, PTS*

kelpoisuus

en validity

1) asetettujen vaatimusten täyttäminen

2) kelpoisuuden (1) aikaan tai paikkaan sidotut rajat

▲ *laatu* ► *aitous, eheys, oikeellisuus, todennettavuus, vaatimus* ▼ *kelpuutus, käyttökelppoisuus, tarkastaa (1)*

kelpuutus

en validation

kelpoisuuden myöntäminen tai toteaminen

▲ *kelpoisuus* ► *akkreditointi, valtuutus*

Kerberos

joukko hajautetuissa tietojärjestelmissä käytettyjä monipuolisia tunnistuksen, pääsynvalvonnan, resurssien aidoituksen ja avaintenjakelun toimintoja, jotka on toteutettu monissa käyttöjärjestelmissä

IETF-standardi RFC 1510.

▲ *IETF-standardi, pääsynvalvonta, todennus*

Kerchoffsin periaate

en Kerchoffs' principle

periaate, jonka mukaan käytetty salakirjoitusmenetelmä täytyy olettaa vihollisen tuntemaksi, jolloin voi vain luottaa salausavaimen salassa pysymiseen

▲ *salakirjoitus* ♣, *tietojärjestelmäsodankäynti*

kerta-avain

en one-time key

salausavain, jota käytetään vain yhden tapahtuman tai siirron ajan

▲ *avain, salausavain* ♣ ▶ *kertasalain, kertatunnus* ▼ *SSH*

kertakirjaus

en single sign-on

sisäänkirjaus, joka mahdollistaa pääsyn samalla kertaa useisiin palveluihin ja verkkoihin

▲ *sisäänkirjaus*

kertasalain

en one-time pad

jonosalauksen menetelmä, jossa avain on täysin satunnainen ja yhtä pitkä kuin salakirjoitettava teksti

Menetelmä on turvallinen, mutta avaimen pituuden takia hankala käyttää.

▲ *jonosalaus, salain* ▶ *kerta-avain*

kertatunnus

en session key

tunnussana tai salasana, joka kelpaa vain yhtä käyttökertaa varten

▲ *tunnus* ▶ *dynaaminen salasana, kerta-avain*

kevyt salaus

en weak encryption

salaus, joka ei välttämättä kestä väsytyshyökkäystä

Esim. 56 bitin avainta käyttävää symmetristä salausta pidetään kevyenä.

▲ *salaus* ▶ *kevyt tunnistus, vahva salaus, väsytyshyökkäys*

kevyt tunnistus

en weak authentication

tunnistus tai todennus ilman varmennetta, esimerkiksi käyttäjätunnuksen ja salasanan perusteella

▲ *sähköinen tunnistus, tunnistus* ▶ *kevyt salaus, vahva tunnistus*

kielto-oikeus

en right to object

rekisteröidyn oikeus kieltää rekisterinpitäjää käsittelemästä häntä koskevia henkilötietoja markkinointia, mainontaa, sukututkimusta ja eräitä muita lain yleensä sallimia tarkoituksia varten

▲ *henkilörekisteri, oikeus* ▶ *kieltolista*

kieltolista

en Robinson list

rekisteriin tai verkkopalveluun liittyvä luettelo niistä rekisteröidyistä tai palvelun käyttäjistä, jotka eivät halua itseään koskevia tietoja käytettävän kaupallisesti

▲ *verkkopalvelu* ▶ *kielto-oikeus, sulkulista*

kiistattomuus

kts. *kiistämättömyys*

kiistämättömyys

en nonrepudiation

tietoverkossa eri menetelmin saatava varmuus siitä, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi Luovutukseen tai käsiteltäväksi jättämiseen voidaan liittää aikaleima, joka todistaa viestin saapumisajankohdan.

▲ *kiistää, laatu* ▶ *aikaleima, aitous, eheys, leima, turvaposti, verkkonotaari*

kiistää

en repudiate

kieltää olevansa tietyn viestin lähettäjä tai vastaanottaja

▼ *kiistämättömyys*

kirjausketju

en audit trail

alkutositteiden, syöttötietojen ja tulosteiden aukoton ketju, jonka avulla on mahdollista jäljittää yksittäisen tiedon käsittelyvaiheet

▲ *tarkastaa (1), varmistaa* ▶ *eheys, jäljitettävyyys*

kirjepommi

en letter bomb

sähköpostiviesti, jonka tarkoituksena on vahingoittaa vastaanottajan järjestelmää

▲ *pommi*

kolmas mies hyökkäys

kts. *välisävetohyökkäys*

kolmas osapuoli

kts. *luotettu taho*

kontrolli

kts. *varmistus, tarkastus, valvonta*

kontrollihäiriö

kts. *valvontakatko*

koodi

en code

kts. *salakirjoitus* ♣, *salasana, salausavain* ♣

▼ *PIN-koodi*

koodiavain

kts. *salausavain* ♣

koodiesitys

en coded representation

tiedon esittäminen kooditettuna, esimerkiksi salakirjoitettuna

koodin avaaminen

en decryption; deciphering

kooditetun tai salakirjoitetun tiedon muuntaminen alkuperäiseen muotoonsa

▲ *avata (2)* ► *salauksen ratkonta*

kopio

▼ *laiton kopio, toisiokanta, turvakopio, varmuuskopio*

korrupointi

kts. *turmeltuminen*

kortti

▼ *henkilökortti, toimikortti, valtuuskortti, viranomaiskortti*

koukkaus

en leapfrog attack

hyökkäys yhden tai useamman kolmannen osapuolen verkkoaseman kautta

▲ *aktiivinen hyökkäys* ► *hajautettu palvelunestohyökkäys, orja*

krakkeri

kts. *murtautuja, murto-ohjelma*

► *hakkeri*

kryptaus

kts. *salakirjoitus* ♣

kryptoanalyysi

kts. *salauksen ratkonta*

kryptografia

kts. *salaustekniikka*

kryptologia

kts. *salaustutkimus*

kryptoprosessori

kts. *salaussuoritin*

kuittaus

en confirmation; acknowledgement

tieto sanoman vastaanottajalta tai välittäjältä lähettäjälle siitä, että sanoma on vastaanotettu

kuitti

en cookie

kts. *eväste*

kulunvalvonta

en passage control; physical access control
ovien ja kulkuväylien tarkkailu tai valvonta, yleensä tarkoituksella estää asiattomien kulku

▲ *fyysinen turvallisuus, pääsynvalvonta, tarkkailu, toimitilaturvallisuus, valvonta*

kumota

en abort (v)

pysäyttää ajo tai prosessi kesken suorituksen

► *virhelopetus*

kumppaniverkko

kts. *vierasverkko*

kuoria

en skim

jäljentää normaalikäytön yhteydessä luvottomasti luottokortti tai muu valtuuksia sisältävä tietoväline myöhempää väärinkäyttöä varten

► *laiton kopio, luvaton käyttäjä*

kuormanrajoitus

en bandwidth throttling

verkossa siirrettävän datamäärän tarkkailu ja tarvittaessa rajoittaminen, jotta verkko tai palvelin eivät ylikuormitu

kylmä varakeskus

en cold site

toimitilat ja ei toiminnassa oleva laitteisto, jotka voidaan ottaa käyttöön kun normaalisti käytettävän toimitilan käyttö häiriintyy tai estyy

▲ *varakeskus*

käsittelijä

en processor

1) kts. *tietojenkäsittelijä*

2) henkilötietojen käsittelijä, joka on vaitiolovelvollinen

käsittelyvaltuus

en access authority

valtuus tietojen saantiin tai käsittelyyn, esimerkiksi lukuvaltuus, kirjoitusvaltuus, poistovaltuus

▲ *käyttövaltuudet, valtuus* ► *käyttöoikeus*

käynnistyslohkovirus

en boot sector virus

virus, joka tarttuu käyttöjärjestelmän käynnistyslohkoon

▲ *virus* ♣

käytettävyys (1)

en availability

ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla

▲ käyttö (1), laatu, ominaisuus ▶ ajantasaisuus, hallinta, käyttö (2), käyttökelpoisuus, luotettavuus, pääsy, saavutettavuus, sitkeys, suojaus, tietoturvallisuus ♣ ▼ estää, huolto (1), huolto- ja laitevalmiussopimus, huoltovarmuus, häirintä, häiriö, häiriöaika, jatkuvuussuunnitelma, kaatua, katkoton tehonsyöttö, ohitusmenettely, palvelun esto, saastuminen, tietoturvariski, toipuminen, toipumissuunnitelma, turmeltua, turmeltuminen, uhka, vahtiajastin, varajärjestelmä, varakeskus, varalaitteisto, varallaolo, varautuminen, varmistaa, varmistustiedosto, varmuuskopio, vastustuskykyinen, vika, vikakynnys, vikasietoinen, ylläpito

käytettävyys (2)

en usability

helppokäyttöisyys, käyttökelpoisuus

käyttäjä

en user

1) henkilö tai organisaatio, jota tietojärjestelmä palvelee

2) henkilö, joka työssään tai muussa toiminnassaan on välittömästi tekemisissä atk-laitteen kanssa esimerkiksi ohjaten järjestelmän toimintaa, syöttämällä tietoja, tekemällä kyselyjä tai olemalla keskustelukäytön osapuolena

▲ tietojärjestelmä ▶ (käyttäjän) manipulointi, salasana ▼ esittäytyminen, hakkeri, luvaton käyttäjä, nimimerkki, pääkäyttäjä (1), pääkäyttäjä (2), pääsynvalvontaohjelmisto, valtuutettu käyttäjä

käyttäjän profiili

en user profile

1) käyttöjärjestelmän, ohjelmiston tai palvelun käyttäjäkohtaiset asetukset

2) yhteenveto tai analyysi tietoverkon käyttäjän käynteistä verkon palvelussa tai palveluissa

▶ (käyttäjän) manipulointi, tietosuoja ♣, urkintatekniikka, verkkojälki

käyttäjätunnus

en user identifier

sisäänkirjauksen yhteydessä käyttäjän ilmoitettava hänet yksilöivä tunnistus

▲ tunnus ▶ henkilötunnus ▼ peitenimi

käyttö (1)

en use; utilization

(palvelun tai tietojärjestelmän) hyödyntäminen tarkoitukseensa

▲ tietojärjestelmä ▼ anonymikäyttö, etäkäyttö, hakkerointi, käytettävyys (1), käyttöoikeus, loiskäyttö, salakäyttö, tietotekniikan väärinkäyttö, tunnisteen käyttö, valtuus, viranomaiskäyttö

käyttö (2)

en operation(s)

työ tietoteknisen laitteiston pitämiseksi toiminnassa, mihin kuuluvat muun muassa alkuasetukset, toiminnan valvonta, töiden syöttäminen ja tietovälineiden asettaminen käyttölaitteisiinsa

▶ huolto (1), käytettävyys (1), loki ▼ aikakatkaistu, jatkoaloitus, käyttöturvallisuus, uudelleenaloitus, varmistuskohta

käyttöarkisto

en working archive

käyttäjää tai keskuslaitteistoa lähellä sijaitseva arkisto, josta tallenteet saadaan tarvittaessa nopeasti esille

▲ arkisto ▶ turva-arkisto, varmuusarkisto

käyttökelpoisuus

en usability

se, missä määrin tiedot täyttävät tietyn käytön asettamat vaatimukset esimerkiksi eheyden, kattavuuden, oikeellisuuden, relevanssin ja ajantasaisuuden suhteen

▲ kelpoisuus, ominaisuus ▶ eheys, käytettävyys (1), vaatimus

käyttöoikeus

en access right

oikeus käyttää tietojärjestelmän tiedostoja ja ohjelmia tietyillä tavoin, esimerkiksi lukemalla, päivittämällä tai muiden käyttöoikeuksia muuttaen

▲ käyttö (1), oikeus ▶ käsittelyvaltuus, käyttövaltuudet, pääsynvalvonta, valtuus ▼ viiteseurain

käyttöturvallisuus

en operations security

tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvät keinot tietoturvallisuuden parantamiseksi

▲ käyttö (2), tietoturvallisuus ♣, turvallisuus ▶ fyysinen turvallisuus, tietotekniikan turvallisuus, ylläpito ▼ katkoton tehonsyöttö

käyttövaltuudet

en usage rights; authorization

tietojärjestelmän käyttäjälle myönnetty yksilöidyt oikeudet nimettyjen osajärjestelmien käyttöön tai tietojen saantiin, esimerkiksi lukuvaltuus, kirjoitusvaltuus, poistovaltuus

▲ valtuus ▶ käyttöoikeus ▼ käsittelyvaltuus, käyttövaltuuksien hoitaja, luvaton käyttäjä

käyttövaltuuksien hallinta

en usage rights management

tietoturvallisuuden käyttövaltuuksia koskeva osa-alue

▲ hallinta, tietoturvallisuus ♣, valtuus

käyttövaltuuksien hoitaja

en security administrator

henkilö, jonka tehtävänä on käyttövaltuuksien käsittely, valtuuksien ylläpito ja hallinta sekä käytön seuranta

▲ käyttövaltuudet, vastaava

käytäntö

en protocol

1) yleisesti sovittu menettely kahdenvälistä yhteydenpitoa varten

2) tietoliikenteessä säännöstö, jota lähettävän ja vastaanottavan laitteen tulee noudattaa, jotta datansiirto onnistuisi tarkoitetulla tavalla

▲ yhteys ► menetelmä ▼ avaintenvaihtokäytäntö, turvakäytäntö, yhteyskäytäntö

L**laadunhallinta**

en quality management

asiakkaiden tarpeista ja odotuksista lähtevä organisaation toiminta, joka pyrkii toiminnan ja toimintaketjujen sekä niiden tuottamien tulosten korkeaan laatuun

▲ hallinta, laatu ► ISO 9000

laatu

en quality

kokonaisuuden menestymiseksi siltä tai sen osalta vaadittava ominaisuus tai ominaisuuksien joukko

Organisaation toimivuuden kannalta organisaation tuottamalta tai käyttämältä tiedolta vaadittavia ominaisuuksia voivat olla esimerkiksi *eheys*, *luottamuksellisuus*, *lainmukaisuus*, *käytettävyyys*, *kiistämättömyys* ja *todennettavuus*.

► arviointi, ominaisuus ▼ hyvä tiedonhallintatapa, ISO 9000, kelpoisuus, laadunhallinta, palvelutaso

laatuvarmenne

en qualified certificate

Euroopan Unionin sähköisen allekirjoituksen direktiivin mukaiset vaatimukset täyttävä varmenne. Laatuvarmennetta käytetään pelkästään allekirjoittamiseen, eikä siitä yleensä säilytetä kopioita.

▲ varmenne ► digitaalinen allekirjoitus, sähköisen allekirjoitus

laiton kopio

en pirate copy

ohjelman tai aineiston laittomasti tai sopimuksen vastaisesti valmistettu kopio

▲ kopio, luvaton, tekijänoikeus ► aineisto, avainpiiri, kuoria, piiloleima

laitteistoturvallisuus

en computer security; facilities security

tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi

▲ fyysinen turvallisuus, tietoturvallisuus ♣, turvallisuus ► aineistoturvallisuus, ohjelmistoturvallisuus, tietoliikenneturvallisuus

laki

► eettiset ohjeet, normi, oikeudenloukkaus, perusrakenne, sääntö, tietotekniset perusrakenteet ▼ allekirjoituslaki, arkistolaki, henkilökorttilaki, henkilötietolaki, julkisuuslaki, pakkokeinolaki, sananvapauslaki, tekijänoikeuslaki, televiestinnän tietosuojalaki, tietosuojalaki, työelämän tietosuojalaki, valmiuslaki, verkkoasiointilaki, verkkokauppalaki, verkkorikoslaki, verkkotunnuslaki, viestintämarkkinlaki

langaton julkisen avaimen järjestelmä

en wireless PKI

langattoman siirtotien kautta käytettävissä oleva julkisen avaimen järjestelmä

▲ julkisen avaimen järjestelmä

laskennallisesti murtovarma

en computationally secure

sellainen (salakirjoitus), jota ei uskota olevan mahdollista murtaa väsytystekniikkaa käyttäen nykyisin ajateltavissa olevalla laskentakapasiteetilla ja käytettävissä olevassa ajassa

► avain, murto-ohjelma, vahva salaus, väsytystekniikka

lataus

en payload

viruksen tai muun haittaohjelman se osa, joka on tarkoitettu tekemään tuhotyö kohdekoneessa

▲ haittaohjelma ♣, tuholaisohjelma ♣, virus ♣ ► liipaisin

LDAP

Lightweight Directory Access Protocol

X.500-hakemiston kanssa yhteensopiva yksinkertainen saantikäytäntö

▲ hakemistopalvelu ► RADIUS

leima

en stamp (s)

yleensä ulkopuolisen tahon dokumenttiin kiinnitämä tunniste, varmenne tai muu lisätieto

Leimaa käytetään usein dokumenttiin liittyvän seikan varmentamiseen, hyväksymiseen tai valtuuttamiseen.

▶ *kiistämättömyys, tunniste, tunnus, tuntomerkki, varmenne* ▼ *aikaleima, leimata, piiloleima*

leimata

en stamp (v)

liittää leima, esimerkiksi tieto tapahtuma-ajasta viestiin, tiedostoon tai muuhun tietoon

▲ *leima* ▶ *varmentaminen, yksilöidä*

levyrikko

en disk crash; head crash

vika, jossa magneettilevyn lukupää koskettaa levyn pintaa aiheuttaen tallennettujen tietojen tuhoutumisen kosketuskohdassa tai laajemminkin

▲ *vika* ▶ *turmeltuminen*

liipaisin

en trigger (s)

1) tapahtuma tai ehto, jonka toteutuminen käynnistää tietyn toiminnan

2) mekanismi, joka havaitsee ehdon toteutumisen ja käynnistää toiminnan

Esim. 1) tietokannan toiminto, joka muutoksen tapahtuttua käynnistää ennalta ohjelmoidun sarjan tarkistus- ja päivitystoimenpiteitä

Esim. 2) viruksen osa, joka havaitsee tartunnan tapahtuneeksi ja käynnistää panoksen

▲ *ehdollinen pommi, virus ♣* ▶ *lataus, vikakynnys*

lohkosalaus

en block cipher

salakirjoitus, jossa kiinteä määrä tietoalkioita salakirjoitetaan kerrallaan

▲ *salakirjoitus ♣, salaustekniikka* ▶ *jonosaluus*
▼ *DES, IDEA, symmetrinen lohkosalaus*

loiskäyttö

en war driving

suojaamattomien langattomien lähiverkkojen paikantaminen ja niiden luvaton käyttö esimerkiksi ajoneuvolla liikkuen

▲ *hyökkäys, käyttö (1)* ▶ *luvaton käyttäjä, modeemihyökkäys, salakäyttö*

loisohjelma

en parasite; parasitic virus

haittaohjelma, yleensä virus, joka toimiessaan lähinnä kuluttaa tietokoneen kapasiteettia, mutta saattaa tehdä muutakin vahinkoa

▲ *haittaohjelma ♣, ohjelma, virus ♣* ▶ *bakteeri, tiedostovirus*

loki

en log (s)

tiedosto, johon tehdään aikajärjestyksessä merkinnät tapahtumista ja niiden aiheuttajista

Loki kerätään yleensä automaattisesti ja samaan järjestelmään liittyviä lokeja voi olla useita, esimerkiksi vikaloki, laskutusloki.

▶ *asiakirja, käyttö (2), merkintä, seurain, turvallisuushäiriö* ▼ *näppäinloki*

loukkaus

▼ *oikeudenloukkaus, tietoturvaloukkaus, viestintäsalaisuuden loukkaus, yksityisyyden loukkaus*

luokitella

en classify

erottaa (esimerkiksi tietoja) ryhmiä jollakin perusteella

Tietojen luokittelamisen perusteena voi olla esimerkiksi niiden suojaustarve, omistajuus tai tosiaikaisuusvaatimus.

▼ *luokitus, turvaluokitus*

luokitus

en classification; taxonomy

luokkiin jakamisen kriteeristö tai tulos, jolla on toiminnallista tai oikeudellista merkitystä

▲ *luokitella* ▼ *tietojen luokitus, turvaluokitus, tärkeysluku*

luotaus

en probe (s)

tietojen hankkiminen verkkoasemasta tai sen käyttäjistä vahingonteon valmistelemiseksi

▶ *salakuuntelu, skannaus, tiedustelu, tiedustelupaketti, tietomurto* ▼ *haavoittuvuusskannaus, porttiskannaus*

luotettavuus

en reliability

todennäköisyys, että tietojen tai tietojenkäsittelyprosessin eheys on säilynyt, tai että laite, järjestelmä tai palvelu on käytettävissä normaalisti tietyn ajan

▲ *ominaisuus* ▶ *ajantasaisuus, eheys, käytettävyys (1), oikeellisuus, saavutettavuus, sitkeys, tarkastettavuus, todennettavuus, toipuminen, turvallisuus* ▼ *häiriö, kaatua, luotettu taho, sinetti, varajärjestelmä, varmistaa*

luotettu taho

en trusted (third) party

taho, usein viranomainen tai tunnettu yritys, jolle uskotaan erityistä luottamusta vaativia tehtäviä, esimerkiksi oikeusistuin, pankki, teleyritys, notaari, valantehnyt kielenkääntäjä

Tietoverkossa luotetun tahon tehtäviä liittyy mm. julkisen avaimen järjestelmän hallintaan tai verkkonotaarina toimimiseen.

▲ *luotettavuus, luottamuksellisuus* ▶ *allekirjoituslaki, julkisen avaimen järjestelmä, tarkastus (2), turvatalletus, varmentaja, viranomainen* ▼ *ai-kaleimapalvelu, akkreditointi, varmenne, verkkonotaari*

luottamuksellinen

en confidential

vain tietyn henkilön tai tiettyjen henkilöiden tietoon tarkoitettu

Valtionhallinnon turvaluokituksen mukaan luottamuksellinen vastaa III turvaluokkaan kuuluvaa tietoa.

▶ *arkaluonteinen tieto, julkinen, salainen, turvaluokitus, viranomaisen asiakirja, viranomaiskäyttö* ▼ *luottamuksellisuus, paljastus*

luottamuksellisuus

en confidentiality

1) tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta

2) se, missä määrin luottamuksellisuutta pidetään tärkeänä

▲ *laatu, luottamuksellinen* ▶ *eheys, tietoturvalisuus ♣, yksityisyys, yrityssalaisuus* ▼ *luotettu taho, salassapitorikkomus*

luvaton

en illegal; unauthorized

säännösten tai sääntöjen vastainen

Esim. lain, yleisen käytännön, tietoturvasuutta koskevan ohjeen tai sopimuksen vastainen.

▲ *sääntö* ▼ *laiton kopio*

luvaton käyttäjä

en unauthorized user

käyttäjä, jolla ei ole käyttövaltuuksia

▲ *käyttäjä, käyttövaltuudet* ▶ *kuoria, loiskäyttö, nimenvaltaus, paljastus, salakäyttö, tunkeutuminen, valtuutettu käyttäjä*

lähiverkko

en local area network

lyhyillä etäisyyksillä, usein yhden organisaation tai rakennuksen sisällä käytettävä nopea tietoverkko tai dataverkko

▲ *suljettu verkko, tietoverkko ♣, verkko ♣* ▶ *etätö, etäyhteys* ▼ *verkonhallintaohjelmisto*

läpialaus

en end-to-end encryption

salakirjoitettujen viestien toimittaminen lähettäjältä vastaanottajalle saakka ilman, että viestit välillä avataan ja salakirjoitetaan uudelleen

▲ *salaus* ▶ *turvakäytäntö*

M**maatunnus**

en country code; country domain name

Internet-osoitteessa valtiota tai muuta maantieteellistä aluetta tarkoittava ylätasoinen verkkotunnus

▲ *tunnus* ▼ *fi-juuri*

MAC (1)

Message Authentication Code

ISO 8731-1 standardin mukaisesti symmetrisellä salauksella tuotettu varmistus

▲ *standardi, symmetrinen salaus ♣, varmistus*

makrovirus

en macro virus

sovellusohjelman käsiteltäväksi tarkoitettuun dataan, esimerkiksi tekstidokumentiin kätkeytyvä sovellusohjelman toimintaa ohjaavia tulkittavia makroja käyttäen kirjoitettu virus

▲ *virus ♣* ▶ *datapohjainen hyökkäys, sähköpositivus, tiedostovirus*

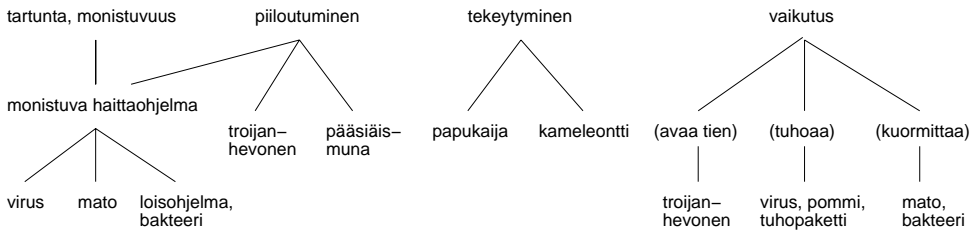
(käyttäjän) manipulointi

en social engineering

tietojen tai niihin liittyvien omaisuusarvojen luvaton hankinta urkkimalla tai harhauttamalla

▶ *identiteettivarkaus, käyttäjä, käyttäjäprofiili, tekeytyminen, yritysvakoilu*

Haitta- ja tuholaisohjelmia jonkin ominaispiirteensä mukaan



mato ♣
en worm

haittaohjelma, joka leviää lähinnä palvelinten välillä itsenäisesti ilman ihmisen toimenpidettä käyttäen hyväksi ohjelman virhettä tai haavoittuvuutta. Vaikka madon ja viruksen käsitteet eivät ole selkeästi erillisiä, eroina pidetään usein mm. seuraavia: 1) virus piiloutuu ohjelmaan tai tekstiin, kun taas mato on erillinen ohjelma 2) virus pyrkii yleensä suoraan haittavaikutukseen kun taas tähän mennessä havaitut madot ovat pyrkineet lähinnä leviämään ja näin kuluttamaan datansiirto- ja palvelinten käsittelykapasiteettia

▲ *haittaohjelma ♣, monistuva ohjelma, tuholaisohjelma ♣* ▶ *bakteeri, tartunta, virus ♣*

menetelmä

▶ *käytäntö* ▼ *haastemenetelmä, julkisen avaimen menetelmä ♣*

merkintä

▶ *loki* ▼ *rekisterimerkintärikos, turvamerkintä*

MITMA

man-in-the-middle attack
välitavetohyökkäys

mittaustiedustelu

en electronic intelligence

vastustajan muista kuin viestijärjestelmistä lähtöisin oleviin sähköisiin signaaleihin kohdistuva tiedustelu

Näitä ovat muun muassa anturi- ja navigointisignaalit.

▲ *signaalitiedustelu ♣, tiedustelu* ▶ *viestitiedustelu*

modeemihyökkäys

en war dialing

modeemia käyttäviin järjestelmiin murtautuminen puhelinnumeroita systemaattisesti kokeillen

▲ *hyökkäys, tietomurto* ▶ *loiskäyttö*

monistuva ohjelma
en replicator

ohjelma, joka tietyissä olosuhteissa monistaa itseään

Kyseessä on yleensä haittaohjelma, esimerkiksi *virus ♣, mato ♣* tai *bakteeri*.

▲ *ohjelma* ▶ *haittaohjelma ♣, toisintaa, tuholaisohjelma ♣*

monitoimikortti

en multi-use smart card

toimikortti, jonka avulla voidaan käyttää useita erilaisia palveluja

Esim. sähköinen henkilökortti, jota voi käyttää myös pankkikorttina ja terveystietokorttina.

▲ *toimikortti, verkkoasiointi, verkkopalvelu*

monitori

sama kuin *seurain*

▶ *etähuolto, tietomurtohälytys, verkonhallintaohjelmisto, virustutka* ▼ *nuuskin, televalvonta, vah-tiajastin*

monivarmenneympäristö

en multiple certificate environment

kaksi tai useampia varmennejärjestelmiä saman käyttäjäkunnan käytettävissä

▲ *varmenne, varmennepalvelu, varmennusorganisaatio*

muistivuoto

en memory leak

ohjelmavirheestä johtuva ilmiö, jossa ohjelma varaa toistuvasti keskusmuistia enemmän kuin vapauttaa sitä ja täyttää vähitellen koko muistin

▲ *virhe (1)* ▶ *bakteeri, eheyttää, ylivuoto*

murtaa

en break (v); breach (v); crack

saada selville salasana tai salausavain tai avata salakirjoitettu tai muuten suojattu tieto laittomasti tai luvatta

▶ *avata (2), murtautua* ▼ *väsytystekniikka*

murtautua

en crack

tunkeutua luvatta suojattuun kohteeseen, esimerkiksi tietojärjestelmään

▲ *aktiivinen hyökkäys* ▶ *murtaa, peesaus, tunkeutuminen* ▼ *murtautuja, tietomurto*

murtautuja

en cracker; cyberhacker

henkilö, joka tunkeutuu luvatta tietoverkkoon tai siinä olevaan tietoa-asemaan tai -järjestelmään mahdollisesti aiheuttaakseen vahinkoa

▲ *murtautua, tunkeutuminen* ▶ *ansa, hakkeri, hyökkääjä, skriptari, valkolakki*

murto-ohjelma

en cracker; cracking program

tuntemattoman salasanan tai salausavaimen löytämiseen tarkoitettu valmisohjelma

Murto-ohjelma perustuu yleensä kaikkien mahdollisten salasanojen tai avainten kokeiluun, mutta väsytystekniikan lisäksi on kehitetty muita menetelmiä, jotka hyödyntävät tietoa käyttäjästä, salakirjoitusmenetelmästä tai salakirjoitettavasta tai salakirjoitetusta viestistä.

▲ *ohjelma, tietomurto* ▶ *haittaohjelma ♣, las-kennallisesti murtovarma, murtopakki, sanakirjahyökkäys, turvaohjelma ♣, väsytystekniikka*

murtopakki

en root kit

ohjelmisto, joka sisältää valmiita välineitä murtautujan käyttöön, muun muassa viestien ja salasanojen sieppaamiseen

▲ *tietomurto* ▶ *murto-ohjelma, nuuskin, tiedustelupaketti, troijanhevonen*

N**NAT**

Network Address Translation

Internet-standardi, joka määrittelee lähiverkon sisäisten IP-osoitteiden antamisen ja niiden muuntamisen ulkoisiksi Internet-verkon osoitteiksi

Osoitteen muunnos toteutetaan yleensä reitittimissä tai palomuurissa.

▲ *IETF-standardi, palomuuuri ♣* ▶ *välipalvelin*

NCSC

National Computer Security Center

USA:n liittovaltionhallinnon tietoturaviranomainen ja NSA:n osasto, joka muun muassa laatii kehittämänsä turvaluokituksen mukaisia tietojärjestelmien turvanormeja

Luokituksen tasoja ovat D, C1, C2, B1, B2 ja A1, joista A1 on tiukin.

▲ *NSA, tietoturvanormi* ▶ *ENISA* ▼ *C-tason turvallisuus, Orange Book*

nimenvaltaus

en cybersquatting

verkkotunnuksen oikeudeton käyttö tai haltuunotto

▲ *kaapata, rikos, tietoverkkorikos, verkkotunnus* ▶ *ICANN, luvaton käyttäjä, verkkotunnuksen kaappaus*

nimimerkki

en anonymous user identity

anonymikäytössä palvelun käyttäjän omaksuma tunnus

▲ *käyttäjätunnus, tunnus* ▶ *anonymikäyttö*

nimipalvelin

en name server

osoitepalvelin nimi-osoite muunnoksia varten, esimerkiksi Internet-verkossa

▲ *palvelin*

NIPC

National Infrastructure Protection Center

Yhdysvaltain valtionhallinnon virasto, jonka tehtävänä on yhteiskunnan perusrakenteisiin kohdistuvien uhkien torjuminen

▶ *CIAO, ENISA, infrastruktuurisodankäynti, ISAC, NISCC, NSA, OCIEPE, poikkeusolot*

NISCC

National Infrastructure Security Coordination Centre

Britannian valtionhallinnon viranomaisen, jonka tehtävänä on yhteiskunnan perusrakenteiden turvaaminen

▲ *tietoturvapoliittika, valmiussuunnittelu*
▶ *CIAO, infrastruktuurisodankäynti, KBM, NIPC, OCIEPE, PTS*

NIST

National Institute for Standards and Technology

Yhdysvaltain standardointiviranomainen

Entiseltä nimeltään NBS, National Bureau of Standards.

▲ *standardointielin* ▶ *SFS*

normi

en norm

yleisesti noudatettava sääntö, esimerkiksi sitova tekninen standardi

▲ sääntö ▶ eettiset ohjeet, laki, standardi, säädökset, viranomainen ▼ tietoturvanormi

notaaripalvelin

en authentication server

verkkonotaarin toimintoja suorittava palvelin

▲ palvelin, turvapalvelin, verkkonotaari ▼ aikaleimapaalvelin

notaaripalvelut

en notary services

verkkonotaarin palvelut, esimerkiksi aikaleimojen antaminen ja tiedostojen säilytys

▲ palvelu, verkkonotaari

notarointi

en notarization

(verkko)notaarina toimiminen esimerkiksi lisäämällä viestiin aikaleima tai säilyttämällä luottamuksellista aineistoa

▲ verkkonotaari ▼ aikaleima

NSA

National Security Agency

Yhdysvaltain liittovaltion virasto, jolla on toimivaltaa kansalliseen turvallisuuteen liittyvissä asioissa, kuten salaustieteessä

▶ CIAO, Echelon, NIPC ▼ NCSC

nuuskia

en sniff

seurata verkon liikennettä tarkoituksena valvoa sitä tai hankkia tietoja verkossa liikkuvista viesteistä ja salasanoista

▲ passiivinen hyökkäys, urkintatekniikka ▶ valvoa ▼ Carnivore, nuuskin

nuuskin

en sniffer; packet sniffer

tietoverkossa ohjemisto, joka lukee verkon liikennettä

▲ monitori, nuuskia, seurain ▶ murtopakki, pakettisuodatin, tiedustelupaketti, verkkoanalysointori

näppäinloki

en key logger

tietokoneeseen salaa asennettu ohjelma, joka tallentaa käyttäjän kaikki näppäimen painallukset niin, että ohjelman asentaja voi ne myöhemmin lukea

▲ loki, siepata, urkintatekniikka ▶ hajasäteily, salakuuntelu

O

OCIPEP

Office of Critical Infrastr. Protection & Emergency Preparedness

Kanadan elintärkeiden perusrakenteiden turvaamisesta huolehtiva viranomainen

▲ tietoturvapoliittikka, valmiussuunnittelu ▶ infrastruktuurisodankäynti, KBM, NIPC, NISCC

ohitusmenettely

en bypass procedure

toimenpiteet toiminnan edelleen jatkamiseksi häiriön tai virheen sattuesssa sitä välittömästi korjaamatta

▲ käytettävyys (1) ▶ toipumismenettely

ohjaus

en control (1)

toiminnan kulun määrääminen annetun tavoitteen mukaisesti, usein palautteen perusteella

▶ hallinta, järjestelmän omistaja, puuttuminen, sääntö, tarkkailu, valvonta ▼ tietohallinto

ohje

▼ eettiset ohjeet, valtionhallinnon tietoturvaohjeisto

ohjelma

▼ haittaohjelma ♣, loisoohjelma, monistuva ohjelma, murto-ohjelma, ohjelmajäte, suodatusohjelma, tuholaisohjelma ♣, turvaohjelma ♣, viruksentorjuntaohjelma

ohjelmajäte

en cruft

tarpeettomiksi käyneet mutta poistamatta jätetyt ohjelman osat

▲ ohjelma ▶ jäännöstieto

ohjelmisto

▼ pääsynvalvontaohjelmisto, suojausohjelmisto, verkonhallintaohjelmisto

ohjelmistoturvallisuus

en software security

käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, eristämisen-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi

▲ tietoturvallisuus ♣, turvallisuus ▶ aineistoturvallisuus, hallinnollinen tietoturvallisuus, laitteistoturvallisuus, tietoliikenneturvallisuus, tietotekniikan turvallisuus

oikeellisuus

en accuracy

virheettömyys, yhtäpitävyys todellisen asiointilan kanssa

▲ *ominaisuus* ▶ *eheys, jakojäännösvarmistus, kelpoisuus, luotettavuus* ▼ *tarkistaa (1), tarkistaa (2), virhe (1)*

oikeudenloukkaus

en infringement; violation of right

henkilöllä tai organisaatiolla lain, yleisen tavan tai sopimuksen mukaan olevaa oikeutta vahingoittava tai heikentävä teko

▲ *loukkaus, oikeus* ▶ *istunnon kaappaus, laki, puuttuminen, tietotekniikkarikos, tietoturvaloukkaus, vahinko* ▼ *tietotekniikkarikos, viestintäsalaisuuden loukkaus, yksityisyyden loukkaus*

oikeus

▶ *vastuunrajausilmoitus* ▼ *kielto-oikeus, käyttö-oikeus, oikeudenloukkaus, tarkastusoikeus, teki-jänoikeus, tieto-oikeus, tietosuoja ♣, tietotekniikkaoikeus, tietoturva-oikeus, yksityisyys, yritysvaikoilu*

oikeusinformatiikkakts. *tietotekniikkaoikeus***oikeutettu henkilö**kts. *valtuutettu käyttäjä***omaverkko**

en intranet

1) ulkopuolisilta suojattu organisaation tietoverkko

2) organisaation sisäinen Internet-käytännöllä toteutettu tietoverkko, jossa voi olla Internetille ominaisia palveluja kuten web tai SMTP-sähköposti

▲ *tietoverkko ♣, verkko ♣* ▶ *Internet, vierasverkko, yksityisverkko*

ominaisuus

en property

▶ *laatu, standardi* ▼ *aitous, ajantasaisuus, eheys, haavoittuvuus, julkinen, jäljitettävyyys, käytettävyyys (1), käyttökelpoisuus, luotettavuus, oikeellisuus, palvelutaso, saavutettavuus, sitkeys, tarkastettavuus, todennettavuus, tunnistettavuus, uusittavuus, vastustuskykyinen, vikasietoinen, yksityisyys, ylläpidettävyyys*

OpenPGP

PGP-menetelmän toteutus Internet-standardina

▲ *IETF-standardi, PGP*

Orange Book

Yhdysvaltain liittovaltion dokumentti, joka esittää TCSEC-tietoturvakriteerit

▲ *NCSC* ▶ *Common Criteria*

organisatorinen tietoturvallisuuskts. *hallinnollinen tietoturvallisuus*

▲ *tietoturvallisuus ♣*

orja

en zombie

verkkoasema, jonka hyökkääjä on valtuutetun käyttäjän tietämättä kaapannut käyttääkseen sitä hyökkäyksiin verkossa

▲ *kaapata* ▶ *hajautettu palvelunestohyökkäys, koukkaus*

osoitteen kaappaus

en address hijacking

IP-osoitteen luvaton muuttaminen tarkoituksena ohittaa palomuri tai saada toiselle osoitettu tietoliikenne itselleen, tai esiintyä tämän osoitteen omistajana

▲ *kaappaus, tietoverkkorikos* ▶ *istunnon kaappaus, tekeytyminen*

P**P3**

Platform for Privacy Preferences

Internet-verkossa määritelty toiminto, jonka avulla käyttäjä voi todeta tietosuojansa koskevien vaatimusten ja palveluntuottajan tietosuojapolitiikan vastaavuuden

▲ *Internet*

PAC

privilege attribute certificate

käyttöoikeuden varmenne

▲ *varmenne*

paikannus

en positioning

sijainnin selvittäminen, esimerkiksi kartan ja kompassin tai matkaviestinverkon tukiasematietojen perusteella

▶ *paikantaminen*

paikannusjärjestelmä

en positioning system

joukko välineitä ja toimintoja, joita käyttäen voi saada selville sijainnin, esimerkiksi GPS

paikantaminen

en continuous positioning

jatkuvasti, määrävällein tai muuten ajantasaisesti tapahtuva paikannus

▶ *paikannus*

paikata

en patch (v)

korjata virhe tai puute tilapäisjärjestelyin

paketti

▼ jäljituspaketti, tiedustelupaketti, tuhopaketti

pakettisuodatin

en packet filter

verkon solmussa ohjelma, joka tutkii solmun kautta kulkevat paketit ja estää annettujen kriteerien mukaisten paketien edelleen lähettämisen

▲ suodatin, verkonhallinta ▶ nuuskin, palomuur☛, roskapostisuodatin, verkkoanalysointilaite, web-suodatin

pakkokeinolaki

en Coercive Measures Act

pakkokeinolain (450/1987) 5a luku (muutettu 646/2003) määrittelee ne ehdot, joilla Suomessa voidaan harjoittaa telekuuntelua, televalvontaa ja teknistä tarkkailua

▲ laki, tietotekniikkaoikeus ▶ telekuuntelu, televalvonta, valvonta

palautevarmistus

kts. kaikuvarmistus

paljastus

en illegal disclosure

luottamuksellisen tiedon joutuminen lain tai sääntöjen vastaisesti ulkopuolisen tietoon

▲ luottamuksellinen ▶ luvaton käyttäjä, tietovuoto, yritysvakoilu

palomuri ☛

en firewall

ylsi tai useampi turvapalvelin, jotka yhdistävät organisaation sisäisen verkon toiseen verkkoon, jossa on käytössä eri tietoturvaliikenne turvallisesti niin, että valtuudetomat käyttäjät eivät pääse ulkopuolelta sisäiseen verkkoon, tai pääsevät vain tiettyihin osoitteisiin, ja että myös sisäisen verkon tietojen kulkeutumista ulkopuolisiin osoitteisiin voidaan rajoittaa

Palomuurissa määrätään, mitkä sisäisen verkon IP-osoitteet voidaan näyttää ulospäin. Se kirjaa lokiin kaiken liikenteen ja usein myös peittää sisäisestä verkosta ulos lähtevän viestin lähettäneen verkkoaseman IP-osoitteen.

▲ turvapalvelin ▶ harmaa vyöhyke, pakettisuodatin, suodatin, VPN-verkko, välipalvelin ▼ NAT

palomuurilohko

en firewall segment

se osa palomuurilla suojatusta verkosta, jonka palveluihin verkon ulkopuolisilla on mahdollisuus päästä

palvelin

en server

verkon tai sen osan työasemien käytettävissä oleva tiettyä tehtävää, kuten tulostusta, tiedon säilyttämistä tai verkkojen välisen yhteyden turvaamista hoitava laite tai ohjelmisto

▲ tietoverkko ☛ ▼ aikaleimapalvelin, anonymipalvelin, nimipalvelin, notaaripalvelin, toisipalvelin, turvapalvelin, välipalvelin, web-palvelin

palvelinvarmenne

en server certificate

palvelimen tunnuksen kytketty varmenne sen takaamiseksi, että asiakas on yhteydessä tarkoittamaansa palveluun eikä mahdollisesti sitä matkivaan palveluun

▲ varmenne

palvelu

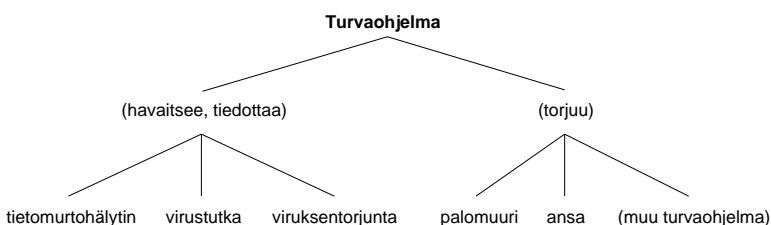
▶ asiointi ▼ aikaleimapalvelu, anonymipalvelu, asiointipalvelu, hakemistopalvelu, huolto (2), notaaripalvelut, tapahtumapalvelu, tiedotuspalvelu, varmennepalvelu, verkkopalvelu, yhteispalvelupiste

palvelujärjestelmä

en front end system

tietojärjestelmä, johon asiakas on yhteydessä saadakseen sähköisen asiainn palvelua

▲ sähköinen asiointi, verkkoasiointi ▼ tapahtumapalvelu



palvelun esto

en denial of service

tietojärjestelmän käytettävyyden heikentäminen tai lakkauttaminen siihen kohdistuneen hyökkäyksen avulla

▲ *esto, käytettävyys (1), tietotekniikkarikos* ► *estää* ▼ *hajautettu palvelunestohyökkäys*

palvelunestohyökkäys

en DoS attack; saturation attack

tietoverkon palveluun tai palvelimeen kohdistuva hyökkäys, jonka tarkoituksena on häiritä sen toimintaa tai lamauttaa se

Estohyökkäys tapahtuu yleensä siten, että palvelimeen lähetetään enemmän viestejä kuin se kykenee käsittelemään.

▲ *aktiivinen hyökkäys, esto, haittaohjelma ♣, hyökkäys* ► *hukuttaminen, häirintä, tietoliikenteen häirintä, tuhopaketti* ▼ *hajautettu palvelunestohyökkäys, sähköpostipommitus*

palvelutaso

en quality of service

1) palvelun laatutaso 2) erityisterminä tietoliikenneyhteydelle asetetut tai sovitut laatuvaatimukset, usein tietyn palveluluokan puitteissa

Vaatimukset voivat koskea muun muassa viivettä, kaistanleveyttä, siirron virhesuhdetta ja palvelun luotettavuutta.

▲ *laatu, ominaisuus* ► *vaatimus*

palveluverkko

en service network; value added network

tietoverkko, joka tarjoaa yleisölle palveluja, kuten viesti-, pankki-, kauppa-, opiskelu-, asiantuntija- tai asiointipalveluja

▲ *verkko ♣* ► *avoin verkko, tietoverkko ♣*

papukaija

en mockingbird

haittaohjelma, joka matkii luvallisen ohjelman toimintoja

▲ *haittaohjelma ♣, tuholaisohjelma ♣* ► *houkutuslintu, tekeytyminen*

passiivinen hyökkäys

en passive attack

hyökkäys, jonka tarkoituksena on vain saada järjestelmän tietoja

▲ *hyökkäys* ► *aktiivinen hyökkäys* ▼ *nuuskaa, salaovi*

peesaus

en piggybacking; tailgating

pääsynvalvonnan kiertäminen toimimalla luvallisen käyttäjän siivellä, esimerkiksi tämän kannoilla ovesta kulkien tai toisen käyttäjän valtuudet kaapamalla

► *murtautua, pääsynvalvonta, tekeytyminen*

peitenimi

en pseudonym

käyttäjätunnus, jota käytetään oikean tai virallisen asemesta lyhyden vuoksi tai henkilöllisyyden peittämiseksi tietoverkossa toimittaessa

▲ *käyttäjätunnus* ► *anonyymitunnus*

pengonta

en scavenging; dumpster diving

tietojen luvaton saanti jäännöstietoja tutkimalla esimerkiksi pois heitetyistä tulosteista

▲ *tiedustelu* ► *jäännöstieto, silppuri, urkintatekniikka*

perkaus

en debugging

järjestelmässä, esimerkiksi ohjelmassa ilmenneiden tai testauksen tuloksena havaittujen järjestelmän toimintaa, käytettävyyttä tai suorituskykyä haittaavien virheiden poistaminen ja korjaaminen

▲ *virhe (2)* ► *testata, testaus*

perusrakenne

en infrastructure

rakentamisen, organisoinnin, kouluttamisen tai lainsäädäntö- tai muun työn tulos, joka on tarkoitettu pitkän ajan kuluessa mahdollistamaan tai helpottamaan taloudellisia tai yhteiskunnallisia toimintoja

► *laki* ▼ *infrastruktuurisodankäynti, tietotekniset perusrakenteet*

perusrekisteri

en national base register

viranomaisen ylläpitämä koko maan kattava hallinnollinen rekisteri

Perusrekisterit ovat väestötietojärjestelmä, kiinteistörekisterit, liikenteen tietojärjestelmä ja yrityrekisterit.

► *viranomainen*

perusturvallisuus

en baseline security

tietoturvallisuuden taso, jossa järjestelmän omistaja on varautunut vastaamaan rutiinomaisiin toimin normaalioloissa sattuviin vahinkoihin ja keskeytyksiin

▲ *tietoturvallisuus ♣, turvallisuus* ► *poikkeusolot, tietoturvasuunnitelma* ▼ *C-tason turvallisuus*

perusvalmius

en basic readiness

turvallisuuden ja varautumisen kannalta toiminnallinen tila, joka tulee saavuttaa ja ylläpitää normaaliaikana

▲ *valmius* ► *tehostettu valmius, täysvalmius*

petos▼ *tietokoneavusteinen petos*

PGP

pretty good privacy

julkisohjelmana saatava julkisen avaimen menetelmä, jota käytetään laajasti sähköpostin salakirjoittamiseen

▲ *julkisen avaimen järjestelmä, vahva salausalgoritmi* ▼ *OpenPGP*

PICS

Platform for Internet Content Selection

tekniikka tietoaiteiston, kuten web-sivustojen valitsemiseksi automaattisesti selaimessa annettuja parametrejä asettamalla

PICS-tekniikkaa käytetään usein verkkosivujen saannin rajoittamiseksi.

▲ *suodatin* ► *roskapostisuodatin, web-suodatin*

piilojäljite

en Web bug; pixel beacon

yhden kuva-alkion kokoinen vastaanottajalle näkymätön verkkojäljite, jollaista usein käytetään urkintatarkoituksiin

▲ *urkintatekniikka, verkkojäljite*

piilokirjoitus ♣

en steganography

salauksen tekniikka, jolla tiedon tai viestin olemassaolo pyritään kätkemään

Perinteisiä piilokirjoituksen menetelmiä ovat mm. näkymättömän musteen käyttö tai tekstisivun pienentäminen i:n pisteeksi. Tietotekniikalla tietoa voidaan piilokirjoittaa esimerkiksi numeeriseen kuva- tai äänitiedostoon.

Piilokirjoituksen tarkoituksena voi olla esimerkiksi tekijänoikeuden osoittaminen tai viruksen levittäminen. Taustakohinaa tai kuvapisteiden väriarvoja muunnetaan niin, että ihminen ei havaitse muutosta, mutta tekninen laite voi sen tehdä.

▲ *salaustekniikka* ► *salakirjoitus ♣* ▼ *piiloleima, salasanoma*

piiloleima

en digital watermark; digital fingerprint

piilokirjoituksen avulla video-, kuva- tai äänitallenteeseen kätkeytyvä tieto, jota käytetään tallenteen valtuudettoman kopioinnin tai valtuudettoman kopion käytön estämiseen

Piiloleima voi olla piilokirjoitettu tai havaittava, salakirjoitettu tai ilmitekstiä.

▲ *leima, piilokirjoitus ♣* ► *laiton kopio*

piilovirus

en stealth virus

virus, joka peittää läsnäolonsa niin, että viruksen-
torjuntaohjelma ei sitä havaitse

▲ *virus ♣* ► *itsekoodaava virus, retrovirus, valevirus*

piiloyhteys

en covert channel

tietojärjestelmässä tai tietoverkossa fyysinen tai looginen yhteys, joka mahdollistaa tiedon siirtämisen tai paljastamisen tietoturvaperiaatteiden vastaisesti

▲ *yhteys* ► *salaovi, tietoturvaperiaatteet*

pimittää

en suppress

estää (tiedon tai ohjelman) käyttäminen tai saaminen käytettäväksi

► *esto, estää, salata*

PIN

personal identification number

1) käyttäjän yksilöimiseksi tai tietojärjestelmän käyttöoikeuden osoittamiseksi käytettävä tunnus, koodi tai salasana

2) henkilötunnus

▲ *tunnus* ► *henkilötunnus, salasana*

PIN-koodi

en PIN code

henkilökohtainen salasana

▲ *koodi*

PING

Packet Internet Groper

tiedustelupakettien lähettämisen ja niihin vastauksen yhteyskäytäntö

► *urkintatekniikka* ▼ *tiedustelupaketti*

ping-komento

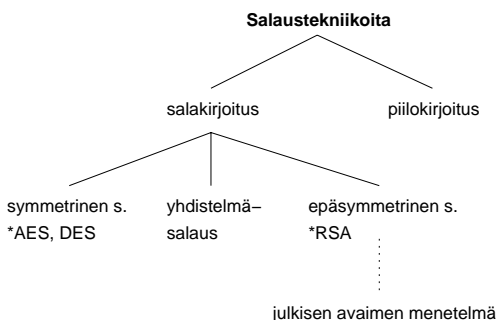
en ping command

käyttöjärjestelmän komento, jolla lähetetään tiedustelupaketti annettuun verkko-osoitteeseen sen selvittämiseksi, onko kohde verkossa

► *tiedustelupaketti*

pipari

kts. eväste



piraattikopio

ks. *laiton kopio*

piratismi

en piracy

aineettoman omaisuuden kuten ohjelman tai tietoineiston luvaton kopiointi ja kopioiden myynti tai muu käyttö hyötymistarkoituksessa

▲ *tekijänoikeus, tietotekniikkarikos*

piristoutuminen

en fragmentation

toistuvien poistojen ja lisäämisten aiheuttama tietojen hajautuminen osiksi, jolloin muistin käyttö on tehotonta

▲ *eheys* ► *eheyttää, turmeltuminen*

PKA

public key architecture

julkisen avaimen järjestelmä

PKCS

Public Key Cryptography Standards

RSA Data Security Inc-yhtiön julkaisemat standardit, jotka määrittelevät, miten julkisen avaimen menetelmiä tulee käyttää luotettavasti, turvallisesti ja yhteensopivasti

▲ *julkisen avaimen menetelmä* ♣, *RSA*

PKI

public key infrastructure

julkisen avaimen järjestelmä

▼ *WPKI*

PKI-varmenne

en PKI certificate

julkisen avaimen järjestelmän mukainen varmenne

▲ *varmenne*

PKIX

Internet-yhteistyöhön kuuluva työryhmä, jonka tehtävänä on kehittää julkisen avaimen järjestelmän alaan kuuluvia standardeja

poikkeusolot

en extraordinary circumstances

kansainvälisestä tilanteesta tai suuronnettomuudesta johtuva vakava vaara Suomen väestön toimeentulolle, talouselämälle, oikeusjärjestykselle, kansalaisten perusoikeuksille, maan alueelliselle koskemattomuudelle tai itsenäisyydelle

Valmiuslain (1080/1991, muut. 198/2000) mukaan mahdollisia poikkeusoloja ovat mm.

- Suomeen kohdistuva aseellinen hyökkäys, sota ja sodan jälkitila

- alueellisen koskemattomuuden vakava loukkaus ja sodanuhka

- vieraiden valtioiden välinen sota, josta on vaaraa Suomelle

- tuonnin vaikeutumisesta aiheutuva vakava taloudellinen uhka

- suuronnettomuus.

▲ *tilanne* ► *erityistilanne, huoltovarmuus, katastrofi, NIPC, perusturvallisuus, poikkeustilanne, Puolustustaloudellinen suunnittelukunta, tehostettu valmius, televiestinnän tietosuojalaki, tärkeyslukuitus, täysvalmius, valmiuslaki* ▼ *valmiussuunnitelma*

poikkeustilanne

en exceptional situation

organisaatiota kohtaava tilanne, joka voi esiintyä myös normaalioloissa, kuten tulipalo, sähkö- tai ilmastointihäiriö, tuhoisa rikos, lakko tai avainhenkilöstön menetys

▲ *tilanne* ► *erityistilanne, katastrofi, poikkeusolot, varautuminen*

poletti

en token

esine, esimerkiksi *toimikortti* tai puhelimen salaussiru, jota yhdessä salasanan kanssa käytetään tunnistamiseen tai todentamiseen

▲ *todennus, toimiavain, turvamoduuli*

politiikka

▼ *salakirjoituspolitiikka, tietosuojapolitiikka, tietoturvapolitiikka, turvallisuuspolitiikka, varmennepolitiikka*

pommi

en bomb

viesti tai tuholaisohjelma, joka aiheuttaa kohteena olevan järjestelmän kaatumisen

▲ *haittaohjelma* ♣, *tuholaisohjelma* ♣ ► *kaatua, tuhopaketti* ▼ *aikapommi, ehdollinen pommi, kirjepommi, sähköpostipommitus, Windows-pommi*

porttipyyhkäisy

en port scan

sama kuin *porttiskannaus*

► *tunnustella*

porttiskannaus

en port scan

tietokoneessa avoimena olevien porttien tiedustelu lähettämällä niihin yhteydenavauspyyntöjä ja tutkimalla vastauksia

▲ *luotaus, skannaus, tiedustelu* ► *haavoittuvuusskannaus, porttipyyhkäisy, tunnustella, verkkoskannaus*

postmaster

kts. *järjestelmävastaava*

protokolla

kts. *käytäntö, yhteyskäytäntö*

PTS

Puolustustaloudellinen suunnittelukunta

▶ *CIAO, KBM, NISCC*

puhdistus

en purging

jäännöstitiedon poisto tietovälineestä

▲ *huolto (1)* ▶ *jäännöstieto*

puheentunnistus

en speech recognition

puheen piirteiden avulla tapahtuva sanojen tai jatkuvan puheen automaattinen tunnistaminen ja muuttaminen konekoodiseen muotoon

▲ *tunnistaa (2), tunnistus* ▶ *puhujan tunnistus, äänentunnistus*

puhujan todennus

en speaker verification

henkilöllisyyden todentaminen henkilön puheään perusteella

▲ *todennus* ▶ *puhujan tunnistus*

puhujan tunnistus

en speaker recognition; speaker identification

henkilön tunnistus puheesta äänen ja puhutavan perusteella; sama kuin *äänentunnistus*

▲ *biotunnistus, tunnistaa (2), tunnistus* ▶ *puheentunnistus, puhujan todennus, äänentunnistus*

puolustautuva tietoturvallisuus

en defensive information security

tietoturvapoliittikka, jossa painopiste on tunnettu-
jen uhkien torjunnassa

▲ *tietoturvallisuus ♣, tietoturvapoliittikka* ▶ *ennakoiva tietoturvallisuus*

Puolustustaloudellinen suunnittelukunta

en National Board of Economic Defence

kauppa- ja teollisuusministeriön hallinnonalaan kuuluva pysyvä komitea, joka muun muassa kehittää hallinnon ja elinkeinoelämän tieto- ja viestintäalan varautumista

▲ *varautuminen, viranomainen* ▶ *poikkeusolot, valmiussuunnittelu*

puuttuminen

en interference

toiminnan kulkuun tai tuloksiin valtuudetta vaikuttaminen

▲ *tietotekniikkarikos* ▶ *ohjaus, oikeudenloukkaus, saastuminen* ▼ *tiedon peukalointi*

pääkäyttäjä (1)

en administrator; superuser

1) käyttäjätunnus, jonka haltijalla on laajat oikeudet hallinnoida muiden käyttäjien käyttäjätunnuksia, laiteresursseja ja tiedostoja sekä järjestelmän suojauksia

2) käyttäjä, jolla on pääkäyttäjän (1) vastuu tietyn sovelluksen osalta

▲ *käyttäjä, vastaava* ▶ *valtuutettu käyttäjä*

pääkäyttäjä (2)

en root

Unix-ympäristössä asiantuntija, joka hallinnoi käyttöoikeuksia, asentaa ja päivittää käyttäjien ohjelmia sekä suorittaa joitakin järjestelmätuen tehtäviä

▲ *käyttäjä* ▶ *valtuutettu käyttäjä*

pääsy

en access (s)

tietojenkäsittelyssä mahdollisuus saada tietojärjestelmän tai tiedoston tietoja tai muuttaa niitä

▲ *tietojärjestelmä* ▶ *ei-julkinen tieto, julkinen, käytettävyys (1), tietomurto* ▼ *pääsynvalvonta, saavutettavuus, salaovi, viranomaispääsy*

pääsynvalvonta

en access control

toiminnot ja menettelyt, joiden avulla tietojärjestelmään pääsy tai tiedon saanti sallitaan vain valtuutetuille henkilöille tai sovelluksille

▲ *pääsy, tietoturvallisuus ♣, valvonta* ▶ *käyttöoikeus, peesaus* ▼ *Kerberos, kulunvalvonta, pääsynvalvontaohjelmisto*

pääsynvalvontaohjelmisto

en access control software

ohjelmisto, joka valvoo pääsyä tarkistamalla käyttäjien valtuudet

▲ *käyttäjä, ohjelmisto, pääsynvalvonta*

pääsyvaltuus

en access right

valtuus tietojen saantiin

▲ *valtuus*

päätös

▼ *huoltovarmuuspäätös, kansallinen tietoturvastrategia, valtionhallinnon tietoturvapäätös*

pöytätestaus

en desk checking

tietojärjestelmän tai sen osan, esimerkiksi ohjelman toimivuuden tarkastus jäljittelemällä sen toimintaa tietokonetta käyttämättä

▲ *testaus*

R

r-komento

Unixin etäkomento, jolla kohdekoneetta voidaan käyttää käyttömukavuuden lisäämiseksi ilman salasanaa

Käyttäjän todentaminen tapahtuu kohdekoneessa käyttäjän kotihakemistossa olevan `.rhosts`-tiedoston avulla. `r`-komentoja ovat `rlogin`, `rsh`, `rcp`, `rdist`. Ne voidaan korvata turvallisemmalla SSH-ohjelmalla.

▶ *SSH*

raaka voima-tekniikka

kts. *väsytystekniikka*

RADIUS

Remote Authentication Dial-in User Services palvelintekniikkaa valintayhteyksin käytettäessä yleinen todennuskäytäntö

▲ *todennus* ▶ *LDAP, TACACS+*

RAID

redundant arrays of inexpensive disks
eräs vikasietoinen levyjärjestelmä

rakenteinen virheenhallinta

en structured error handling

ohjelmoinnissa välineet ja niiden käyttö virhetilanteisiin varautumiseksi sekä virheiden esiintuomiseksi ja käsittelemiseksi

▲ *virhe (2)* ▶ *testaus*

Reed-Solomon koodi

itsekorjaava koodi, jolla on useita käyttöaloja, esimerkiksi datansiirrossa, matkaviestinnässä ja datan tallennuksessa tietovälineisiin

▲ *itsekorjaava koodi*

rekisterimerkintärikos

en falsification of register entry

väärän tiedon antaminen rekisteriviranomaiselle tai sen hyväksikäyttö (rikoslain 16 luku 7 §)

▲ *henkilötietolaki, merkintä, rikos*

rekisterinpitäjä

en registrar

henkilö, yhteisö tai säätio, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä sen käytöstä, tai jonka tehtäväksi rekisterinpito on lailla säädetty

▲ *henkilötietolaki, vastaava* ▶ *henkilörekisteri, järjestelmän omistaja*

rekisteriseloste

en personal file description

henkilötietolain edellyttämällä tavalla laadittu ja saatavilla pidettävä määrämuotoinen kuvaus henkilörekisterin sisällöstä, käytöstä ja suojauksesta

▲ *henkilörekisteri, henkilötietolaki, järjestelmäseloste, seloste* ▶ *tietosuojaseloste*

rekisteröity

en register object; data subject

1) kohde, jota rekisterissä oleva tieto koskee

2) henkilö, jota henkilörekisterissä oleva tieto koskee

▲ *henkilörekisteri* ▶ *tarkastusoikeus*

retrovirus

en retrovirus

virus, joka kohdistaa hyökkäyksensä viruksentorjuntaohjelmaan ja -tiedostoihin

▲ *virus* ♣ ▶ *piilovirus*

Rijndael-menetelmä

kts. *AES*

rikkomus

▼ *henkilörekisteririkkomus, salassapitorikkomus*

rikos

▼ *henkilörekisteririkos, kaappaus, nimenvaltaus, rekisterimerkintärikos, tietorikos, tietosuojarikos, tietotekniikkarikos, tietoverkkorikos, viestintärikos*

riski

en risk

1) todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon

2) uhkaan liittyvän vahingon rahallinen arvo tai odotusarvo (=arvo x todennäköisyys)

▶ *altistus, haavoittuvuus, suojaus, turvallisuus, uhka, vaarantaa, vahinko* ▼ *tietoriski, tietoturvariski*

riskianalyysi

en risk analysis

systemaattisin menetelmin tapahtuva uhkien ja riskien arviointi

▲ *analyysi, riskienhallinta, tietoturvatarkastus* ▶ *haavoittuvuustutkimus, uhka-analyysi*

riskienhallinta

en risk management

järjestelmällinen toiminta riskien rajoittamiseksi niini, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa

Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän valinta, päätös riskien poistamisesta, alentamisesta tai pitämisestä omalla vastuulla, sekä riskienhallinnan organisointi.

▲ *hallinta, tietoturvapoliitiikka* ▶ *haavoittuvuus, tietoriski* ▼ *riskianalyysi*

rlogin

etäkäytön mahdollistava Unix-käyttöjärjestelmän palvelu

▲ *etäkäyttö, r-komento*

roolivarmenne

en role certificate

varmenne, joka yhdistää haltijansa tiettyihin käyttöoikeuksiin tai johonkin tehtävään, esimerkiksi viranomaistehtävään

▲ *varmenne* ▶ *henkilövarmenne, toiminto-osoite, viranomaiskortti*

roskaindeksointi

en spamdexing

tietoverkossa tarjotun sivuston varustaminen turhilla ja mahdollisesti harhaanjohtavilla hakusanoilla sivuston näkyvyyden parantamiseksi verkon hakupalveluissa ja halutun hakutuloksen aikaansaamiseksi

roskaposti

en junk mail; spam (s)

ei-haluttu sähköpostiviesti tai verkkofoorumien aihepiiriin sopimaton viesti, erityisesti mainosposti

roskapostiansa

en spam trap

1) sähköpostiosoitteeseen tehty muutos, joka tekee osoitteesta virheellisen niin, että ihmisen oletetaan osaavan korjata virheen mutta roskapostia lähettävän ohjelman ei

Esim. sähköpostiosoite "nimi@osoite" muutetaan muotoon "nimi-ät-osoite"

2) sama kuin *roskapostisuodatin*

▲ *ansa* ▶ *turvaohjelma ♣*

roskapostisuodatin

en spam filter

ohjelma, joka pyrkii havaitsemaan saapuvan roskapostin ja poistaa tai merkitsee epäilyttävät viestit tai ohjaa ne eri kansioon

▲ *suodatin* ▶ *pakettisuodatin, PICS, turvaohjelma ♣, web-suodatin*

RPC

remote procedure call

etäkutsu

RS

Reed-Solomon code

kts. *Reed-Solomon koodi*

RSA

Rivest-Shamir-Adelman algorithm

epäsymmetrinen salausalgoritmi, jossa avaimen pituudella ei ole ylärajaa

RSA on yleinen algoritmi julkisen avaimen menetelmän avainparien muodostamisessa ja käytössä. 2000-luvun alussa usein käytetty avaimenpituus oli 1024 tai 2048 bittiä.

▲ *epäsymmetrinen salaus, vahva salausalgoritmi* ▼ *PKCS*

S

S-HTTP

Secure Hypertext Transfer Protocol

HTTP-käytännön laajennus, joka toteuttaa yksittäisten viestien salauksen, aidoituksen, eheyden ja alkuperän kiistämättömyyden

▲ *turvakäytäntö* ▶ *HTTPS*

S/MIME

Secure MIME

MIME-sähköpostin laajennus, joka sisältää viestin salauksen ja digitaalisen allekirjoituksen

▲ *turvaposti, vahva salausalgoritmi* ▶ *digitaalinen allekirjoitus*

saastua

en be contaminated

tulla käyttökelvottomaksi vieraan aineksen mukaan sekoittumisen johdosta

▶ *eristää, turmeltua*

saastuminen

en contamination

vieraan ja asiattoman tai vahingollisen aineksen sekoittuminen käytettävään tietoon tai ohjelmaan niin, että tämä menettää käyttökelpoisuutensa

▲ *käytettävyys (1)* ▶ *puuttuminen, tartunta, tiedon peukalointi, turmeltuminen, vahinko*

saavutettavuus

en accessibility

kohteen, kuten palvelun, verkkosivuston tai tiedon ominaisuus, että siihen on riittävän esteetön, vaivaton tai nopea pääsy

▲ *ominaisuus, pääsy* ▶ *käytettävyys (1), luotettavuus, verkkoskanuus*

salaava tiedostojärjestelmä

en encrypting file system

tiedostojärjestelmä, joka salakirjoittaa levyille tallennettavat tiedot automaattisesti käyttäen julkisen avaimen menetelmää

salain

en encryptor
 salauksen suorittava laite tai ohjelma
 ▲ *salaus* ▼ *kertasalain*

salainen

en secret (a)
 vain tiettyjen harvojen tietoon tarkoitettu
 Valtionhallinnon turvaluokituksen mukaan II turvaluokkaan kuuluva asiakirja, joka sisältää erityäin arkaluonteista, salassa pidettävää tietoa.
 ▲ *tietojen luokitus, tietoturvallisuus ♣, turvaluokitus* ▶ *arkaluonteinen tieto, ei-julkinen tieto, erityissuojattava tieto, julkinen, luottamuksellinen, salaisuus, turvaluokitettava tieto, viranomaiskäyttö* ▼ *erittäin salainen*

salainen avain

en secret key
 symmetrisessä salauksessa käytettävä, toisilta salassa pidettävä avain
 ▲ *avain, salausavain ♣* ▶ *julkinen avain, symmetrinen salaus ♣, yksityinen avain*

salaisuus

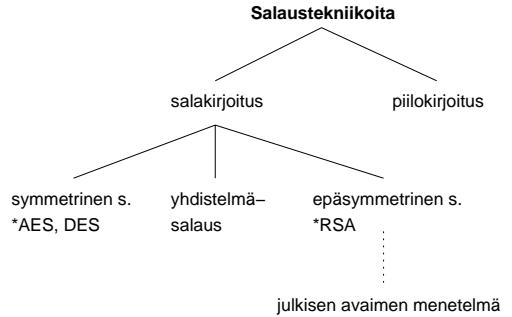
en secret (s)
 salassa pidettävä seikka
 ▶ *salainen, viestintäsalaisuuden loukkaus* ▼ *yrittäsalaisuus*

salakirjoittaa

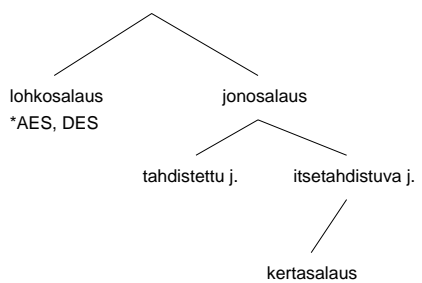
en encrypt
 käyttää menetelmää tiedon esityksen muuttamiseksi sellaiseksi, että tiedon alkuperäinen sisältö on mahdollista saada selville vain samaa tai soveltuvaa käänteistä menetelmää käyttäen
 Salakirjoittaminen tapahtuu salausavainta käyttäen tietyn salausalgoritmin mukaisesti.
 ▲ *suojaus* ▶ *salakirjoitus ♣* ▼ *avata (2)*

salakirjoitus ♣

en cryptography; encryption
 salakirjoittaminen tai sen tulos
 ▶ *piilokirjoitus ♣, salakirjoittaa, salaustekniikka, selväkieliteksti, turvakäytäntö* ▼ *jonosalaus, Kerchoffsin periaate, lohkosalaus, salasanoma, salateksti, salauksen ratkonta, salausalgoritmi, salausavain ♣, salauskuori, salaustuote, salaus-tutkimus*



Symmetrinen salakirjoitus



salakirjoituspolitiikka

en cryptography policy
 valtiossa noudatettavat toimintaperiaatteet salakirjoituksen käytön suhteen
 Salakirjoituspolitiikka voi ottaa kantaa muun muassa seuraaviin kysymyksiin:
 - salausmenetelmän valinnan vapaus
 - vahvan salauksen käytön sallittavuus kotimaisessa ja kansainvälisessä viestinnässä
 - onko varmenteiden antaminen elinkeino- vai viranomaistoimintaa
 - vaaditaanko turvatalletus tai vara-avainjärjestelmä
 - vahinkovastuiden järjestäminen.
 ▲ *politiikka, tietoturwapolitiikka* ▶ *varmennepolitiikka, WPISP* ▼ *salaustuote, turvatalletus, vara-avainjärjestelmä*

salakuuntelu

en eavesdropping; wiretapping
 oikeudeton teknisellä laitteella tapahtuva toisen puhelujen kuuntelu tai viestien lukeminen tai tallentaminen
 Salakuuntelu on rikoslain 24:5 mukainen tieto- ja viestintärikos.
 ▲ *tiedustelu, tietorikos, tietoverkkorikos, urkintatekniikka, viestintärikos* ▶ *luotaus, näppäinloki, siepata, tekninen valvonta, telekuuntelu, televalvonta, tietomurto, ylikuuluminen*

salakäyttö

en derf

toimintaan jätetyn tietokoneen luvaton käyttö

▲ käyttö (1) ► loiskäyttö, luvaton käyttäjä

salalause

en passphrase

yleensä kielen sanoista muodostettu lause, jota käytetään salasanaan

Salalause saattaa olla yli 100 merkin pituinen, jolloin sitä on - sanojen valinnasta ja kielestä riippuen - paljon vaikeampi murtaa kuin tavanomaisista 6-8 merkin salasanaa.

► haastemenetelmä, salasana

salaovi

en trap door

1) ohjelmaan tahallisesti sijoitettu valtuudettoman pääsyn mahdollisuus

2) sama kuin takaportti

▲ passiivinen hyökkäys, pääsy, tietoturva-aukko

► ansoittaa, piiloyhteys, takaportti, tietoturva-aukko, troijanhevonen

salasana

en password

vain käyttäjän tiedossa oleva merkkijono, jonka avulla tietojärjestelmä voi todentaa käyttäjän tunnistuksen

▲ tunnus ► identiteettivarkaus, käyttäjä, PIN, salalause, todennus ▼ dynaaminen salasana

salasanahallinto

en password management

salasanojen käytön ja suojauksen periaatteiden ja menettelyjen määrittely, ylläpito ja valvonta

▲ tietohallinto

salasanatunnistus

en password identification

tunnistus tai todennus salasanan perusteella

▲ todennus, tunnistus ► biotunnistus, haastemenetelmä, sähköinen tunnistus, äänentunnistus

salasanoma

en encrypted message

salakirjoitettu tai piilokirjoitettu sanoma

▲ piilokirjoitus ♣, salakirjoitus ♣

salassa pidettävä tieto

en information in confidence

laissa salassa pidettäväksi säädetty asiakirja tai tieto

Suomessa salassapitoa koskevia säädöksiä on muun muassa julkisuuslain 22 ja 24 §:ssä.

▲ julkisuuslaki, tieto, turvaluokitus ► arkaluontainen tieto, viranomaisen asiakirja ▼ salassapitorikkomus

salassapitorikkomus

en breach of secrecy

aseman tai tehtävän perusteella tietoon saadun salassa pidettävän seikan paljastaminen tai hyväksikäyttö

▲ luottamuksellisuus, rikkomus, salassa pidettävä tieto, tietotekniikkarikos ▼ viestintäsalaisuuden loukkaus

salata

en encrypt

kts. salaus, salakirjoittaa, vrt pimittää

salateksti

en ciphertext; encrypted text

salakirjoitettu teksti

▲ salakirjoitus ♣ ► selväkieliteksti

salauksen ratkonta

en cryptanalysis

toiminta salakirjoituksen avaamiseksi avainta tuntematta, salakirjoitettua tietoa ja mahdollisesti vastaavaa selväkielistä tietoa tutkimalla

Salauksen ratkonta on vaikeampaa, jos myöskään salausmenetelmää ei tiedetä.

▲ analyysi, avata (2), salakirjoitus ♣ ► koodin avaaminen, salaustutkimus ▼ sanakirjahyökkäys, väsytystekniikka

salaus

en encryption

1) tiedon, esimerkiksi toiselle henkilölle lähetettävän viestin käsittely niin, että ulkopuolinen ei saisi haltuunsa tietoa tai viestiä tai sen sisältämää informaatiota

2) salakirjoitus

▼ epäsymmetrinen salaus, heikko salaus, jonosalaus, kevyt salaus, läpisalaus, salain, salausalgoritmi, symmetrinen salaus ♣, vahva salaus, yhdistelmäsalaus

salausalgoritmi

en encryption algorithm

sarja ohjelmoitavia matemaattisia toimituksia, joita käyttäen tieto salakirjoitetaan tai salakirjoitettu tieto avataan

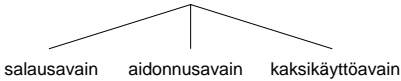
▲ algoritmi, salakirjoitus ♣, salaus ► kaksikäyttötuote, salausavain ♣, salausuoritin ▼ AES, Clipper chip, DES, symmetrinen salausalgoritmi, vahva salausalgoritmi, yksisuuntainen salausalgoritmi

salasavain ♣

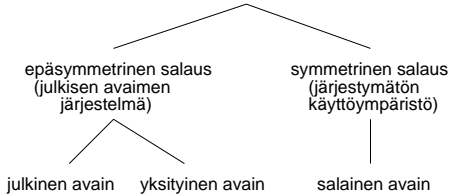
en cryptographic key; encryption key
merkki- tai bittijono, jota tietyn salausalgoritmin mukaisesti käytetään tiedon salakirjoittamiseen, avaamiseen, todentamiseen tai aidontamiseen

▲ *avain, salakirjoitus ♣* ▶ *kaksikäyttöavain, salausalgoritmi* ▼ *avaimen palautus, avaimenhaltija, avaintenhallinta, julkinen avain, kerta-avain, salainen avain, vara-avainjärjestelmä, yksityinen avain*

Avain salakirjoituksessa käytön mukaan



Avain salakirjoituksessa käyttöympäristön mukaan



salasukuori

en digital envelope
salakirjoitusmenettely, jossa viesti salakirjoitetaan symmetrisellä avaimella, joka puolestaan salakirjoitetaan julkisen avaimen menetelmällä

▲ *salakirjoitus ♣, salaustekniikka*

salasuuoritin

en cryptoprocessor
salausalgoritmin toteuttava suoritin

▲ *salaustekniikka* ▶ *salausalgoritmi*

salaustekniikka

en cryptography
tiedon salaamisen ja kätkemisen välineet ja menetelmät ja niiden käytön osaaminen

▲ *tekniikka* ▶ *kaksikäyttötuote, salakirjoitus ♣, salaustutkimus, tietoturvatekniikka* ▼ *elliptinen salaustekniikka, jonosalasaus, lohkosalasaus, piilokirjoitus ♣, salasukuori, salasuuoritin*

salaustuote

en encryption product
ohjelmatuote tai laite, jota käytetään tai joka soveltuu käytettäväksi salakirjoituksen tuottamiseen tai avaamiseen

▲ *salakirjoitus ♣, salakirjoituspolitiikka* ▼ *kaksikäyttötuote*

salaustutkimus

en cryptology
salakirjoituksen menetelmien ja niihin perustuvien tiedon suojauksen menetelmien tutkiminen

▲ *salakirjoitus ♣* ▶ *salauksen ratkonta, salaustekniikka*

sanakirjahyökkäys

en dictionary attack
salasanana hakeminen kokeilemalla vuoron perään sanoja tähän tarkoitukseen laaditusta luettelosta

Sanakirjahyökkäyksen teho perustuu siihen, että salasanaksi usein valitaan luonnollisen kielen sana.

▲ *hyökkäys, salauksen ratkonta* ▶ *murto-ohjelma, väsytyshyökkäys*

sanavapauslaki

en Freedom of Speech Act
laki sananvapauden käyttämisestä joukkoviestinnässä (460/2003) sisältää muun muassa määräyksiä verkkojulkaisuihin ja muihin tietoverkossa yleisön saataville pantuihin aineistoihin liittyvistä vastuista ja oikeudellisista seuraamuksista

▲ *laki* ▶ *julkisuuslaki, tekijänoikeuslaki, verkko-kauppalaki*

SANS

SysAdmin, Audit, Network, Security
tietoturvallisuuden ammattiväen tiedotus-, koulutus- ja tutkimusyhteistyön organisaatio

▶ *CISA, CISSP, ISC2* ▼ *GIAC*

SATU

sähköinen asiointitunnus

▶ *HETU*

sekasumma

en hash total
sama kuin *varmistussumma*

▲ *tiiviste*

seloste

▼ *järjestelmäseloste, rekisteriseloste, tietosuoja-seloste*

selväkieliteksti

en clear text; plaintext
teksti, jota lukutaitoinen henkilö voi sellaisenaan lukea ja ymmärtää

▶ *salakirjoitus ♣, salateksti*

sertifikaatti

kts. *turvallisuustodistus, varmenne*

sertifioida

en certify

1) tehdä arviointi ja antaa sen tuloksista lausunto tai todistus, esimerkiksi *akkreditointi* tai *turvallisuustodistus*

2) antaa *varmenne*

▲ *arviointi*

sertifiointi

kts. *sertifioida, akkreditointi, varmentaminen, turvallisuustodistus*

SET

Secure Electronic Transactions

VISA:n ja Mastercardin kehittämä julkisen avaimen menetelmää käyttävä varmennus luotto- tai pankkikortilla tietoverkossa maksamista varten

Yksinkertaisempi Verified by Visa varmennus on 2002 alkaen korvaamassa SET'in.

▲ *vahva salausalgoritmi, varmentaminen*

seurain

en monitor (s)

toimintaa seuraava tai valvova laite tai ohjelma

► *etähuolto, loki, monitori, televalvonta, verkohallintaohjelmisto, virustutka* ▼ *ASIM, nuuskin, tietomurtohälytyn, vahtiajastin, verkkoanalysointori, viiteseurain*

SFS

Suomen standardointiviranomainen

▲ *standardointielin, viranomainen* ► *CEN, ETSI, NIST*

SHS

Secure Hash Standard

Yhdysvaltain valtionhallinnossa standardoitu tiivistysfunktio (FIPS 180)

▲ *tiivistysfunktio*

siepata

en intercept

ottaa kopio siirrettävänä olevasta tiedosta tai käynnissä olevasta puhelusta viestijän tietämättä

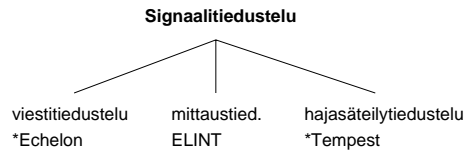
▲ *tietoverkkorikos, urkintateknikka* ► *hajasäteily, kaapata, salakuuntelu, telekuuntelu* ▼ *näppäinloki*

signaalitiedustelu ♣

en signals intelligence

vastustajan sähköisiin viestintä-, navigointi-, mittaus- ja hajasäteilysignaaleihin kohdistuva tiedustelu

▲ *sähköinen sodankäynti, tiedustelu, tietosodankäynti ♣* ► *hajasäteily* ▼ *Echelon, mittaustiedustelu, Tempest, viestitiedustelu*



siivuteknikka

en salami technique

ohjelmoitu menetelmä, jolla tietojenkäsittelyn yhteydessä anastetaan kerrallaan pieniä varallisuuseriä useasta lähteestä

▲ *tietokoneavusteinen petos*

silppuri

en shredder

laite, joka leikkaa siihen syötetyt paperit pieniksi palasiksi tai ohuiksi siivuiksi niin, että alkuperäisen sivun niistä uudelleen rakentaminen on erittäin työlästä

▲ *jäännöstieto* ► *pengonta*

sinetti

en seal (s)

tietoon kiinteästi yhdistetty lisä, esimerkiksi tiedosta muodostettu varmistus, jonka avulla vastaanottaja voi varmistua tiedon lähettäjistä ja aitoudesta

▲ *luotettavuus* ► *digitaalinen allekirjoitus, varmistus* ▼ *sinetöidä*

sinetöidä

en seal (v)

varustaa sinetillä tai digitaalisella allekirjoituksella

▲ *sinetti* ► *varmistaa*

sirukortti

kts. *toimikortti*

sisäinen uhka

en insider threat

organisaation oman henkilöstön toiminnasta aiheutuva uhka

▲ *uhka* ► *ulkoinen uhka*

sisäänkirjaus

en log-in; login; sign-on

järjestelmän hyväksymä käyttäjän ilmoittautuminen tietojärjestelmään sen käytön aloittamiseksi

▶ *todennus, tunnistus* ▼ *esittäytyminen, kertakirjaus, SSO*

sitkeys

en robustness

(järjestelmän) kestävyys vikoja, virheitä ja systeemimurtoja vastaan

▲ *ominaisuus* ▶ *haavoittuvuus, käytettävyyys (1), luotettavuus, vastustuskykyinen, verkkolinnake, vikasietoinen*

skannaus

en scan (s); scanning

1) (optinen) lukeminen

2) tietoverkossa tehty automaattinen tiedustelu, jonka tarkoituksena on hankkia tietoa verkon työasemista, palveluista tai palvelimista

▲ *tiedustelu* ▶ *luotaus* ▼ *haavoittuvuusskannaus, porttiskannaus, tiedustelupaketti, verkkoskannaus*

skriptari

en script kiddie

aloitteleva, usein nuori hakkeri, joka käyttää verkossa tarjolla olevia valmiita haittaohjelmia

▶ *hakkeri, murtautuja*

SMART

Self-Monitoring, Analysis and Reporting Technology

käyttöjärjestelmän ja kiintolevyn välinen rajapinta, joka seuraa levyn toimintaa ja varoittaa mahdolliseen vikaan tai virheeseen viittaavista oireista

▲ *ennakoiva tietoturvallisuus*

sniffata

kts. *nuuskia*

SNMP

Simple Network Management Protocol

TCP/IP-käytäntö verkonhallintatietojen siirtämiseksi hallintaohjelman ja verkon osien välillä

SNMP:n versio 2 sisältää useita tietoturvaominaisuuksia.

▲ *TCP/IP, verkonhallinta*

sodankäynti

▼ *elektroninen sodankäynti, infrastruktuurisodankäynti, johtamissodankäynti, sähköinen sodankäynti, tietojärjestelmäsodankäynti, tietosodankäynti ♣, verkkosodankäynti ♣*

sormenjälki

kts. *piiloleima*

sovelma

en applet

yleensä Java-kielinen sovellus tai ohjelma, joka suoritetaan web-selaimen käynnistämänä tulkiten

▶ *web-selain*

spammi

kts. *roskaposti*

spoofing

kts. *tekeytyminen*

spämmi

kts. *roskaposti*

SSH

Secure Shell

Suomessa kehitetty suojattu yhteyskäytäntö

SSH perustuu viestin salaamiseen satunnaisella symmetrisellä kerta-avaimella, joka lähetetään vastaanottajalle tämän julkisella avaimella salattuna. Vastaanotettaessa avataan ensin avain, siten viesti.

▲ *kerta-avain, vahva salausalgoritmi, yhteyskäytäntö* ▶ *r-komento*

SSL

Secure Sockets Layer

Netscape-yhtiön kehittämä yhteyskäytäntö, jossa salaista avainta käyttämällä luodaan turvallinen datayhteys IP-verkossa

SSL-käytäntöä vaativan web-sivun tunnus alkaa "https:".

▲ *turvakäytäntö, vahva salausalgoritmi, yhteyskäytäntö* ▶ *TLS* ▼ *FTPS, HTTPS, SSMTP*

SSMTP

Secure SMTP

SMTP- ja SSL-käytännöt yhdistämällä toteutettu suojattu sähköpostin yhteyskäytäntö

▲ *SSL, yhteyskäytäntö*

SSO

single sign-on

kertakirjaus

▲ *sisäänkirjaus*

standardi

en standard

valtuutetun tahon tietyllä alalla käytettäväksi hyväksymä tai alalla laajasti omaksuttu tuotetta tai toimintaa koskeva malli, mitta, ominaisuus tai nimitys

▶ *normi, ominaisuus, sääntö* ▼ *IETF-standardi, MAC (1), tietoturvastandardi*

standardointielin

▼ *CEN, CENELEC, ETSI, EWOS, ISO/IEC JTC 1, NIST, SFS*

steganografia

kts. *piilokirjoitus ♣*

suljettu verkko

en closed network

samaan organisaatioon kuuluville käyttäjille tarkoitettu tietoverkko, johon ulkopuolisten pääsy on estetty tai rajoitettu

▲ *verkko ♣* ▶ *avoin verkko, VPN-verkko, yksityisverkko* ▼ *lähiverkko*

sulkulista

en revocation list

1) järjestelmästä poistettujen käyttäjien luettelo
2) julkisen avaimen järjestelmässä käytöstä poistettujen varmenteiden luettelo

▲ *hakemistopalvelu, julkisen avaimen järjestelmä, varmenne* ▶ *kieltolista*

suodatin

en filter

1) ehto tai joukko ehtoja käsiteltävän tiedon rajaamiseksi

2) laite, ohjelma tai niiden yhdistelmä, joka seuraa liikennettä ja poistaa ei-halutut tiedot, esimerkiksi signaalin jotkin komponentit tai annetut kriteerit täyttävät datapaketit

▲ *suojaus* ▶ *palomuri ♣, turvaohjelma ♣* ▼ *pakettisuodatin, PICS, roskapostisuodatin, suodatusohjelma, web-suodatin*

suodatus

en filtering

saapuvan tietoliikenteen systemaattinen tarkkailu ja ei-toivottujen osuuksien poistaminen

▲ *tietoturvallisuus ♣* ▶ *tarkkailu, valvonta*

suodatusohjelma

en censorware

ohjelma, joka estää annetut kriteerit täyttävien sivujen haun selaimeen

▲ *ohjelma, suodatin*

suoja-arkisto

kts. *turva-arkisto*

suojaaminen

kts. *suojaus, tietosuoja ♣, tietoturvallisuus ♣, turvallisuus, valvonta*

suojakopio

kts. *turvakopio*

suojaus

en protection

haitallisen ulkopuolisen vaikutuksen torjuminen tai ennalta ehkäisy

▶ *häirintä, käytettävyyys (1), riski, tietoturva-aukko, turvallisuus* ▼ *eristää, erityissuojattava tieto, salakirjoittaa, suodatin, turvaprotiili*

suojausohjelmisto

en data protection software

tietojen suojaukseen tarkoitettu ohjelmisto, kuten käyttövaltuutuksien hallintaohjelmisto tai salausohjelmisto

▲ *ohjelmisto, tietosuoja ♣* ▶ *turva-arkkitehtuuri, turvaohjelma ♣*

suoritinkortti

kts. *toimikortti*

suunnitelma

▼ *jatkuvuussuunnitelma, tietoturvasuunnitelma, toipumissuunnitelma, valmiussuunnitelma, varautumissuunnitelma*

suunnittelu

▼ *tietoturvasuunnittelu, toipumissuunnittelu, valmiussuunnittelu, varautuminen*

suurenergialaser

en high energy laser

aseena käytettävä laserlähetin, joka voi keskittää useiden megawattien tehon kohteeseensa ja näin tehdä käyttökelvottomiksi esimerkiksi tietokoneita ja sähköisiä tallenteita

▲ *sähköinen sodankäynti* ▶ *suuritehoinen mikroaaltoase, sähkömagneettinen pulssi*

suuritehoinen mikroaaltoase

en high power microwave weapon

asevaikutuksen omaava lähetin, joka emittoi mikroaaltoäteilyä hyvin suurella teholla taajuusalueella 1-30 Ghz

Säteily voi häiritä tai tuhota tietokoneiden mikropiirejä.

▲ *sähköinen sodankäynti* ▶ *suurenergialaser, sähkömagneettinen pulssi*

syklinen ylimäärävarmistus

en cyclic redundancy checking

tiedon varmistuksen matemaattinen menetelmä, jolla saavutetaan korkea virheiden paljastus- ja korjaussuhde erityisesti virheryöppyjen osalta

▲ *ylimäärävarmistus* ▶ *virheryöppy*

symmetrinen lohkosalaus

en symmetric block cipher

salakirjoitus, jossa käytetään lohkosalausta ja yhtä avainta

Symmetrisiä lohkosalaimia käytetään erityisesti pakettivälitteisessä tietoliikenteessä. Niitä ovat mm. DES, AES, Blowfish, IDEA, RC5 ja Twofish.

▲ lohkosalaus ▼ 3DES, AES, Blowfish

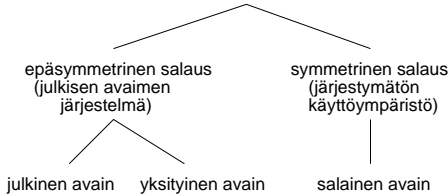
symmetrinen salaus ♣

en symmetric encryption

salakirjoitus, jossa viestin salaus ja avaaminen tehdään samalla avaimella, jonka on näin ollen oltava sekä lähettäjän että vastaanottajan tiedossa mutta muulta salassa

▲ salaus ► epäsymmetrinen salaus, salainen avain, yhdistelmäsalaukset ▼ avaintenvaihtokäytäntö, MAC (1)

Avain salakirjoituksessa käyttöympäristön mukaan



symmetrinen salausalgoritmi

en symmetric encryption algorithm

symmetriseen salaukirjoitukseen käytettävä algoritmi

▲ salausalgoritmi

systemin kunnossapito

en system maintenance

tietojärjestelmän pitäminen toimintakunnossa sekä virheiden korjaaminen

▲ ylläpito

systeminmurtaja

kts. murtautuja

sähköinen allekirjoitus

en electronic signature

1) digitaalinen allekirjoitus

2) muu tietokoneen luettavassa muodossa oleva henkilön nimikirjoituksen vastine osoituksena nimikirjoitukseen liittyvän asiakirjan tai viestin yhteydestä tähän henkilöön

Suomessa sovellettavat säädökset ovat laissa sähköisistä allekirjoituksista (14/2003).

▲ allekirjoitus ► allekirjoituslaki, digitaalinen allekirjoitus, henkilövarmenne, laatuvarmenne, sähköinen asiakirja, varmentaminen

sähköinen asiakirja

en electronic document

tietoteknisellä tallenteena lähetettävä ja käytettävä asiakirja

▲ asiakirja ► sähköinen allekirjoitus

sähköinen asiointi

en online service

sama kuin verkkoasiointi, joskin sähköiseen asiointiin sisällytetään joskus myös puhelimella tai faksilla tapahtuva asiointi

▲ asiointi ▼ asiointipalvelu, hallinnon sähköinen asiointi, palvelujärjestelmä, tapahtumapalvelu, tiedotuspalvelu, vaativa sähköinen asiointi, yhteispalvelupiste

sähköinen asiointitunnus

en electronic client identifier

valtionhallinnon julkisen avaimen järjestelmässä käytettävä asiakasnumero

Sähköisen asiointitunnuksen antaa väestörekisterikeskus, joka merkitsee sen myös väestötietoihin. Luonnollisen henkilön tunnus ei voi olla sama kuin henkilötunnus, juridisen henkilön sähköisenä asiointitunnuksena käytetään organisaation tunnusta, esimerkiksi LY-tunnusta tai kunnanumeroa.

▲ asiointi, hallinnon sähköinen asiointi, tunnus

sähköinen henkilökortti

en electronic identity card

tietyllä fyysiselle henkilölle kuuluva toimikortti, jota hän voi käyttää virallisena henkilötodistuksena sekä mahdollisesti matkustusasiakirjana tai turvattuun verkkoasiointiin ja verkkokauppaan joko henkilökohtaisesti tai organisaationsa myöntämin valtuuksin

Henkilökorttilain (829/1999) mukaan sähköinen henkilökortti sisältää näkyvästi esitettyjen henkilötietojen, valokuvan ja nimikirjoituksen lisäksi konekoodisen osuuden, johon on tallennettu verkkoasiointiin tarvittava yksityinen avain, tiedot korttiin liittyvän varmenteen antajasta sekä mahdollisesti kortin muihin käyttötarkoituksiin liittyviä tietoja.

▲ hallinnon sähköinen asiointi, henkilökortti, sähköinen tunnistus, toimikortti ► HST, monitoimikortti, varmennettu verkkoasiointi ▼ viranomaiskortti

sähköinen identiteetti

kts. sähköinen tunnistus, sähköinen henkilökortti, sähköinen asiointi

sähköinen sodankäynti

en electronic warfare

1) sama kuin tietosodankäynti
2) sodankäynnissä sähkömagneettisen energian käyttö tuhoamiseen, häirintään, harhauttamiseen ja tiedusteluun

▲ *sodankäynti, tietosodankäynti* ♣ ▶ *johtamis-sodankäynti, täsmäase* ▼ *EP, signaalitiedustelu* ♣, *suurenergialaser, suuritehoinen mikroaaltose, sähkömagneettinen pulssi*

sähköinen tunnistus

en electronic identification

henkilöllisyyden tunnistaminen ja todentaminen tietokoneessa tai tietoverkossa, esimerkiksi käyttäen salasanaa tai julkisen avaimen menetelmää

▲ *tunnistus* ▶ *biotunnistus, julkisen avaimen menetelmä* ♣, *salasanatunnistus, varmenne* ▼ *kevyt tunnistus, sähköinen henkilökortti, vahva tunnustus*

sähkömagneettinen pulssi

en electromagnetic pulse

ilmakehässä tapahtuvan ydinräjähdys aiheuttama erittäin lyhyt sähkömagneettinen aalto, joka vaikutusalueellaan lamauttaa sähkölaitteet ja sähköiset piirit, mutta ei vaikuta magneettisiin tai optisiin välineisiin

EMP-suojaus on jaettu luokkiin 70 dB, 40 dB ja ylijännitesuojattu.

▲ *sähköinen sodankäynti* ▶ *hajasäteily, suurenergialaser, suuritehoinen mikroaaltose*

sähköpostipommitus

en mail bombing

turhien sähköpostiviestien lähettäminen palvelimeen tai työasemaan enemmän kuin se pystyy käsittelemään tarkoituksena saattaa kohdekone toimintakyvyttömäksi

▲ *hukuttaminen, palvelunestohyökkäys, pommi*

sähköpostivirus

en e-mail virus

virus, joka on sijoitettu sähköpostin liitteeksi tai liitteeseen ja käynnistyy, kun liite avataan

Levitäkseen virus usein käyttää hyväkseen isäntäkoneen postijärjestelmän osoitteistoa.

▲ *virus* ♣ ▶ *makrovirus, tiedostovirus, web-virus*

säädökset

kts. *laki, oikeus, tietotekniikkaoikeus*

▶ *eettiset ohjeet, normi* ▼ *tietoturvanormi*

sääntö

en rule

(yleensä kirjallinen) kuvaus siitä, miten tietyssä asiassa tai tilanteessa tulee (tai ei tule) menetellä

▶ *laki, ohjaus, standardi, tietotekniset peruskenteet* ▼ *eettiset ohjeet, luvaton, normi, virhe* (2)

T

TACACS+

Terminal Access Controller Access Control System +

TCP-perustainen Internet-todennuskäytäntö; RFC 1492

▲ *Internet, todennus* ▶ *RADIUS*

tahdistettu jonosalaus

en synchronous stream cipher

lähinnä datansiirron salakirjoituksessa käytetty jonosalauksen menetelmä, jossa siirron kummassakin päässä toimivat tahdistetut satunnaislukukehittimet luovat jatkuvasti vaihtuvat salausavaimet

Menetelmän käyttö edellyttää suurta tarkuutta siirron tahdistuksessa.

▲ *jonosalaus* ▶ *itsetahdistava jonosalaus*

takaisinsoitto

kts. *vastakutsu*

takaovi

sama kuin *takaportti*

takaportti

en back door

1) salausalgoritmiin sisältyvä mahdollisuus viranomaisen avata salakirjoitus avainta tuntematta

2) sama kuin *salaovi*

▶ *ansoittaa, Clipper chip, salaovi*

tapahtumapalvelu

en transaction service

sähköisen asioinnin palvelu, jossa on varauduttu käsittelemään yksittäisen asiakkaan tietoja

▲ *palvelu, palvelujärjestelmä, sähköinen asiointi*

tarkastaa (1)

en check (v); inspect

tutkia, esiintyykö virheitä tai muita epäsäännöllisyyksiä

▲ *eheys, kelpoisuus, virhe* (2) ▶ *tarkistaa* (1), *testata, testaus, varmistaa* ▼ *kirjausketju, tarkastaja, tarkastusoikeus*

tarkastaa (2)

en audit (v)

tutkia kohteen, esimerkiksi toimivan organisaation tai tietojärjestelmän kuvausta ja toimintäsääntöjä sekä tosiasiallista toimintaa ja toiminnan tuloksia sen selvittämiseksi, täyttääkö kohde sille säädetty tai asetetut vaatimukset

▶ *tarkastus (2), vaatimus* ▼ *tarkastettavuus, tarkastus (2)*

tarkastaja

en auditor

tarkastuksen suorittaja, tai se, jolla on tähän pätevyys

▲ *tarkastaa (1), tarkastus (2)* ▼ *atk-tarkastaja, CI-SA, tilintarkastaja*

tarkastettavuus

en auditability

järjestelmään ominaisuus, että se sisältää piirteitä ja toimintoja, jotka tuovat esille järjestelmän toiminnassa esiintyviä virheitä, epäsäännöllisyyksiä ja väärinkäytöksiä

▲ *ominaisuus, tarkastaa (2)* ▶ *jäljitettävyys, luotettavuus, todennettavuus, tunnistettavuus, uusittavuus, varmistus (2)*

tarkastus (1)

en check (s)

kts. *tarkastaa*

▲ *turvallisuus* ▼ *hyväksymistarkastus*

tarkastus (2)

en audit (s)

riippumattoman tahon suorittama kohteen, sen toiminnan ja toiminnan tulosten yleensä määräajoin tapahtuva tutkiminen sen selvittämiseksi, vastaako järjestelmä siihen kohdistuvia vaatimuksia

Vaatimuksia voivat olla esimerkiksi oikeellisuus, säädösten ja sopimusten mukaisuus, taloudellisuus, tuloksellisuus ja sidosrymien odotukset. Tarkastavan tahon riippumattomuus on tarpeen, koska tarkastuksen tulokset voivat vaikuttaa järjestelmän toimijain vastuisiin.

▲ *tarkastaa (2)* ▶ *arviointi, katselmus, luotettu taho, tarkastaa (2), valvonta* ▼ *tarkastaja, tietojenkäsittelyn tarkastus, tietoturvatarkastus*

tarkastusoikeus

en right to inspect

1) rekisteröidyn oikeus salassapitosäännösten estämättä tarkastaa itseään koskevat rekisteritiedot

2) viranomaisen oikeus tehdä tarkastuksia toimivaltansa puitteissa

▲ *oikeus, tarkastaa (1)* ▶ *rekisteröity, viranomaispääsy*

tarkistaa (1)

en revise

muuttaa oikeammaksi tai paremmin muuttuneita olosuhteita vastaavaksi

▲ *oikeellisuus* ▶ *tarkastaa (1), varmistaa, varmistus (1), virhe (2)* ▼ *itsekorjaava koodi, toistin*

tarkistaa (2)

en verify

tutkia, onko asiointila oletetun mukainen

▲ *oikeellisuus* ▼ *todennus*

tarkistusmerkkikts. *varmistusmerkki***tarkistussumma**kts. *varmistussumma***tarkkailu**

en monitoring

jatkuva tai toistuva samaan kohteeseen, esimerkiksi henkilöön tai organisaatioon kohdistuva tiedon hankinta

▶ *ohjaus, suodatus, tiedustelu, valvonta* ▼ *kulunvalvonta, tekninen valvonta*

tartunta

en infection

viruksen aktivoituminen tai monistuminen tietokoneessa tai sijoittuminen niin, että se aktivoituu normaalin käyttötoiminnon, esimerkiksi alkulatauksen yhteydessä

▶ *epidemia, mato ♣, saastuminen, tiedostovirus, virus ♣*

TCP/IP

Transmission Control Protocol/ Internet Protocol Internetin toiminnan perusta: verkkokerroksen (IP) ja kuljetuskerroksen (TCP) yhteyskäytännöt, jotka yhdessä hoitavat sanomien reitityksen ja luotettavan tiedonkulun

▲ *Internet* ▼ *SNMP*

tehostettu valmius

en increased preparedness

joissakin organisaatioissa määritelty välitila perusvalmiuden ja täysvalmiuden välillä

▲ *valmius* ▶ *perusvalmius, poikkeusolot, täysvalmius*

tekeytyminen

en impersonation; masquerading; spoofing

1) tietojärjestelmän harhauttaminen pitämään väärää käyttäjää tai ohjelmaa oikeana

2) verkossa, esimerkiksi palvelimessa olevan ohjelman luvallinen käyttö toisen käyttäjän oikeuksin

▲ *aktiivinen hyökkäys, hyökkäys* ▶ *disinformatio, haittaohjelma ♣, houkutuslintu, istunnon kaappaus, kaapata, (käyttäjän) manipulointi, osoitteen kaappaus, papukaija, peesaus, tietomurto, verkko-osoitteen väärentäminen, välistä-vetohyökkäys*

tekijänoikeus

en copyright

teoksen tekijän lakisääteinen oikeus määrätä teoksen käytöstä ja saada käytöstä korvausta

▲ *oikeus, tieto-oikeus, tietotekniikkaoikeus* ▼ *laiton kopio, piratismi, tekijänoikeuslaki*

tekijänoikeuslaki

en copyright law

tekijänoikeuden määrittelevä laki tai lainsäädäntö Suomen tekijänoikeuslaki (404/1961) suojaa mm. tietokoneohjelman kirjallisenä teoksena.

▲ *laki, tekijänoikeus, tietotekniikkaoikeus* ▶ *sananvapauslaki*

tekniikka

▼ *salaustekniikka, tietosuojatekniikka, tietoturva-tekniikka, urkintatekniikka*

tekninen tietojärjestelmä

en computer system; data processing system

tietojärjestelmän ne osat, joissa tietojen käsittely ja siirto tapahtuu automaattisesti ohjelman ohjaamana

▲ *tieto, tietojärjestelmä* ▶ *tekninen valvonta*

tekninen turvaaminen

en technical assurance

teknisten välineiden avulla tapahtuva turvaaminen

▲ *turvallisuus*

tekninen valvonta

en employee monitoring

työnantajan työntekijään kohdistama teknisin välinein tapahtuva valvonta, esimerkiksi työntekijän sähköpostia tai tietoverkon käyttöä seuraamalla

▲ *tarkkailu, valvonta* ▶ *salakuuntelu, tekninen tietojärjestelmä, telekuuntelu, työelämän tietosuojalaki*

telehallintaverkko

en telecommunications management network

ITU:n suosituksessa M.3010 määriteltyjen televerkon hallintatietojen siirtoon ja käsittelyyn kuuluvat toiminnot

▲ *verkko ♣, verkonhallinta*

telekuuntelu

en (legal) wiretapping; lawful interception

viranomaisen oikeuden päätöksellä suorittama yleisen viestiverkon kautta tiettyyn teleliittymään tai sähköpostiosoitteeseen tulevien tai siitä lähtevien viestien kuuntelu tai tallentaminen

Pakkokeinolain 5a luku sisältää säädökset telekuuntelusta Suomessa.

▲ *urkintatekniikka* ▶ *pakkokeinolaki, salakuuntelu, siepata, tekninen valvonta, televalvonta*

telemarkkinalaki

kts. *viestintämarkkinalaki*

televalvonta

en telemonitoring; remote surveillance

1) tapahtumien tai tilanteiden automaattinen havainta ja tiedon välittäminen niistä televiestintää käyttäen

2) tunnistustietojen hankkiminen tietoverkossa lähetetyistä viesteistä

3) matkaviestimen sijaintitiedon hankkiminen (pakkokeinolain 5a luku 1 §)

▲ *monitori, urkintatekniikka, valvonta* ▶ *etähuolto, pakkokeinolaki, salakuuntelu, seurain, telekuuntelu*

televiestinnän tietosuojalaki

en Act on Privacy in Telecommunications

laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999) sisältää säädöksiä muun muassa televiestinnän luottamuksellisuudesta ja suojauksesta sekä poikkeusoloihin varautumisesta.

▲ *laki, tietosuoja ♣, tietosuojalaki, tietotekniikkaoikeus, tietoturvallisuus ♣, tietoturva-oikeus* ▶ *poikkeusolot, viestintämarkkinalaki*

Tempest

Yhdysvaltain puolustushallinnon hanke ja standardit elektroniikkalaitteiden hajasäteilyn mittaamiseksi ja rajoittamiseksi

Verbinä sana voi myös tarkoittaa näytön hajasäteilyn kaappaamista urkintatarkoituksessa tai kaappaamisen torjumista.

▲ *signaalitiedustelu ♣, tietoturvastandardi* ▶ *hajasäteily*

testata

en test (v)

tutkia (järjestelmän, ohjelman tai menettelyn) toimivuutta, oikeellisuutta tai määrittystenmukaisuutta ja osoittaa korjattavat seikat

▶ *perkaus, tarkastaa (1), virhe (2)* ▼ *testaus*

testaus

en testing

järjestelmän toimivuuden, käytettävyyden, suorituskyvyn, määrittysten mukaisuuden tai muun ominaisuuden selvittämiseksi tehtävä toimenpidesarja

▲ *testata* ▶ *perkaus, rakenteinen virheenhallinta, tarkastaa (1), todennus* ▼ *pöytätestaus*

testiaineisto

en test data

ohjelman testauksessa käytettävät, usein keino-tekoiset syöttötiedot

▲ *aineisto*

TETRA

Terrestrial Trunked Radio

ETSI:n kehittämä turvallisen matkaviestinnän standardi

Suomen turvallisuus- ja pelastusviranomaisten suljettu VIRVE-verkko perustuu TETRA-standardiin.

▲ *ETSI* ▶ *VIRVE*

tiedon peukalointi

en data diddling; data tampering

luvaton puuttuminen syöttötietoihin

▲ *puuttuminen* ▶ *eheys, saastuminen, turmeltu-*
minen

tiedostovirus

en file infector virus

virus, joka tarttuu ohjelmätiedostoon ja leviää ohjelman mukana

▲ *virus ♣* ▶ *loisohjelma, makrovirus, sähköpostivirus, tartunta, web-virus*

tiedotuspalvelu

en information service

sähköisen asiointin palvelu, joka julkaisee tietoja tai antaa tai hakee julkisesti saatavissa olevia tietoja

▲ *palvelu, sähköinen asiointi, verkkopalvelu*
▶ *asiointipalvelu*

tiedustelu

en intelligence (2)

tietojen systemaattinen hankinta valitusta kohteesta

Esim. tietojen hankinta ja rikastus valtion tai muun organisaation tarpeisiin julkisista ja muista lähteistä; tietotekniikassa tietojen automaattinen hankinta tietoverkon ominaisuuksista ja osista.

▲ *tieto* ▶ *luotaus, tarkkailu, urkintatekniikka, yrittäjävakoilu* ▼ *mittaustiedustelu, pengonta, portitiskannaus, salakuuntelu, signaalitiedustelu ♣, skannaus, tiedustelupaketti, viestitiedustelu*

tiedustelupaketti

en ping packet

standardimuotoinen 64 tavun ohjauspaketti, johon saatavasta vastauksesta selviää, onko annetussa Internet-osoitteessa toimiva verkkoasema

▲ *paketti, PING, skannaus, tiedustelu* ▶ *luotaus, murtopaketti, nuuskin, ping-komento, tuhopaketti, tunnustella, turvaohjelma ♣, verkkoskannaus*

tieto

▼ *aineisto, arkaluonteinen tieto, avain, ehyt tieto, ei-julkinen tieto, erityissuojattava tieto, hallinnollinen tietoturvallisuus, henkilötieto ♣, jäännöstieto, salassa pidettävä tieto, tekninen tietojärjestelmä, tiedustelu, tieto-oikeus, tunnus, turvaluokiteltava tieto, valtuustieto*

tieto-oikeus

en information law

tietoon sekä tietojenkäsittelyyn ja viestintään sekä näitä prosesseja käyttäviin toimintoihin liittyvät oikeudelliset kysymykset ja niiden ratkaiseminen Tietoturvallisuuden näkökulmasta tieto-oikeuteen kuuluu mm.:

- yksilön oikeuksien turvaaminen tietoturvariskeiltä

- tietoon kohdistuvien oikeuksien turvaaminen

- tietoon perustuvan taloudellisen toiminnan oikeudellinen perusta

- yhteiskunnan perustoimintojen ja valtakunnan turvallisuuden suojaaminen tietoriskeiltä

- historiatiedon jatkuvuuden turvaaminen.

▲ *oikeus, tieto* ▶ *tietorikos, tietotekniikkaoikeus*
▼ *tekijänoikeus*

tietoaineistojen luokitus

kts. *tietojen luokitus*

tietohallinto

en information management

ohjaustoiminnot, joiden tarkoituksena on kehittää, ylläpitää ja varmistaa organisaation tietojenkäsittelyä, tietovarantoja ja tietojärjestelmien yhteentoimivuutta, tietotekniikan ja tietotekniikkapalvelujen hankintaa ja tarjontaa sekä tietotoimintojen turvallisuutta ja taloudellisuutta

▲ *hallinto, ohjaus* ▶ *tietoturvallisuus ♣, turvallisuusjohtaminen* ▼ *salasanahallinto*

tietojen luokitus

en classification of data

tietojen jakaminen luokkiin tietojen omistajan asettamien perusteiden mukaisesti

Luokitusperusteena voi olla esimerkiksi tiedon luottamuksellisuus tai sen merkitys organisaation toiminnalle.

Valtionhallinnon turvaluokituksen perusteena on tietojen haavoittuvuus asiattomalle käsittelylle ja paljastumiselle sekä tästä yhteiskunnalle tai valtiolle aiheutuva menetys tai haitta.

▲ *aineistoturvallisuus, luokitus, tietoturvallisuus* ♣
▶ *julkinen* ▼ *ei-julkinen tieto, salainen, turvaluokitus, tärkeysluokitus*

tietojen turvaaminen

en information security assurance

tietoturvaluuteen tähtäävä toiminta

▲ *tietoturvallisuus* ♣ ▶ *varmistaa*

tietojen varmistaminen

kts. *varmuuskopiointi, varmistaa*

tietojenkäsittelijä

en (data) processor

1) tietojenkäsittelyn osatehtävää suorittava henkilö

2) toimija työketjussa, jossa on käsin tehtäviä työvaiheita

▶ *käsittelijä*

tietojenkäsittelyn tarkastus

en information audit

organisaation tietovarastojen, tietokantojen, tietovirtojen, tietojen tuotannon ja käytön sekä näistä koituvien hyötyjen ja kustannusten arviointi organisaation ja sen jäsenten ja sidosryhmien tarpeisiin nähden

▲ *tarkastus (2)* ▶ *tietoturvatarkastus* ▼ *CISA*

tietojenkäsittelyoikeus

kts. *tietotekniikkaoikeus, tieto-oikeus*

tietojenkäsittelyrikos

kts. *tietotekniikkarikos*

tietojärjestelmä

en information system

1) ihmisistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi

2) abstrakti systeemi, jonka muodostavat tiedot ja niiden käsittelysäännöt

▶ *atk-tarkastaja* ▼ *hyökkäys, järjestelmäseloste, järjestelmävastaava, käyttäjä, käyttö (1), pääsy, tekninen tietojärjestelmä, varajärjestelmä*

tietojärjestelmäluokitus

kts. *tärkeysluokitus*

tietojärjestelmäsodankäynti

en information systems warfare

tietosodankäynnin toiminnot, jotka kohdistuvat vastustajan tietojärjestelmien ja -verkkojen tuhoamiseen ja vääristämiseen ja omien suojaamiseen

▲ *sodankäynti, tietosodankäynti* ♣ ▶ *verkkosodankäynti* ♣ ▼ *Kerchoffsin periaate*

tietokoneavusteinen petos

en computer-assisted fraud

tietotekniikkaa käyttäen suoritettu petos

Tietokoneavusteisia petoksia ovat mm. tiedon tai ohjelman syöttäminen, muuttaminen, pyyhkiminen, pimittäminen tai muu tietojenkäsittelyyn puuttuminen, joka aiheuttaa toiselle taloudellista vahinkoa, kun tarkoituksena on hankkia laitonta hyötyä itselle tai jollekin muulle.

▲ *petos, tietotekniikkarikos* ▼ *siivutekniikka*

tietokoneavusteinen väärennys

en computer-assisted forgery

tietoon, ohjelmaan tai tietojenkäsittelyyn puuttuminen, jonka tuloksena on asiakirjan väärennös

▲ *tietotekniikkarikos* ▶ *asiakirja*

tietokonerikos

kts. *tietotekniikkarikos*

tietokonevirus

kts. *virus* ♣

tietoliikenneturvallisuus

en telecommunications security

1) tavoitella, jossa tietoturvallisuus on toteutettu tietoliikenteen laitteiden, järjestelmien ja niissä kulkevien tietojen osalta

2) lainsäädäntö, normit ja toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus

Tietoliikenneturvaluuteen tähtääviä keinoja ovat mm. laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaaminen ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.

▲ *tietoturvallisuus* ♣, *turvallisuus, viestintämarkkinalaki* ▶ *laitteistoturvallisuus, ohjelmistoturvallisuus, verkonhallinta, viestintärikos* ▼ *virusvaroitus*

tietoliikenteen häirintä

en interference with telecommunications
 puuttuminen viestintälaitteen toimintaan tai tahallinen häiritsevien viestien lähettäminen
 Rikoslain 38:5 §mukaan rikoksen tekee törkeäksi se, jos sen tekijä on telelaitoksen palveluksessa.

▲ häirintä, tietoverkkorikos, viestintärikos ▶ palvelunestohyökkäys, tietomurto

tietomurtaja

kts. murtautuja

tietomurto

en cracking; data trespass
 valtuudeton tunkeutuminen suojattuun tietojärjestelmään tai tunkeutumattakin järjestelmässä olevan tiedon luvaton jäljentäminen teknisen erikoislaitteen avulla

Tietomurto tai sen yritys on rikoslain 38:8 §mukaan rangaistava teko.

▲ aktiivinen hyökkäys, murtautua, tietotekniikka-rikos, tietoturvaloukkaus ▶ hakkerointi, luotaus, pääsy, salakuuntelu, tekeytyminen, tietoliikenteen häirintä, tietomurtohälytin, tunkeutuminen ▼ modeemihyökkäys, murto-ohjelma, murtopakki, tietoturva-aukko

tietomurtohälytin

en intrusion detection system
 organisaation verkossa oleva ohjelmisto, jonka tehtävänä on havaita tietojärjestelmään tunkeutumiset

▲ seurain, tunkeutuminen, turvaohjelma ♣ ▶ ansa, hälytysviesti, monitori, tietomurto, viruksentorjuntaohjelma, virustutka, virusvaroitus ▼ ASIM

tietorikos

en data crime; data trespass
 lainvastainen valtuudeton puuttuminen tietoon

Suomen rikoslain mukaan kyseessä voi olla joko tietomurto, salassapitorikos tai henkilötietorikos tai -rikkomus.

▲ rikos ▶ tieto-oikeus, tietotekniikka-rikos ▼ identiteettivarkaus, salakuuntelu, yritysvalkaisu

tietoriski

en information risk
 tietoon kohdistuva tai tiedosta aiheutuva riski
 ▲ riski ▶ riskienhallinta, tietoturvallisuus ♣, tietoturvariski ▼ jäännöstieto, tietovuoto

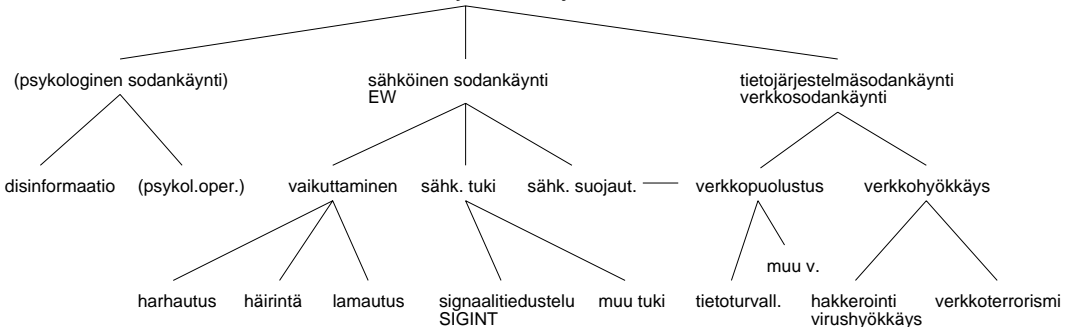
tietosodankäynti ♣

en cyberwarfare; information warfare
 tiedon, tietojärjestelmien ja tietoverkkojen käyttö sekä aseina että kohteina (yleensä valtioiden välisessä) konfliktissa
 Tähän kuuluvat mm. toiseen valtioon tai osapuoleen kohdistuvat toimet, joilla pyritään lamauttamaan tai vahingoittamaan kohteen tieto- ja teleteknistä varustusta, tietojärjestelmiä tai niissä olevia tietoja sekä tietojärjestelmistä riippuvia toimintoja, tai jotka toteutetaan tieto- ja teleteknisiä välineitä käyttäen.

Tietosodankäynnin keinoja ovat mm. tietomurrot elintärkeisiin tietojärjestelmiin, virusten ja muiden tuholaisohjelmien sekä virusvalheiden levittäminen kohteeseen tietoverkkoihin, verkkojen ja palvelimien lamauttaminen hukuttamalla ne turhiin viesteihin, vastustajan viestien sieppaaminen ja avaaminen, sekä tietokonekeskuksiin, datayhteyksiin ja tietovarastoihin kohdistuvat hyökkäykset.

▲ sodankäynti ▶ DII, haavoittuvuus ▼ disinformaatio, häirintä, infrastruktuurisodankäynti, johtamissodankäynti, signaalitiedustelu ♣, sähköinen sodankäynti, tietojärjestelmäsodankäynti, verkkosodankäynti ♣

Tietosodankäynnin muotoja



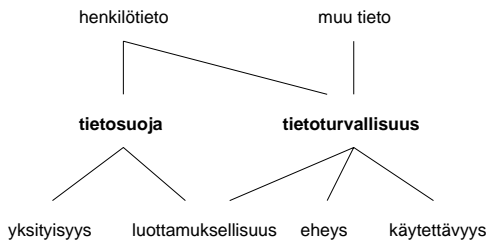
tietosuoja ♣

en privacy protection

tietosuojaan kuuluvat ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä

▲ *henkilötieto ♣, oikeus* ▶ *käyttäjäprofiili, tietoturvallisuus ♣, tietovalkama, yksityisyyden loukkaus* ▼ *henkilötietolaki, suojaohjelmisto, televiestinnän tietosuoja-laki, tietosuojalautakunta, tietosuojarikos, tietosuojatekniikka, tietosuojavaltuutettu, työelämän tietosuoja-laki*

Tietosuoja ja tietoturvallisuus: kohteita ja painopisteitä



tietosuoja-laki

en privacy law

yksityisyyden suoja tietojenkäsittelyssä koskeva laki tai lainsäädäntö

Suomen lainsäädäntö, kts. *henkilötietolaki*.

▲ *laki* ▶ *julkisuuslaki* ▼ *televiestinnän tietosuoja-laki, työelämän tietosuoja-laki*

tietosuojalautakunta

en data protection board; privacy protection board viranomainen, joka käsittelee henkilötietolain soveltamisen periaatteellisia kysymyksiä ja käyttää päätösvaltaa tietyissä tietosuoja-asioissa

▲ *tietosuoja ♣, viranomainen* ▶ *henkilötietolaki, tietosuojavaltuutettu*

tietosuoja-politiikka

en privacy protection policy; data protection policy

tietosuoja-säädökset ja niiden toimeenpanoa koskevat päätökset

▲ *politiikka* ▶ *tietoturvapoliitiikka*

tietosuojarikos

en data protection crime

tietosuoja koskevien säädösten vastainen toiminta, joka on laissa määritelty rikokseksi; kts. *henkilörekisteririkos*

▲ *rikos, tietosuoja ♣, tietotekniikkarikos* ▶ *henkilörekisteririkkomus, henkilörekisteririkos*

tietosuoja-seloste

en privacy statement

henkilötietoja käsittelevän tahon ilmoitus siitä, miten se menettelee haltuunsa saamiensa henkilötietojen kanssa ja mitkä ovat rekisteröidyn oikeudet

▲ *seloste* ▶ *järjestelmäseloste, rekisteriseloste, vastuunrajausilmoitus*

tietosuojatekniikka

en privacy enhancing technology

välineet ja menetelmät, joiden avulla pyritään parantamaan tietosuoja erityisesti avoimessa tietoverkossa

▲ *tekniikka, tietosuoja ♣* ▶ *tietoturvatekniikka*

tietosuojavaltuutettu

en privacy commissioner; data protection ombudsman

viranomainen, jonka tehtävänä on henkilötietojen käsittelyä koskeva ohjaus ja neuvonta sekä käsittelyä koskevien säädösten noudattamisen valvonta

▲ *tietosuoja ♣, viranomainen* ▶ *henkilötietolaki, tietosuojalautakunta, WP 29*

tietotekniikan turvallisuus

en IT security

organisaation tietotekniikkaan kuten tietoliikenteeseen, laitteistoihin, ohjelmistoihin ja niiden käyttöön liittyvä tietoturvallisuus

▲ *tietoturvallisuus ♣, turvallisuus* ▶ *fyysinen turvallisuus, käyttöturvallisuus, ohjelmistoturvallisuus*

tietotekniikan varmistus

en IT backup

organisaation tietotekniikan käytettävyyden ylläpito varautumalla varajärjestelmän tai varakeskuksen käyttöön

▲ *varmistus (1)* ▼ *varajärjestelmä, varakeskus*

tietotekniikan väärinkäyttö

en computer abuse

tietotekniikan tai tietoverkon käyttö haitallisella tai epäeettisellä tavalla, jota ei ole kuitenkaan välttämättä säädetty rikolliseksi

▲ *käyttö (1)* ▶ *eettiset ohjeet, tietotekniikkarikos* ▼ *hyökkäys*

tietotekniikkaoikeus

en computer law

tietotekniikan soveltamisen esiin tuomat oikeudelliset kysymykset ja niiden ratkaiseminen

Viittauksia tässä sanastossa mainittuihin tietotekniikka- ja oikeuteen liittyviin suomalaisiin säädöksiin on koottu hakusanan laki alle.

▲ oikeus ▶ tieto-oikeus, tietotekniikkarikos ▼ al-
lekirjoituslaki, henkilökorttilaki, henkilötietolaki,
julkisuuslaki, järjestelmävastuu, pakkokeinola-
ki, tekijänoikeus, tekijänoikeuslaki, televiestin-
nän tietosuojalaki, tietoturva-oikeus, varmentami-
nen, verkkoasiointilaki, verkkokauppalaki, verk-
korikoslaki, verkkotunnuslaki, viestintämarkkina-
laki

tietotekniikkarikos

en computer crime

rikos, joka kohdistuu tietojärjestelmään tai sen tie-
toihin ja jonka tekeminen edellyttää tietoteknistä
osaamista

Suomessa kriminalisoidut tietotekniikka- ja vies-
tintärikokset on koottu pääasiassa rikoslain 38 lu-
kuun. Rikoslaisissa on lisäksi muitakin tietotekniik-
karikoksiin liittyviä tunnusmerkitöitä.

▲ oikeudenloukkaus, rikos ▶ oikeudenloukkaus,
tietorikos, tietotekniikan väärinkäyttö, tietotekniik-
kaoikeus, tietoverkkorikos, viestintärikos ▼ atk-
sabotaasi, henkilörekisteririkos, hyökkäys, identi-
teettivarkaus, palvelun esto, piratismi, puuttumi-
nen, salassapitorikkomus, tietokoneavusteinen
petos, tietokoneavusteinen väärennys, tietomur-
to, tietosuojarikos, vaarantaa

tietotekniset perusrakenteet

en information infrastructure

yhteisön tai organisaation tietotekniikan käytön
aineelliset ja aineettomat edellytykset, kuten tie-
toverkot ja pääsy niihin, tietopalveluja ja tietosuo-
jaa koskevat säädökset sekä tietotekninen osaa-
minen

▲ perusrakenne ▶ laki, sääntö

Tietoturva ry

tietoturvallisuuden kysymyksiä käsittelevä Tieto-
tekniikan liitto ry:n jäsenjärjestö

tietoturva-arkkitehtuuri

en information security architecture

tietoturvallisuutta toteuttavan järjestelmän raken-
ne ja osien tehtävät ja keskinäiset yhteydet

Esim. ISO-standardi 7498-2 esittää yleisen pe-
riaatteellisen tietoturva-arkkitehtuurin.

▲ tietoturvallisuus ♣ ▶ tietoturvalinjaukset, tieto-
turvapoliittikka

tietoturva-aukko

en security breach; loophole

tietojärjestelmän suojauksessa heikko kohta, jon-
ka kautta ulkopuolisen on mahdollista tunkeutua
järjestelmään

▲ haavoittuvuus, tietomurto, tietoturvatarkastus
▶ salaovi, suojaus, tunkeutuminen ▼ salaovi

tietoturvahyökkäys

ks. hyökkäys

tietoturvakäsikirja

en information security manual

ks. tietoturvaohjeisto

tietoturvalinjaukset

en information security guidelines

organisaation omaksumat toimintaperiaatteet, ta-
voitteet ja menettelyt tietoturvallisuuden ylläpitä-
miseksi ja kehittämiseksi

▲ tietoturvapoliittikka ▶ tietoturva-arkkitehtuuri,
tietoturvasuunnittelu ▼ tietoturvaohjeisto, val-
tionhallinnon tietoturvapäätös

tietoturvallisuus ♣

en information security

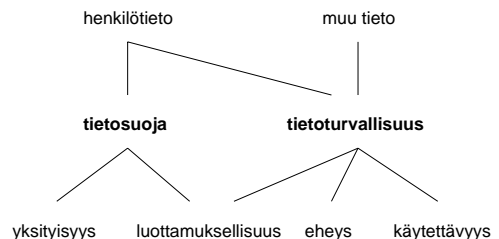
1) tavoitella, jossa tiedot, tietojärjestelmät ja pal-
velut saavat asianmukaista suojaa niin, että nii-
den luottamuksellisuuteen, eheyteen ja käytettä-
vyyteen kohdistuvat uhat eivät aiheuta merkittä-
vää vahinkoa yhteiskunnalle ja sen jäsenille

2) lainsäädäntö ja muut normit sekä toimenpiteet,
joiden avulla pyritään varmistamaan tietoturvalli-
suus (1) niin normaali- kuin poikkeusoloissa

Tietoturvallisuuden toteuttamisessa on tapana
erottaa kahdeksan toimenpidealuetta: hallinnol-
linen, henkilöstö-, fyysinen, tietoliikenne-, lait-
teisto-, ohjelmisto-, tietoaineisto- ja käyttöturvalli-
suus.

▲ turvallisuus ▶ eheys, haavoittuvuus, hy-
vä tietojenkäsittelytapa, käytettävyys (1), luot-
tamuksellisuus, tietohallinto, tietoriski, tietosuo-
ja ♣ ▼ aineistoturvallisuus, ennakoiva tietoturval-
lisuus, fyysinen turvallisuus, hallinnollinen tieto-
turvallisuus, henkilöstöturvallisuus, julkisen avai-
men järjestelmä, järjestelmävastuu, käyttöturval-
lisuus, käyttövaltuuksien hallinta, laitteistoturvalli-
suus, ohjelmistoturvallisuus, organisatorinen tie-
toturvallisuus, perusturvallisuus, puolustautuva
tietoturvallisuus, pääsynvalvonta, salainen, suo-
datus, televiestinnän tietosuojalaki, tietojen luo-
kitus, tietojen turvaaminen, tietoliikenneturvalli-
suus, tietotekniikan turvallisuus, tietoturva-arkki-
tehtuuri, tietoturva-oikeus, tietoturvariski, toimitila-
turvallisuus, tunkeutuminen, turvallisuustodistus,
turvatalletus, vaarantuminen

Tietosuoja ja tietoturvallisuus: kohteita ja painopisteitä



tietoturvaloukkaus

en information security breach

tahallinen tai vahingossa tapahtunut tietoturvallisuuden tai viestintäsalaisuuden rikkoutuminen

▲ *loukkaus* ► *oikeudenloukkaus, turvallisuushäiriö* ▼ *tietomurto, viestintäsalaisuuden loukkaus*

tietoturvanormi

en information security norm

säädös tai viranomaisen määräys, joka tähtää tietojen tai tietojenkäsittelyn luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseen pyrkimällä torjumaan näihin kohdistuvia uhkia tai sääntelemällä tietoturvallisuuden kehittämistoimintaa tai sitä suorittavia organisaatioita

▲ *normi, säädökset* ► *arviointi, tietoturvapoliittika, tietoturvastandardi* ▼ *NCSC, tietoturvaohjeisto, tietoturvatarkastus*

tietoturvaohjeisto

en information security manual

kts. *valtionhallinnon tietoturvaohjeisto*

▲ *tietoturvalinjaukset, tietoturvanormi*

tietoturva-oikeus

en information security law

säädökset ja oikeusperiaatteet, jotka koskevat tietoturvallisuutta

Suomessa tietoturva-oikeutta säätelevät rikoslain 38 luku ja useat erityislait. Tässä sanastossa mainitut tietoturva- tai tietotekniikka-oikeuteen liittyvät säädökset, kts. *laki, päätös*.

▲ *oikeus, tietotekniikka-oikeus, tietoturvallisuus* ♣ ▼ *allekirjoituslaki, henkilökorttilaki, henkilötietolaki, televiestinnän tietosuojalaki, valmiuslaki, verkkokoslaki*

tietoturva-periaatteet

kts. *tietoturvalinjaukset, tietoturvapoliittika*

► *piiloyhteys* ▼ *valtionhallinnon tietoturvaohjeisto*

tietoturvapoliittika

en information security policy

1) valtakunnan tasolla tietoturvanormien ja niiden täytäntöönpanon muodostama kokonaisuus

2) organisaation tasolla johdon hyväksymä näkemys tietoturvallisuuden päämäärästä, periaatteista ja toteutuksesta

Tietoturvapoliittika tai -strategia on kiinteä osa organisaation toiminta- ja tietohallintopoliittikkaa tai -strategiaa.

▲ *politiikka, turvallisuuspolitiikka* ► *BS 7799, ISO 17799, tietosuojapolitiikka, tietoturva-arkkitehtuuri, tietoturvanormi, tietoturvastandardi* ▼ *enakoiva tietoturvallisuus, kansallinen tietoturvastrategia, NISCC, OCIEP, puolustautuva tietoturvallisuus, riskienhallinta, salakirjoituspolitiikka, tietoturvalinjaukset, turvallisuusjohtaminen, valtionhallinnon tietoturvaohjeisto, valtionhallinnon tietoturvapäätös, varmennepolitiikka*

tietoturvapäätös

kts. *valtionhallinnon tietoturvapäätös*

tietoturvariski

en information security risk

tietoon, tietoliikenteeseen tai tietojärjestelmään kohdistuva vahingon vaara

▲ *käytettävyys (1), riski, tietoturvallisuus* ♣ ► *tietoriski, vahinko* ▼ *hajasäteily*

tietoturvastandardi

en information security standard

valtuutetun virallisen tahon vahvistama tai yritysten keskenään sopima standardi, joka koskee tietoturvallisuutta

▲ *standardi* ► *tietoturvanormi, tietoturvapoliittika* ▼ *BS 7799, CEN/ISSS, Common Criteria, IPsec, ISO 17799, ITSEC, Tempest*

tietoturvastrategia

en information security strategy

sama kuin *tietoturvapoliittika*

▼ *kansallinen tietoturvastrategia*

tietoturvasuunnitelma

en information security plan

perusturvallisuuden toteutusta ja ylläpitoa normaalioloissa koskeva suunnitelma

Suunnitelmassa esitetään organisaation tietoturvallisuustoiminnan tavoitteet, hallinto, tehtävät ja menettelyt, osoitetaan elintärkeät tietojärjestelmät ja määritellään niiden toipumisen edellyttämät toimet.

▲ *suunnitelma* ► *jatkuvuussuunnitelma, perusturvallisuus, tietoturvasuunnittelu*

tietoturvasuunnittelu

en information security planning

suunnitteluprosessi, johon kuuluu muun muassa uhka-analyysi, perusturvallisuuden määrittely sekä toipumisvalmiuden ja poikkeusolojen valmiussuunnittelu, ja jonka tuloksena on tietoturvasuunnitelmia, -linjauksia ja -ohjeistoja

▲ *suunnittelu* ► *tietoturvalinjaukset, tietoturvasuunnitelma* ▼ *uhka-analyysi*

tietoturvatarkastus

en information security audit; systems audit
tietojärjestelmän tai organisaation tietojärjestelmien tutkiminen sen selvittämiseksi, täyttävätkö järjestelmät niitä koskevien tietoturvanormien vaatimukset

Tietoturvatarkastus voi kohdistua mm. järjestelmän ja sen toiminnan valvontaan, varmistuksiin ja jatkuvuussuunnitteluun.

▲ tarkastus (2), tietoturvanormi ▶ tietojenkäsittelyn tarkastus ▼ CISA, CISSP, riskianalyysi, tietoturva-aukko

tietoturvatekniikka

en information security technology
laitteet, ohjelmat ja menetelmät, joilla tietojenkäsittelyn ja tietoliikenteen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan ja edistetään
Esim. tekniikat, joilla toteutetaan osapuolten todennus, valtuutus sekä tapahtumatietojen keruu ja tallentaminen.

▲ tekniikka ▶ salaustekniikka, tietosuojatekniikka, urkintatekniikka

tietovalkama

en data haven
valtio tai alue, jossa arkaluonteisten tietojen käsittelyä ja luovutusta ei rajoiteta eikä säädellä

▶ arkaluonteinen tieto, tietosuoja ♣

tietoverkko ♣

en information network
▲ verkko ♣ ▶ dataverkko, palveluverkko ▼ avoin verkko, etäkäyttö, Internet, lähiverkko, omaverkko, palvelin, tietoverkkorikos, verkkoalue, verkkoasema, verkkopalvelu, verkonhallinta, VPN-verkko, yksityisverkko

tietoverkkorikos

en network crime; cybercrime
tietoverkkoon tai sen palveluihin kohdistuva tai niitä hyväksi käytävä rikos

▲ rikos, tietoverkko ♣ ▶ tietotekniikkarikos, viestintärikos ▼ istunnon kaappaus, nimenvaltaus, osoitteen kaappaus, salakuuntelu, siepata, tietoliikenteen häirintä, verkkoterrorismi

tietovuoto

en data seepage; data leakage
tiedon tarkoittamaton siirtyminen suojatun järjestelmän ulkopuolelle

▲ tietoriski ▶ paljastus

tiiviste

en hash value; message digest
tiedosta jonkin säännön mukaan muodostettu lyhyempi uusi tieto tiedon pakkaamiseksi, varmisteen muodostamiseksi tai hajakoodauksessa käytettäväksi

Jos tiiviste muodostetaan tiedon pakkaamiseksi, alkuperäinen tieto on voitava rakentaa uudelleen täydellisenä tai lähes täydellisenä. Jos tiivistettä käytetään varmisteenä, siitä ei tule olla mahdollista saada selville alkuperäistä tietoa, ja todennäköisyyden, että sama tiiviste voidaan muodostaa kahdesta eri alkuperäistiedosta on oltava äärimmäisen pieni. Hajakoodauksessa eri tiedoista tehtyjen tiivistneiden tulee jakautua tasaisesti osoitevaruudessa.

▶ varmisteen ▼ sekasumma, tiivistysfunktio

tiivistysfunktio

en compression function; hash function
funktio tai algoritmi, joka muokkaa kiinteämittaisesta lähtötiedosta kiinteämittaisen, lyhyemmän tiivistein

Jos lähtötieto, esimerkiksi sähköpostiviesti on oletusta pidempi, algoritmi suoritetaan iteroiden tarvittava määrä kertoja.

▲ algoritmi, tiiviste ▼ SHS

tilanne

▼ erityistilanne, poikkeusolot, poikkeustilanne, virhetilanne

tilaturvallisuus

kts. toimitilaturvallisuus

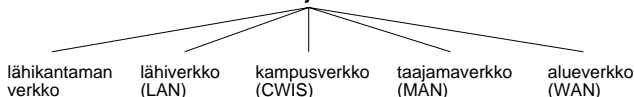
tilintarkastaja

en auditor
erityisesti laskentatoimeen perehtynyt tarkastaja
▲ tarkastaja

tilintarkastus

en audit (s)
kts. tarkastus (2)

Tietoverkko laajuuden mukaan



TLD

top level domain (name)

ylätason verkkoalue tai -tunnus

TLS

Transport Layer Security

SSL-käytännölle perustuva suojattu Internet-yhteyskäytäntö; standardi RFC 2246

- ▲ *IETF-standardi, turvakäytäntö, yhteyskäytäntö*
- ▶ *SSL*

todennettavuus

en verifiability

sellainen kohteen ominaisuus, että olennaiset seikat kohteesta on mahdollista todentaa

- ▲ *laatu, ominaisuus, todentaa* ▶ *kelpoisuus, luotettavuus, tarkastettavuus, tunnistettavuus, uusittavuus*

todennus

en verification; authentication

- 1) varmistuminen kohteen todenmukaisuudestaan, oikeellisuudesta tai alkuperästä
- 2) järjestelmän käyttäjän (henkilön, organisaation tai laitteen) tai viestinnässä toisen osapuolen aitouden varmistaminen

Yleisiä käyttäjän todennuksen menettelyjä ovat:

- käyttäjä tietää ainutkertaisen asian, esimerkiksi salasanan
- hänellä on hallussaan jokin ainutkertainen ominaisuus kuten sormenjälki
- hänellä on hallussaan ainutkertainen väline, esimerkiksi henkilö- tai organisaatiokohtainen henkilökortti.

- ▲ *tarkistaa (2), todentaa* ▶ *esittäytyminen, salasana, sisäänkirjaus, testaus, tunnistus, varmentaminen* ▼ *allekirjoitus, haastemenetelmä, IDAP, Kerberos, poletti, puhujan todennus, RADIUS, salasatatunnistus, TACACS+, vahva todennus, valtuustieto*

todennusavain

en authentication key

salasavain, jota käytetään viestin tai sen lähettäjän aitouden todentamiseen

- ▲ *avain* ▶ *kaksikäyttöavain*

todennustiedot

en authentication data

tiedot, joiden perusteella todennetaan käyttäjän tunnistus

- ▲ *tunnistus* ▶ *haastemenetelmä*

todentaa

en verify; authenticate

varmistua jonkin luotettavuudesta tai aitoudesta, tarkistaa

- ▶ *varmistaa* ▼ *todennettavuus, todennus*

toimentarkastus

kts. *tarkastus (2)*

toimiavain

en smart key

suorittimen ja muistia sisältävä esine, jolla osoitetaan haltijansa valtuus jonkin rajoitetun resurssin käyttöön

Toimiavain voi olla fyysiseltä olemukseltaan esimerkiksi avain, sormus tai kortti.

- ▲ *avain, turvamuodulli, valtuus* ▶ *toimikortti, tonkeli* ▼ *poletti, USB-avain*

toimikortti

en smart card; chip card

suorittimen ja muistia muodostavia mikropiirejä sisältävä luottokortin kokoinen muovikortti, jota käytetään hyvin monenlaisiin tarkoituksiin tietoverkossa ja tietoyhteiskunnassa

Toimikortti toimii vain erityisen lukulaitteen yhteydessä, joka voi olla irrallinen tai kytkettynä esimerkiksi tietokoneeseen, verkkoasemaan tai puhelimeen. Käytettäessä toimikortti on yleensä fyysisessä yhteydessä lukulaitteeseen, mutta se voi myös olla yhteydetön, jolloin se reagoi lähietäisyydeltä lukulaitteen lähettämään signaaliin.

Kortin käyttö vaihtelee siihen ohjelmoitujen toimintojen mukaan. Se voi esimerkiksi ylläpitää tili-saldoa, tallettaa verkkorahaa, toimia pääsynä tietoverkon palveluun tai salakirjoittaa ja avata viestejä.

- ▲ *kortti* ▶ *toimiavain* ▼ *monitoimikortti, sähköinen henkilökortti, valtuuskortti*

toimintahäiriö

en malfunction

ennakoimaton muutos tai keskeytys toiminnassa

- ▲ *häiriö* ▶ *huolto (1), toipuminen*

toiminto-osoite

en functional address

organisaation tai sen tietyn toiminnon sähköpostiosoite, johon lähetettyjä viestejä voi lukea yksi tai useampi tähän valtuutettu henkilö

- ▶ *roolivarmenne, yhteispalvelupiste*

toimitilaturvallisuus

en premises security

toimet tietoteknisten ja muiden toimitilojen turvallisuuden ylläpitämiseksi, kuten kulunvalvonta, tekninen valvonta ja vartiointi sekä palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunta

Valtion toimitilojen turvallisuusluokitus käsittää neljä luokkaa:

- täyssuojaus
- erityissuojaus
- tehostettu perussuojaus
- perussuojaus.

▲ *fyysinen turvallisuus, tietoturvallisuus ♣, turvallisuus ▼ kulunvalvonta*

toipuminen

en recovery

toimintakyvyn palautuminen häiriötilanteen tai seisokin jälkeen

▲ *käytettävyys (1) ► luotettavuus, toimintahäiriö, vara-avainjärjestelmä, virhetilanne*

toipumismenettely

en recovery procedure

toipumisen aikaansaavat toimenpiteet

► *ohitusmenettely*

toipumissuunnitelma

en recovery plan

jatkuvuussuunnitelman tai varautumissuunnitelman osa, joka sisältää ohjeet katastrofista toipumiseen, toiminnan jatkamisesta ja paluusta normaaliin toimintaan, määrittelee tärkeille tietojärjestelmille varajärjestelmävaatimukset, vastuut ja toimet valmiuden luomiseksi sekä antaa ohjeet toiminnasta poikkeustilanteissa

▲ *jatkuvuussuunnitelma, käytettävyys (1), suunnitelma, varautumissuunnitelma ► katastrofi*

toipumissuunnittelu

en recovery planning

toipumissuunnitelman laatiminen ja ylläpito

▲ *suunnittelu*

toisintaa

en mirror (v); replicate

luoda tai ylläpitää tiedoston kopio tai kopioita tai pitää toiminnassa yhtä tai useampaa varalaitteisto palvelukyvyn parantamiseksi tai tietoturvallisuuden varmistamiseksi

► *kahdentaa, monistuva ohjelma, vedostaa*

toisiokanta

en mirror database

tietokanta, joka on toisen tietokannan ajantasainen kopio

▲ *kopio ► toisosivusto, varmistustiedosto*

toisiopalvelin

en mirror server

kuormituksen tasaamiseksi, tietoliikenteen vähentämiseksi tai palvelun nopeuttamiseksi tai varmistamiseksi perustettu toinen palvelin, jolla on samat toiminnot

▲ *palvelin ► toisosivusto, toisiotiedosto*

toisosivusto

en mirror site

sivuston kopio, joka sijaitsee toisessa fyysisessä paikassa

► *toisiokanta, toisiopalvelin*

toisiotiedosto

en mirror file

kts. *toisiokanta*

► *toisiopalvelin*

toistin

en repeater

datansiirrossa laite, joka lähettää vastaanottamansa signaalit eteenpäin ja korjaa siirrossa vääristyneet signaalit alkuperäisiksi

▲ *tarkistaa (1) ► kaikuvarmistus*

tonkeli

en dongle; hardware key

tietokoneen porttiin liitettävä turvamoduuli, jolta suoritettavana oleva ohjelma tarkistaa ohjelman käyttöluvan

▲ *turvamoduuli ► avainpiiri, toimiavain ▼ USB-avain*

torjuntaohjelma

kts. *viruksentorjuntaohjelma, turvaohjelma ♣*

troijalainen

kts. *troijanhevonen*

troijanhevonen

en Trojan horse

viruksen kaltainen haittaohjelma, joka ei kuitenkaan kykene monistamaan itseään, ja sisältää usein salaoven tai muun järjestelmän turvallisuutta heikentävän ominaisuuden

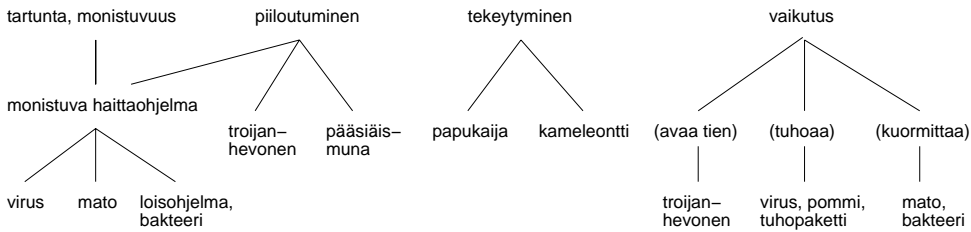
▲ *haittaohjelma ♣, tuholaisohjelma ♣ ► murtopakki, salaovi, virus ♣*

TTP

trusted third party

luotettu taho kuten varmentaja tai verkkonotaari

Haitta- ja tuholaisohjelmia jonkin ominaispiirteensä mukaan



tuholaisohjelma ♣

en malicious program

ohjelma, ohjelman osa tai makro, jonka tarkoituksena on tuhota tai vääristää järjestelmässä olevia tai käsiteltäviä ohjelmia tai tietoja

▲ ohjelma ▶ haittaohjelma ♣, monistuva ohjelma, tuhopaketti, turvaohjelma ♣ ▼ aikapommi, ehdollinen pommi, epidemia, kameleontti, lataus, mato ♣, papukaija, pommi, troijanhevonen, virus ♣

tuhopaketti

en ping of death

väärä tiedustelupaketti, jonka tarkoitus on aiheuttaa vahinkoa verkkoasemissa

▲ paketti ▶ palvelunestohyökkäys, pommi, tiedustelupaketti, tuholaisohjelma ♣, Windows-pommi

tulkita

kts. avata

tunkeutuminen

en intrusion; penetration

onnistunut, yleensä luvaton yritys päästä kohteeseen, esimerkiksi tietojärjestelmään tai tietoverkoon, tai saada sen tietoja

▲ tietoturvaluottelu ♣ ▶ hyökkäys, luvaton käyttäjä, murtautua, tietomurto, tietoturva-aukko ▼ murtautuja, tietomurtohälytint

tunnelointi

en tunneling

1) tekniikka avoimessa verkossa tapahtuvan tietoliikenteen nopeuden, luotettavuuden ja turvallisuuden lisäämiseksi luomalla verkossa datansiirron ajaksi pysyvä ja usein salakirjoittamalla suojattu yhteys, "tunneli", jolloin siirrettävä tieto yleensä salakirjoitetaan

2) puolijohdefysiikan ilmiö

▲ dataverkko

tunnistaa (1)

en identify

erottaa kaikista muista yksiselitteisen nimen tai tunnuksen perusteella

▼ tunniste, tunnistettavuus, tunnistus

tunnistaa (2)

en recognize

havaita samaksi kuin jokin, joka on ennestään tunnettu, tai havaita tietyn joukon jäseneksi

▼ biotunnistus, puheentunnistus, puhujan tunnistus, äänentunnistus

tunniste

en identifier; label

1) tieto, jota käytetään tunnistamaan, nimeämään tai osoittamaan tietoa tai tietojoukkoa

2) tunnistamisen väline, kuten henkilökortti

▲ tunnistaa (1) ▶ allekirjoitus, leima, tunnisteen käyttö, tunnus, tuntoimerkki

tunnisteeton käyttö

en unidentified use

tietoverkon tai sen palvelun käyttö, jossa käyttäjä ei vaadita esittäytymään eikä hänestä kysytä yksilöiviä tietoja

▲ käyttö (1) ▶ anonyymikäyttö, anonyymipalvelin, tunniste

tunnistettavuus

en identifiability

se, että tiettyä yksilöä tai tapahtumaa koskeva tieto voidaan tunnistaa kaikissa käsittelyn vaiheissa

▲ ominaisuus, tunnistaa (1) ▶ tarkastettavuus, todennettavuus

tunnistus

en recognition; identification

menettely, jolla yksilöidään joku tai jokin, esimerkiksi tietojärjestelmän käyttäjä

Tyypillisesti tunnistus tapahtuu tarkistamalla, onko esitetty tunnus tai muu tunniste hyväksyttävien tunnusten joukossa, esimerkiksi käyttäjäksi ilmoittautunut tietojärjestelmän valtuutettujen käyttäjien luettelossa.

▲ *tunnistaa (1), yksilöidä* ▶ *aitous, esittäytyminen, sisäänkirjaus, todennus* ▼ *anonyymikäyttö, biotunnistus, heikko tunnistus, henkilökortti, henkilötunnus, kevyt tunnistus, puheentunnistus, puhujan tunnistus, salasana, salasanatunnistus, sähköinen tunnistus, todennustiedot, tuntomerkki, vahva tunnistus, äänentunnistus*

tunnus

en identifier

jonkin kohteen kuten käyttäjän, ohjelman, dokumentin tai sen osan tai laitteen nimeävä tai yksilöivä tieto

Tunnukselta vaadittavia ominaisuuksia ovat mm. yksiselitteisyys, lajiteltavuus, laajennettavuus, synonyymien estyminen ja lyhyys.

▲ *tieto, yksilöidä* ▶ *allekirjoitus, avain, leima, tunniste* ▼ *anonyymitunnus, FINEID, henkilötunnus, kertatunnus, käyttäjätunnus, maatunnus, nimimerkki, PIN, salasana, sähköinen asiointitunnus, verkkotunnus*

tunnushallintokeskus

en naming authority

palvelu tai viranomainen, joka myöntää tietyn verkkoalueen Internet-verkkotunnukset

Kansainvälinen tunnushallintokeskus on USA:ssa toimiva ICANN, Suomen alueesta vastaa Viestintävirasto FICOM.

▲ *hallinto, Internet, verkkoalue, viranomainen* ▶ *fi-juuri, verkkotunnuslaki* ▼ *IANA, ICANN*

tunnussana

kts. *salasana*

tunnustella

en finger (v)

ottaa yhteys verkoasemaan tietojen hankkimiseksi sen käyttäjistä

▲ *urkintatekniikka* ▶ *porttipyyhkäisy, porttiskanaus, tiedustelupaketti*

tuntomerkki

en characteristic; feature

tunnistuksessa käytettävä piirre, ominaisuus tai osahahmo

▲ *tunnistus* ▶ *biotunnistus, leima, tunniste*

turmeltua

en be corrupted

menettää (datan) eheys tai (ohjelman) käytettävyyttä

▲ *eheys, käytettävyyttä (1)* ▶ *saastua, turmeltuminen*

turmeltuminen

en corruption

tietojen eheyden tai ohjelman käytettävyyden menettäminen

Turmeltumisen voi aiheuttaa esimerkiksi laitevika, ohjelmavirhe, saastuminen, tietojen huolimaton ylläpito tai järjestelmään kohdistunut hyökkäys.

▲ *eheys, käytettävyyttä (1)* ▶ *hyökkäys, levyrikko, pirstoutuminen, saastuminen, tiedon peukalointi, turmeltua, ylläpito*

turva-arkisto

en security archive

varmuusarkisto, joka on sijoitettu toiselle paikkakunnalle tai muuten niin etäälle sen avulla varmistettavasta arkistosta, että molempien tuhoutuminen saman vahingon tai suuronnettomuuden seurauksena on erittäin epätodennäköistä

▲ *arkisto* ▶ *käyttöarkisto, turvakopio, vahinko, varmuusarkisto*

turva-arkkitehtuuri

en security architecture

organisaation tietojärjestelmien systemaattisten turvausmenettelyjen kokonaisuus

▶ *suojausohjelmisto* ▼ *turvallisuusmekanismi*

turvakopio

en safety copy

turvalliseen paikkaan sijoitettu varmuuskopio, joka on käytettävissä, jos alkuperäistä tiedostoa tai varmuuskopiota ei voida käyttää

▲ *kopio* ▶ *turva-arkisto, varmuuskopio*

turvakäytäntö

en security protocol

1) yhteyskäytäntö varmenteen tai käyttövaltuuden voimassaolon tarkistamiseen

2) viestinnän yhteyskäytäntö, jossa käytäntö itsessään huolehtii viestien salauksesta

▲ *käytäntö* ▶ *läpivalvonta, salakirjoitus* ♣, *yhteyskäytäntö* ▼ *avaintenvaihtokäytäntö, HTTPS, S-HTTP, SSL, TLS, WEP*

turvallisuus

en security

olotila, jossa tiedossa olevat uhat eivät merkitse sanottavaa riskiä ja ne voidaan hallita

▶ *luotettavuus, riski, suojaus, uhka* ▼ *aineistoturvallisuus, fyysinen turvallisuus, hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, käyttöturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, perusturvallisuus, tarkastus (1), tekninen turvaaminen, tietoliikenneturvallisuus, tietotekniikan turvallisuus, tietoturvallisuus ♣, toimitilaturvallisuus, turvallisuuspolitiikka*

turvallisuushäiriö

en security incident

tilanne tai tapahtuma, jonka yhteydessä tietoturvallisuus on vaarantunut tai saattanut vaarantua

▲ häiriö ▶ hälytysviesti, loki, tietoturvaloukkaus, vaarantua, valvontakatko

turvallisuusjohtaminen

en security management

vahinkojen ennaltaehkäisyyn tähtäävä toiminnan johtaminen, joka perustuu organisaation turvallisuuspolitiikkaan

Sen osa-alueita ovat mm. tietoturvallisuus, tekninen suojaus, palontorjunta, työsuojelu ja ympäristönsuojelu.

▲ tietoturvapoliitiikka ▶ ennakoiva tietoturvallisuus, tietohallinto

turvallisuuskulttuuri

en security culture

oman, sidosryhmien jäsenten ja ulkopuolistenkin turvallisuuden huomioon ottaminen toiminnassa ja suunnittelussa

▶ turvallisuuspolitiikka, turvallisuustietoisuus

turvallisuusmekanismi

en security mechanism

tietoturvallisuuden ylläpidon periaatteet ja yleiset menetelmät sovellettuina tiettyyn ympäristöön tai käyttöön

▲ turva-arkkitehtuuri

turvallisuuspolitiikka

en security policy

niiden periaatteiden, ratkaisujen ja toimenpiteiden kokonaisuus, joilla vaikutetaan turvallisuuden kehitykseen

▲ politiikka, turvallisuus ▶ turvallisuuskulttuuri, turvallisuustietoisuus ▼ tietoturvapoliitiikka

turvallisuustietoisuus

en security awareness

organisaation henkilöstön tai muun kohdejoukon tiedot ja asenteet, jotka koskevat turvallisuuden tavoitteita ja keinoja

▶ kansallinen tietoturvastrategia, turvallisuuskulttuuri, turvallisuuspolitiikka

turvallisuustodistus

en certificate

kansallisen tai kansainvälisen toimivaltaisen viranomaisen antama tai muu pätevä todistus siitä, että tietotekninen tuote tai palvelu täyttää tiettyä tietoturvallisuuden tasoa vastaavat vaatimukset

▲ tietoturvallisuus ♣ ▶ BS 7799, ISO 17799, vaatimus, varmenne

turvaluokitettava tieto

en classified information

tieto tai asiakirja, joka on lain mukaan salassa pidettävä

Lain viranomaisen toiminnan julkisuudesta 24 pykälän 1 momentin 1.2, 5, 7, 8, 9, 10 tai 11 kohtien mukaan salassa pidettävä asiakirja sisältää yhteiskunnan turvallisuuden tai tiettyjen keskeisten yleisten etujen vuoksi arkaluonteista, salassa pidettävää tietoa. Turvaluokitettava tieto jaetaan kolmeen turvaluokkaan.

▲ aineisto, julkisuuslaki, tieto, turvaluokitus ▶ salainen

turvaluokitus

en security classification

luottamuksellisten asiakirjain ja tietojen jakaminen luokkiin salassapidettävyyden perusteella

Valtionhallinnon turvaluokitus sisältää seuraavat luokat:

I turvaluokka - erittäin salainen: äärimmäisen arkaluonteista, salassa pidettävää tietoa, jota voi käsitellä vain sen vastaanottajaksi merkitty henkilö. Tietoa ei saa lähettää sähköpostissa.

II turvaluokka - salainen: arkaluonteista, salassa pidettävää tietoa, jota voivat käsitellä vain ne, jotka on virastossa oikeutettu käsittelemään salassa pidettäviä asioita. Salaista tietoa voi lähettää sähköpostissa vain riittävän vahvasti salattuna.

III turvaluokka - luottamuksellinen: salassa pidettävää tietoa, jota voivat käsitellä vain ne, jotka tehtävässään sitä tarvitsevat. Tietoa voi lähettää sähköpostissa riittävän vahvasti salattuna.

IV turvaluokka - viranomaiskäyttö: Tiedon paljastuminen heikentäisi viranomaisen toimintaedellytyksiä.

Valtionhallinnon turvaluokitus on tarkemmin selitetty valtiovarainministeriön ohjeessa VM 5/01/2000.

▲ luokitella, luokitus, tietojen luokitus ▶ luottamuksellinen, viranomaisen asiakirja ▼ C-tason turvallisuus, erittäin salainen, erityissuojattava tieto, salainen, salassa pidettävä tieto, turvaluokitettava tieto, turvamerkintä, viranomaiskäyttö

turvamerkintä

en security marking

valtionhallinnon turvaluokituksen mukainen asiakirjaan tehtävä leima tai merkintä, josta ilmenee, mihin turvaluokkaan asiakirja kuuluu ja millä perusteella

▲ merkintä, turvaluokitus

turvamoduuli
en security module

erikoissuojattu komponentti, esimerkiksi mikropiiri, joka liitetään tietoteknisen laitteen kuten tietokoneen, kortinlukijan, verkkolaitteen tai matkapuhelimen osaksi ja joka sisältää tietoturvallisuutta lisääviä tai väärinkäyttöä ehkäiseviä välineitä, esimerkiksi salausalgoritmin ja salausavaimia

▶ *varmalaite* ▼ *avainpiiri, poletti, toimiavain, tonkeli, USB-avain*

turvaohjeet
kts. *tietoturvaohjeisto*

turvaohjelma ♣
en security monitor; tiger

ohjelma, joka pyrkii ylläpitämään isäntäjärjestelmän tietoturvallisuutta esimerkiksi havaitsemalla hyökkäykset ja hälyttämällä niistä tai hakemalla oman järjestelmän turva-aukot ja haavoittuvuudet niiden poistamiseksi

▲ *ohjelma* ▶ *haavoittuvuus, murto-ohjelma, roskapostiansa, roskapostisuodatin, suodatin, suojausohjelmisto, tiedustelupaketti, tuholaisohjelma ♣, valkolakki* ▼ *ansa, houkutuslintu, tietomurtohälytin, viruksentorjuntaohjelma, virustutka*

turvapalvelin
en security server

verkossa jotakin tietoturvallisuuden osa-alueita hoitava palvelin

▲ *palvelin* ▶ *välipalvelin* ▼ *notaaripalvelin, palomuuuri ♣*

turvaposti
en secure e-mail

sähköpostipalvelu tai -tekniikka, joka tarjoaa tietoturvallisuutta lisääviä ominaisuuksia, kuten kiistämättömyyden ja digitaalisen allekirjoituksen

▶ *digitaalinen allekirjoitus, kiistämättömyys* ▼ *S/MIME*

turvaprofiili
en protection profile

tiettyyn suojattavien kohteiden luokkaan liittyvät turvallisuusvaatimukset

▲ *suojaus* ▶ *tärkeysluokitus, vaatimus*

turvareititin
en secure router

tietoturvaominaisuuksin varustettu tai hyökkäyksiä vastaan suojattu reititin

▶ *IPSec*

turvasuunnitelma
kts. *tietoturvasuunnitelma*

turvatalletus
en escrow

salausavaimen tai lähdeohjelman jättäminen luotettavan tahon, esimerkiksi varmennusviranomaisen haltuun turvatoimenpiteenä, jotta talletuksen kohde olisi kaikissa olosuhteissa käytettävissä

Näitä olosuhteita voisivat olla esimerkiksi salausavaimen hukkaaminen, ohjelmiston myyjän konkurssi, tai salausavaimen ottaminen viranomaisen haltuun rikoksen selvittämiseksi.

▲ *salakirjoituspolitiikka, tietoturvallisuus ♣, varmennehallinto* ▶ *avaimen palautus, luotettu taho, vara-avainjärjestelmä*

Twofish
eräs symmetrisen lohkosalauksen menetelmä

▲ *symmetrinen lohkosalaus* ▶ *AES, Blowfish*

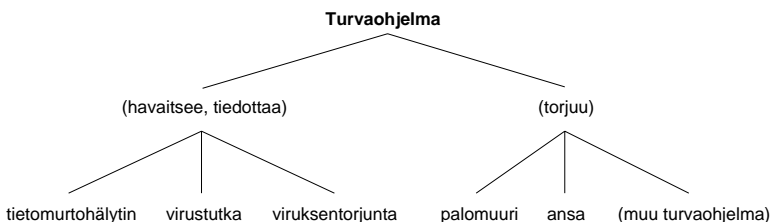
TYVI
tietovirrat yrityksiltä viranomaisille

standardoitu menettely eräille viranomaisille ja eläkeyhtiöille tehtävien toistuvaisilmoitusten lähettämiseksi määrämuotoisena datansiirtona

työelämän tietosuojalaki
en Act on Privacy Protection in the Workplace

laki yksityisyyden suojasta työelämässä (477/2001) täydentää henkilötietolakia muun muassa soveltuvuustestien, työterveyshuollon tietojen ja teknisen valvonnan osalta

▲ *laki, tietosuoja ♣, tietosuojalaki* ▶ *henkilötietolaki, tekninen valvonta*



tärkeysluokitus

en priority classification

1) organisaatioiden, tietojärjestelmien, tietojen, työtehtävien ja muiden olioiden jakaminen luokkiin sen mukaan, miten tarpeellisia ne ovat tarkasteltavan toiminnan jatkuvuudelle

2) valtiovarainministeriön laatima ministeriöiden, virastojen ja laitosten jako kolmeen luokkaan sen perusteella, miten välttämätöntä niiden tietojärjestelmien toiminnan jatkuvuus on yhteiskunnan kannalta

▲ *luokitus, tietojen luokitus* ▶ *poikkeusolot, turva-profiili, valmiussuunnittelu* ▼ *elintärkeä sovellus*

täsmäase

en smart weapon

sulautetun tietotekniikan ansiosta tarkasti osuva tai ajoittuva ase, esimerkiksi pommi, ohjus tai räjähdde

▶ *sähköinen sodankäynti*

täysvalmius

en full preparedness

valmius, jossa kaikki voimavarat on otettu käyttöön ja keskitetty häiriö- ja kriisitilanteen aiheuttamien vaikutusten ehkäisemiseksi ja niistä selviytymiseksi

▲ *valmius* ▶ *perusvalmius, poikkeusolot, tehos-tettu valmius*

töiden etäsyöttö

en remote job entry

tietojenkäsittelytöiden syöttäminen verkon välityksellä

▲ *etäkäyttö*

U

uhka

en hazard; threat

tietoihin tai tietojärjestelmään tietyltä taholta kohdistuvan vahingon tai häiriön mahdollisuus

▲ *käytettävyys (1)* ▶ *haavoittuvuus, hyökkääjä, riski, turvallisuus, vahinko, valmius* ▼ *atk-sabotaasi, sisäinen uhka, ulkoinen uhka, vaarantaa*

uhka-analyysi

en threat analysis

turvattavaa kohdetta vaarantavien uhkien tunnistaminen ja niistä aiheutuvien riskien arviointi perustana tietoturvasuunnittelulle

▲ *analyysi, tietoturvasuunnittelu* ▶ *haavoittu-vuustutkimus, riskianalyysi*

ulkoinen uhka

en outside threat

ulkopuolisten toiminnasta aiheutuva uhka

▲ *uhka* ▶ *sisäinen uhka*

UPS

uninterrupted power supply

katkoton tehonsyöttö tai sen tarjoava järjestelmä

urkintatekniikka

en spyware

menetelmät ja ohjelmat, joilla hankitaan tietoja verkon käyttäjistä tämän huomaamatta

▲ *tekniikka* ▶ *hyökkäys, käyttäjäprofiili, pengon-ta, PING, tiedustelu, tietoturvatekniikka, yritysva-koilu* ▼ *Carnivore, Echelon, nuuskia, näppäinlo-ki, piilojäljite, salakuuntelu, siepata, telekuuntelu, televalvonta, tunnustella*

USB-avain

en USB key

USB-porttiin kytkettävä turvamoduuli, joka sisältää avaimen kiintolevyyn tallennetun datan sala-kirjoittamiseen ja avaamiseen

▲ *avain, toimiavain, tonkeli, turvamoduuli*

USERID

kts. *käyttäjätunnus*

uudelleenaloitus

en restart

keskeytyneen ajon jatkaminen aloittamalla se uu-delleen alusta

▲ *käyttö (2)* ▶ *jatkoaloitus, virhelopetus*

uusinta-ajo

en rerun

virheen tai keskeytymisen vuoksi alusta uudel-leen suoritettava ajo

▶ *jatkoaloitus, uusittavuus*

uusittavuus

en repeatability

toimenpiteen uudelleen suorittamisen mahdolli-suus tietystä tilanteesta lähtien

▲ *ominaisuus* ▶ *jäljitettävyys, tarkastettavuus, todennettavuus, uusinta-ajo*

V

vaarantaa

en compromise (v)

asettaa alttiiksi uhalle tai riskille

Rikoslain 34:9a §koskee tietojenkäsittelyn vaa-rantamisen rangaistavuutta.

▲ *tietotekniikkarikos, uhka* ▶ *riski* ▼ *vaarantua, vaarantuminen*

vaarantua

en be compromised

joutua alttiiksi uhalle tai riskille

▲ vaarantaa ► turvallisuušhäiriö, valvontakatko

vaarantuminen

en compromise (s)

turvallisuuđen pettäminen, mistä voi aiheutua vahinkoa suojattavalle kohteelle

▲ tietoturvaluisuus ♣, vaarantaa

vaatimus

en requirement; criteria

► arkaluonteinen tieto, erityissuojattava tieto, hyväksymistarkastus, kelpoisuus, käyttökelpoisuus, palvelutaso, tarkastaa (2), turvallisuustodistus, turvaprofiili, vaativa sähköinen asiointi

vaativa sähköinen asiointi

en secure e-government service

sähköinen asiointi, joka tyydyttää tiukat tietoturva-vaatimukset

▲ sähköinen asiointi, verkkoasiointi ► vaatimus, varmennettu verkkoasiointi

vahinko

en damage

aiheuttajaansa yhdistettävissä oleva menetys, kuten

- fyysisen tai aineettoman omaisuuden häviäminen

- toiminnan tulosten tai edellytysten heikkeneminen

- ihmisen tai luonnon elinolosuhteiden huononeminen

► fyysinen turvallisuus, oikeudenloukkaus, riski, saastuminen, tietoturvariski, turva-arkisto, uhka, vastuunrajausilmoitus ▼ atk-sabotaasi

VAHTI

valtionhallinnon tietoturvaluisuuden johtoryhmä

valtiovarainministeriön asettama ja johtama hallinnon tietoturva-, tietohallinto- ja turvallisuusvastaavista koostuva laajapohjainen ryhmä, jonka tehtävänä on kehittää ja koordinoida tietoturvaluisuutta valtionhallinnossa

VAHTI mm. käsittelee valtionhallinnon tietoturvaluisuutta koskevat keskeiset ohjeet, suositukset ja määräykset sekä muut linjaukset sekä vastaa valtion tietoturvaohjeiston kehittämisestä.

▲ viranomainen ► valtionhallinnon tietoturvaohjeisto

vahtiajastin

en watchdog timer

ajastin, joka seuraa laitteen tai ohjelman toimintaa ja antaa hälytyksen, jos viive tai toimimattomuus on kestänyt ennalta määrätyn ajan

▲ käytettävyyys (1), monitori, seurain ► aikakatkaisu, aikapommi

vahva salaus

en strong encryption

salakirjoitus, joka ei ole väsytystekniikalla avattavissa tavanomaisella laskentakapasiteetilla ja käytettävissä olevassa ajassa

▲ salaus ► kevyt salaus, laskennallisesti murtovarma, vahva tunnistus

vahva salausalgoritmi

en strong encryption algorithm

vahvan salauksen antava salausalgoritmi

Näitä ovat mm. IDEA, RC4, RC5, Blowfish, MD5, SHA, RSA, ElGamal ja DSS. Vastaavasti vahvoja salaavia käytäntöjä ovat mm. AH, ESP, PGP, Photuris, SET, SKIP, SSH, SSL, S/MIME ja S/WAN.

▲ salausalgoritmi

vahva todennus

kts. vahva tunnistus

▲ todennus

vahva tunnistus

en strong authentication

käyttäjän tunnistus tai todennus, joka käyttää ainakin kahta seuraavista kolmesta menetelmästä:

- käyttäjä ilmoittaa jonkin vain hänen tiedossaan olevan asian, esimerkiksi salasanan

- käyttäjällä on jokin tunnistukseen käytettävä esine tai laite, esimerkiksi avain tai henkilökortti

- käyttäjä tunnistetaan jonkin ominaisuutensa, esimerkiksi puhutavan tai sormenjäljen perusteella

▲ sähköinen tunnistus, tunnistus ► julkisen avaimen menetelmä ♣, kevyt tunnistus, vahva salaus

vahviste

kts. varmenne, varmiste

valevirus

en hoax virus

kiusantekomielessä lähetetty vaaraton viesti, jonka väitetään sisältävän viruksen

▲ virus ♣ ► piilovirus, virusvalhe

valkolakki

en white hat; samurai

hakkeri, joka järjestelmän omistajan toimeksiantosta testaa suojausten pitävyyttä yrittämällä murtautua järjestelmään

► hakkeri, murtautuja, turvaohjelma ♣

valmius

en preparedness

suunnittelun ja valmistelujen tuloksena saavutettu tila, jossa kyetään vastaamaan tiettyihin uhkiin

► uhka ▼ perusvalmius, tehostettu valmius, täysvalmius, varallaolo, varautuminen

valmiuslaki

en Emergency Powers Act

laki (1080/1991, muutettu 198/2000) määrittelee poikkeusolot ja menettelyjä yhteiskunnan turvaamiseksi niiden varalta

▲ laki, tietoturva-oikeus ▶ poikkeusolot

valmiusraportti

en preparedness report

järjestelmän omistajan määräaikainen selvitys elintärkeiden sovellusten tietoturvallisuudesta ja ylläpidosta

▲ valmiussuunnittelu ▶ elintärkeä sovellus

valmiussuunnitelma

en preparedness plan

poikkeusolojen varalta tehtävä varautumissuunnitelman osa

Valmiussuunnitelmassa määritellään mm. tietojenkäsittelyn toimivuusvaatimukset eri tasoilla vahinkotilanteessa, palvelujen hallitun supistamisen vaiheet sekä toipumistimenpiteet normaalioloihin palaamiseksi.

▲ jatkuvuussuunnitelma, poikkeusolot, suunnitelma, varautumissuunnitelma

valmiussuunnittelu

en preparedness planning

varautuminen ja toimenpiteiden suunnittelu poikkeusolojen tai muun vakavan häiriön varalta ja siitä toipumiseksi

▲ suunnittelu, varautuminen ▶ Puolustus-taloudellinen suunnittelukunta, tärkeysluokitus ▼ CIAO, KBM, NISCC, OCIPER, valmiusraportti

valtionhallinnon tietoturvaohjeisto

en government information security directives

valtiovarainministeriön antama hallinnon käyttöön tarkoitettu tietoturva-aiheinen ohjekokoelma, jota käytetään hyväksi myös muualla yhteiskunnassa Ohjeiston kehittämisestä vastaa VAHTI ja se on saatavissa web-sivulta www.vm.fi/vahti.

▲ ohje, tietoturvaperaatteet, tietoturvapoliittikka ▶ VAHTI

valtionhallinnon tietoturvapäätös

en Decision on Information Security in Government

valtiovarainministeriön valmisteleva valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (VM 0024:00/02/99/1998)

▲ päätös, tietoturvalinjaukset, tietoturvapoliittikka

valtuus

en authority

oikeus tiettyjen tietojen käyttöön tai tietojärjestelmäresurssien käyttöön

▲ käyttö (1) ▶ järjestelmän omistaja, käyttö-oikeus, valtuutus ▼ käsittelyvaltuutus, käyttövaltuudet, käyttövaltuuksien hallinta, pääsyvaltuutus, toimivain, valtuuskortti, valtuustieto, valtuutettu käyttäjä, valtuutus, varmennuspäätö, viiteseurain

valtuuskortti

en master card

toimikortti, jota käyttäen voi muuttaa tai lisätä toisen toimikortin tietoja

▲ kortti, toimikortti, valtuus

valtuustieto

en credential(s)

todiste valtuuksien omaamisesta tai viestin lähettäjän aitoudesta

▲ tieto, todennus, valtuus ▶ aitous

valtuutettu käyttäjä

en authorized user

tiettyihin toimiin tarvittavat valtuudet omaava käyttäjä

▲ käyttäjä, valtuus ▶ luvaton käyttäjä, pääkäyttäjä (1), pääkäyttäjä (2)

valtuutus

en authorization

omistajalta tai viranomaiselta saatu valtuus toimia tiettyssä asiassa, esimerkiksi käyttää tietojärjestelmää

▲ valtuus ▶ akkreditointi, kelpuutus, valtuus

valvoa

en monitor (v); supervise

seurata toimintaa, arvioida sitä tai sen tuloksia annettujen kriteerien suhteen ja erojen ilmaantuessa tarvittaessa puuttua toiminnan kulkuun

▶ nuuskia, varmistaa ▼ valvonta

valvonta

en control (1); monitoring; supervision

toiminnan tai tapahtumien seuranta ja ryhtyminen tarvittaessa toimiin

▲ valvoa ▶ ohjaus, pakkokeinolaki, suodatus, tarkastus (2), tarkkailu, viranomaispääsy ▼ kulunvalvonta, pääsynvalvonta, tekninen valvonta, televalvonta, valvontakatko

valvontakatko

en control failure

tapahtuma, jossa valvonta pettää ja riski toteutuu

▲ valvonta ▶ turvallisuushäiriö, vaarantua

valvontalaite

kts. seurain

vara-avainjärjestelmä**en** key escrow (system)

järjestelmä, jonka mukaan salausavainten turvatalletus on säädetty pakolliseksi ja turvatalletuksessa oleva avain on tietyissä tilanteissa tai oikeuden päätöksellä luovutettava edelleen sitä vaativalle viranomaiselle

Suomessa salaisista avaimista ei yleensä oteta kopioita, mikä toisaalta saattaa vaikeuttaa toipumista onnettomuuksista ja häiriöistä.

▲ *salakirjoituspolitiikka, salausavain* ♣ ▶ *avaimen palautus, toipuminen, turvatalletus* ▼ *viranomaispääsy*

varajärjestelmä**en** backup system; fallback system

tietojärjestelmä tai laitteisto, joka voidaan ottaa käyttöön, kun normaalisti käytettävän järjestelmän käyttö häiriintyy tai estyy

▲ *käytettävyyys (1), luotettavuus, tietojärjestelmä, tietotekniikan varmistus* ▶ *häiriö, VAVK*

varakeskus**en** backup site

tietokonekeskus, joka voidaan ottaa käyttöön, kun normaalisti käytettävän tietokonekeskuksen käyttö häiriintyy tai estyy

▲ *käytettävyyys (1), tietotekniikan varmistus* ▶ *varakonesopimus, varalaitteisto, varatila, varautumissuunnitelma* ▼ *kylmä varakeskus, VAVK*

varakonesopimus**en** backup system agreement

sopimus toisen hallinnassa olevan varakeskuksen tai varalaitteiston käytöstä

▲ *varautumissuunnitelma* ▶ *varakeskus, varalaitteisto*

varalaitteisto**en** backup hardware

laitteisto, joka voidaan ottaa käyttöön, kun normaalisti käytettävän laitteiston käyttö häiriintyy tai estyy

▲ *käytettävyyys (1)* ▶ *varakeskus, varakonesopimus, varallaolo, varautumissuunnitelma*

varallaolo**en** standby

(laitteen) valmius ryhtyä suorittamaan tehtävää vikaantuneen laitteen sijasta

▲ *häiriö, käytettävyyys (1), valmius* ▶ *varalaitteisto*

varareitti**en** alternate route

fyysinen tai tietoliikennereitti, joka voidaan ottaa käyttöön, kun normaalisti käytetyn reitin käyttö häiriintyy tai estyy

▲ *varautumissuunnitelma*

varatila**en** backup premises

ennalta valmisteltu toimitila, jossa tuhon sattessa toimintaa voidaan jatkaa

▶ *varakeskus*

varautuminen**en** contingency planning

toiminta, jonka tarkoituksena on luoda ja ylläpitää organisaation riittävä valmius normaaliolojen häiriötilanteiden ja poikkeustilanteiden varalta

Varautuminen käsittää suunnitteluna sekä tarvittavat etukäteisvalmistelut.

▲ *käytettävyyys (1), suunnittelu, valmius* ▶ *häiriö, poikkeustilanne* ▼ *huoltovarmuus päätös, Puolustustaloudellinen suunnittelukunta, valmiussuunnittelu, varautumissuunnitelma*

varautumissuunnitelma**en** contingency plan

suunnitelma, jossa esitetään järjestelyt tietojenkäsittelyä tai tietoliikennettä kohtaavan häiriön tai keskeytyksen varalta sekä normaali- että poikeusoloissa

▲ *suunnitelma, varautuminen* ▶ *jatkuvuussuunnitelma, varakeskus, varalaitteisto* ▼ *toipumissuunnitelma, valmiussuunnitelma, varakonesopimus, varareitti*

varmalaitte**en** trusted device; secure device

uskottavasti suojattu laite, esimerkiksi toimikortti tai turvamoduuli, joka noudattaa luotetun tahon sille lähettämiä käsittelysääntöjä

Esim. kassapäätte, joka vastaanottaa pankilta rahan käsittelyä koskevat säännöt.

▶ *turvamoduuli* ▼ *varmennuspäätte*

varmenne**en** certificate

konekoodinen aitoustodistus, jonka ulkopuolinen luotettu taho (varmentaja) on myöntänyt palveluverkossa asiakkaana, palveluntuottajana, varmentajana tai muussa ominaisuudessa toimivalle Varmenteen haku, myöntäminen, ylläpito ja käyttö tapahtuvat julkisen avaimen järjestelmän puitteissa.

Varmenne sisältää varmenteen haltijan julkisen avaimen ja tunnistetiedot, tietoja varmenteen myöntäjältä sekä muita varmenteen käytön kannalta tarpeellisia tietoja esimerkiksi toimiluvista ja -valtuuksista. Varmenne on julkinen, mutta alikirjoitettu varmentajan omalla yksityisellä avaimella, jolloin sen aitouden voi todeta avaamalla varmenteen varmentajan julkisella avaimella.

Varmenteen sisältö ja käyttötarkoitus voivat vaihdella, esimerkiksi

- henkilövarmennetta käytetään henkilön tunnistamiseen, digitaaliseen allekirjoitukseen ja viestin salakirjoittamiseen
- roolivarmennetta todisteena mm. organisaatioon tai organisaatioyksikköön kuulumisesta tai tietyistä käyttövaltuuksista
- palvelinvarmennetta todistamaan, että palveluntuottaja on se, joka hän väittää olevansa
- sähköpostivarmennetta sähköpostin turvallista käyttöä varten.

▲ *julkisen avaimen järjestelmä, luotettu taho* ▶ *aitous, hallinnon sähköinen asiointi, leima, sähköinen tunnistus, turvallisuustodistus, varmiste*
▼ *digitaalinen allekirjoitus, henkilövarmenne, julkisen avaimen varmenne, juurivarmenne, kansalaisvarmenne, laatuvarmenne, monivarmenneympäristö, PAC, palvelinvarmenne, PKI-varmenne, roolivarmenne, sulkulista, varmentaja, varmentaminen*

varmennehakemisto

en certificate directory

julkinen hakemisto, joka sisältää tietyn varmennehallinnon puitteissa myönnetty, varmentajan allekirjoittamat varmenteet

▶ *hakemistopalvelu, varmentaja*

varmennehallinto

en certificate administration

julkisen avaimen järjestelmässä yhden varmennusorganisaation jäsenen muodostama toiminnallinen kokonaisuus

▲ *hallinto, julkisen avaimen järjestelmä, varmentaja* ▶ *varmennepalvelu, varmennusorganisaatio, viranomaispääsy* ▼ *turvatalletus*

varmennepalvelu

en certification service

varmentajan tehtäviin liittyvä palvelu

▲ *palvelu, varmentaja, varmentaminen* ▶ *varmennehallinto* ▼ *monivarmenneympäristö*

varmennepolitiikka

en certificate policy

varmentajan julkaisema asiakirja, jossa kuvataan, miten varmennepalveluja tuotetaan niiden käyttäjille

▲ *politiikka, tietoturvapolitiikka* ▶ *salakirjoituspolitiikka*

varmennepolku

en certificate path

varmenteiden sarja, joka tulee voida muodostaa kahden osapuolen välille, jotta ne voivat turvallisesti asioida toistensa kanssa

Polku saadaan aikaan joko siten, että molemmille löytyy jollakin varmennehallinnon tasolla yhteinen varmentaja, tai että eri varmennehallinnoissa toimivat varmentajat ovat sopineet vastavuoroisesti toistensa varmenteiden hyväksymisestä.

varmennettu verkkoasiointi

en certified e-government service

sähköistä henkilökorttia käyttäen tapahtuva asiointi

▲ *verkkoasiointi* ▶ *sähköinen henkilökortti, vaativa sähköinen asiointi*

varmenneviranomainen

kts. *varmentaja*

varmennus

kts. *varmentaminen*

varmennusorganisaatio

en certification hierarchy

hierarkia, joka käsittää eritasoisia varmentajia

▲ *varmentaja* ▶ *akkreditointijärjestelmä, varmennehallinto* ▼ *juurivarmenne, monivarmenneympäristö*

varmennuspäät

en authorization terminal

kassapäätteeseen kuuluva tai erillinen laite, jonka välityksellä tarkistetaan maksajan valtuus käyttä hallussaan olevaa maksukorttia

▲ *valtuus, varmalaitte*

varmentaja

en certificate authority

julkisen avaimen järjestelmässä luotettu taho, joka tuottaa järjestelmän käyttäjille avainparit ja tuottaa, allekirjoittaa ja jakelee varmenteet ja tallettaa ne julkiseen hakemistoon sekä tarvittaessa peruuttaa varmenteet

EU-maassa varmentaja ei saa pitää hallussaan asiakkaansa yksityistä avainta, ellei asiakas tätä pyydä.

▲ *julkisen avaimen järjestelmä, varmenne* ▶ *avainten jakelukeskus, luotettu taho, varmennehakemisto* ▼ *akkreditointijärjestelmä, varmennehallinto, varmennepalvelu, varmennusorganisaatio, ylin varmentaja*

varmentaminen

en certification

julkisen avaimen todistaminen tietyille henkilöille tai organisaatiolle kuuluvaksi liittämällä siihen varmenne

Varmentamistoimintaa Suomessa säätelee laki sähköisistä allekirjoituksista (14/2003).

▲ *tietotekniikkaoikeus, varmenne* ▶ *akkreditointi, leimata, sähköinen allekirjoitus, todennus, varmistus (1)* ▼ *SET, varmennepalvelu*

varmistaa

en assure; back up; check (v); ensure; secure (v)
 1) tehdä varmemmaksi tai luotettavammaksi
 2) varautua virheiden, vikojen, toimintahäiriöiden, ulkopuolisen sekaantumisen tai muun poikkeavan tilanteen varalta

▲ *käytettävyys (1), luotettavuus* ▶ *sinetöidä, tarkastaa (1), tarkistaa (1), tietojen turvaaminen, todentaa, valvoa* ▼ *kahdentaa, kirjausketju, varmiste, varmistus (1), varmistus (2), varmuuskopio, vastakutsu, vedostaa*

varmiste

en check symbol

tiedon siirron tai tallentamisen varmistamiseen käytetty tiedosta muodostettu tiiviste, joka siirretään tai tallennetaan sisältötiedon mukana

Vastaanotetun tai tallennetun tiivisteen ja tiedosta samoin muodostetun uuden tiivisteen välinen ero on osoituksena tiedon siirrosta tai tallennuksessa tapahtuneesta virheestä.

▲ *varmistaa* ▶ *sinetti, tiiviste, varmenne, virhe (2)* ▼ *MAC (1), varmistusbitti, varmistusmerkki, varmistusnumero, varmistussumma*

varmistus (1)

en control (2)

suunnitelmallinen jatkuva toiminta tai toistuva toimenpide, jolla toteutetaan valvonta

▲ *varmistaa* ▶ *tarkistaa (1), varmentaminen*
 ▼ *tietotekniikan varmistus*

varmistus (2)

en check (s); checking; error control

tiedon tarkastettavuuden aikaansaanti toistoa tai varmistetta käyttäen

▲ *varmistaa* ▶ *tarkastettavuus* ▼ *itsevarmistava koodi, jakojäännösvarmistus, kaikuvarmistus, ylimäärä*

varmistusbitti

en check bit

varmisteenä käytetty bitti, esimerkiksi pariteetti-bitti

▲ *varmiste*

varmistuskohta

en checkpoint

ohjelman kohta tai ajon vaihe, jossa varaudutaan jatkoaloitukseen

▲ *käyttö (2)*

varmistusmerkki

en check character

varmisteenä käytetty merkki tai merkin mittainen bittijono

▲ *varmiste*

varmistusnumero

en check digit

yhden merkin mittainen numeerinen varmiste

▲ *varmiste*

varmistussumma

en checksum; proof total

varmiste, joka muodostetaan laskemalla yhteen määrämittäisiä tiedon osia ikään kuin ne olisivat lukuja

▲ *varmiste*

varmistustiedosto

en backup file

tiedoston varmuuskopio

▲ *käytettävyys (1), varmuuskopio* ▶ *toisiokanta*

varmuusarkisto

en backup archive

arkisto, joka sisältää tallenteiden varmuuskopiot siltä varalta, että käyttöarkistoon talletettu ei ole käytettävissä

▲ *arkisto* ▶ *käyttöarkisto, turva-arkisto, varmuuskopio*

varmuuskopio

en backup copy; backup

taltion, tiedoston tai ohjelman kopio, joka on tarkoitettu käytettäväksi, jos alkuperäinen menetetään vian tai vahingon takia

▲ *kopio, käytettävyys (1), varmistaa* ▶ *turvakopio, varmuusarkisto* ▼ *varmistustiedosto, varmuuskopiointi*

varmuuskopiointi

en backup

varmuuskopioiden tekeminen

▲ *varmuuskopio*

vastaava

▼ *järjestelmävastaava, käyttövaltuuksien hoitaja, pääkäyttäjä (1), rekisterinpitäjä, verkkovastaava, web-vastaava*

vastakutsu

en call-back (1)

tunnistuksen varmistaminen siten, että järjestelmä ottaa uuden yhteyden sitä kutsuneeseen käyttäjään tiedossaan olevalla verkko-osoitteella tai puhelinnumerolla

▲ *etäkäyttö, varmistaa* ▶ *haastemenetelmä*

vastasoitto

kts. *vastakutsu*

vastustuskykyinen

en resilient; resistant

toimintakykynsä eri tilanteissa säilyttävä

▲ *käytettävyys (1), ominaisuus* ▶ *katastrofisetoinen, sitkeys, vikasetoinen*

vastuunrajausilmoitus

en disclaimer

tuotteeseen, esimerkiksi valmisohjelmistoon liitetty ilmoitus, jonka mukaan tuotteen valmistaja ei vastaa ilmoituksessa luetelluista tuotteen käytöstä mahdollisesti aiheutuvista vahingoista

▶ *oikeus, tietosuojaseloste, vahinko*

VAVK

Valtion atk-varmistamiskeskus

Huoltovarmuuskuskuksen ylläpitämä varakeskus, jonka tehtävänä on poikkeusolojen tai vakavien häiriöiden sattua tarjota palveluja valtionhallinnon ja muille keskeisille organisaatioille

▲ *Huoltovarmuuskeskus, varakeskus* ▶ *varajärjestelmä*

vedostaa

en dump (v)

tallentaa muistissa olevaa tietoa tietovälineeseen tai oheismuistiin yleensä varmistustoimia tai tilanteen tutkimista varten

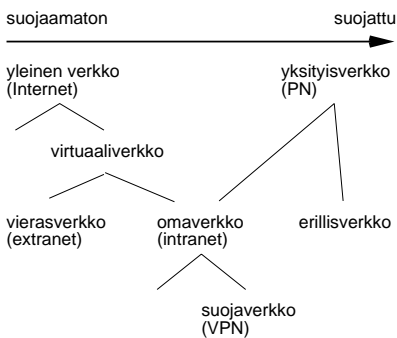
▲ *varmistaa* ▶ *kahdentaa, toisintaa* ▼ *välivedos*

verkko ♣

en net; network

▼ *avoin verkko, dataverkko, lähiverkko, omaverkko, palveluverkko, suljettu verkko, telehallintaverkko, tietoverkko ♣, vierasverkko, VPN-verkko, yksityisverkko*

Tietoverkko suojaustason ja -tavan mukaan



verkko-osoitteen väärentäminen

en IP spoofing

hyökkäys, jossa murtautuja tekeytyy joksikin toiseksi käyttämällä tämän IP-osoitetta

▲ *hyökkäys* ▶ *tekeytyminen*

verkkoalue

en administrative domain

tietoverkon osoitteiden hierarkkiseen jakoon perustuva osaverkko

Verkkoalue muodostaa tietoverkon hallinnollisen yksikön ja voidaan edelleen jakaa osaverkkoihin esimerkiksi organisaation tai palvelimen mukaan.

▲ *tietoverkko ♣* ▼ *tunnushallintokeskus, verkko-tunnus*

verkkoanalysaattori

en network analyzer; packet sniffer

verkonhallinnan ohjelma, joka seuraa liikennettä ja tallentaa annetut kriteerit täyttävät paketit mahdollista tarkastelua varten

▲ *analyysi, seurain, verkonhallinta* ▶ *nuuskin, pakettisuodatin, verkkojälki*

verkkoasema

en host

verkkoon kytketty tietokone, yleensä työasema, joka voi hyödyntää verkon palveluja ja ominaisuuksia

▲ *tietoverkko ♣* ▼ *verkkolinnake*

verkkoasiointi

en e-business; electronic commerce; home shopping

asian hoitaminen, esimerkiksi ostoksen teko tai hallinnollisen toimen vireillepano osaksi tai kokonaan tietoverkossa tarjottua palvelua käyttäen

Asiointiin käytettävän palvelun tarjoaja voi olla esimerkiksi verkkokauppa, rahalaitos tai viranomainen.

▲ *asiointi, verkkopalvelu* ▶ *julkisen avaimen järjestelmä* ▼ *anonymiasointi, asiointipalvelu, monitoimikortti, palvelujärjestelmä, vaativa sähköinen asiointi, varmennettu verkkoasiointi*

verkkoasiointilaki

en Act on Online Government Services

laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) sisältää säädöksiä verkkoasiointin menettelyistä hallinto- ja oikeudenkäyttöasioissa

▲ *laki, tietotekniikkaoikeus* ▶ *hallinnon sähköinen asiointi*

verkkoasiointiosoitte

kts. *toiminto-osoite*

verkkoasiointitunnus

kts. *sähköinen asiointitunnus*

verkköjäljite

en Web beacon

kuitin eli evästeen kanssa yhdessä toimiva tieto, jonka avulla ulkopuolinen saa tietoa verkon käyttäjän toiminnasta, esimerkiksi mainosivustonsa käytöstä tai lähettämänsä viestin perille menosta tai avaamisesta

▶ *eväste* ▼ *piilojäljite*

verkköjälki

en network trace

tietoverkon käytöstä verkon eri pisteisiin tallennetut käyttäjän liikenne-, käynti- ja asiointitiedot

▶ *jäljityspaketti*, *käyttäjäprofiili*, *verkkooanalysointori*

verkkokauppalaki

en Act on Electronic Commerce

laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002)

▲ *laki*, *tietotekniikkaoikeus* ▶ *julkisuuslaki*, *sananvapauslaki*

verkkolinnake

en secure host; bastion host

verkon haavoittuvaan kohtaan sijoitettu hyökkäyksille vastustuskykyinen verkkoasema

▲ *verkkoasema* ▶ *haavoittuvuus*, *hyökkäys*, *sitkeys*

verkkonimi

kts. *verkkotunnus*

verkkonotaari

en network notary

luotettu taho, joka tarjoaa tietoverkossa notariaattityyppisiä palveluja kuten aikaleimojen antamisen ja asiakirjojen säilyttämisen

▲ *luotettu taho* ▶ *aikaleimapalvelu*, *kiistämättömyys* ▼ *notaaripalvelin*, *notaaripalvelut*, *notarointi*

verkkopalvelu

en network service

tietoverkossa tieto- ja teletekniikan avulla toteutettu palvelu

▲ *palvelu*, *tietoverkko* ♣ ▶ *etähuolto*, *etätyö* ▼ *aikaleimapalvelu*, *asiointipalvelu*, *hakemistopalvelu*, *kieltolista*, *monitoimikortti*, *tiedotuspalvelu*, *verkkosointi*

verkkorikoslaki

en cybercrime law

Euroopan Neuvoston yleissopimuksen pohjalta työryhmä on laatinut ehdotuksen laiksi tietoverkkorikoksista (2003)

▲ *laki*, *tietotekniikkaoikeus*, *tietoturva-oikeus*

verkkoskannaus

en network scan

verkon rakenteen ja siinä olevien järjestelmien saavutettavuuden automaattinen tiedustelu

▲ *skannaus* ▶ *porttiskannaus*, *saavutettavuus*, *tiedustelupaketti*

verkkosodankäynti ♣

en netwar; network-centric warfare

tietosodankäynnin toiminnot, jotka kohdistuvat vastustajan tietoverkkoihin vaikuttamiseen haitallisesti sekä omien tietoverkkojen suojaamiseen

▲ *sodankäynti*, *tietosodankäynti* ♣ ▶ *hakkerointi*, *tietojärjestelmäsodankäynti* ▼ *verkkoterrorismi*

verkkoterrorismi

en cyber terrorism

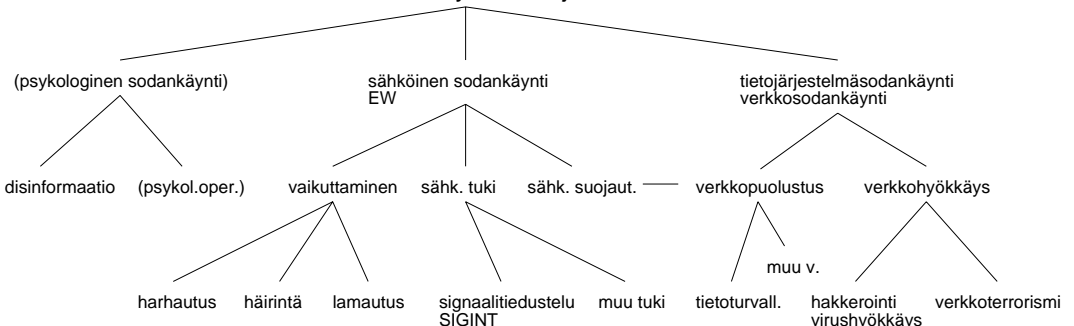
terroriteoksi luettava tietoverkkoihin ja niissä oleviin resursseihin kohdistuva tuhoistoiminta tai häirintä, erityisesti jos tekijänä on muu kuin valtio

▲ *tietoverkkorikos*, *verkkosodankäynti* ♣

verkkotunnuksen kaappaus

en domain name grabbing

Tietosodankäynnin muotoja



sellaisen verkkotunnuksen varaaminen, joka on sama kuin toisen henkilön tai organisaation nimi tai muistuttaa sitä, yleensä kiusantekomielessä tai taloudellisen hyödyn saamiseksi

▲ *kaappaus, verkkotunnus* ▶ *nimenvaltaus*

verkkotunnus

en domain name

verkkoseman tai verkkoalueen symbolinen tunnisteen Internet-verkossa

Verkkotunnus muodostuu hierarkkisesti ISO-standardin mukaisesta maatunnuksesta (USA:n ulkopuolella), verkkoalueen tunnuksesta, sen aliverkon ja mahdollisen alialiverkon tunnuksesta sekä mahdollisesti organisaatioyksikön ja palvelimen tunnuksesta. Ylätason verkkotunnuksia ovat maatunnukset kuten .fi (Suomi), .se (Ruotsi), .ee (Eesti) tai .ru (Venäjä). USA:ssa ylin taso tarkoittaa toimialaa, esimerkiksi .com (kaupallinen), .gov (julkishallinto), edu (opetus) tai .org (järjestö).

▲ *Internet, tunnus, verkkoalue* ▶ *verkkotunnuslaki* ▼ *fi-juuri, nimenvaltaus, verkkotunnuksen kaappaus*

verkkotunnuslaki

en Domain Names Act

Suomelle kuuluvan fi-juuren verkkotunnusten saannin ja käytön määrittelevä laki (228/2003)

▲ *Internet, laki, tietotekniikkaoikeus* ▶ *fi-juuri, tunnushallintokeskus, verkkotunnus, Viestintävirasto*

verkkovastaava

en network administrator

henkilö, jolle kuuluu huolehtia verkonhallinnan tehtävistä ja verkkopalvelujen ylläpidosta

▲ *vastaava, verkonhallinta* ▶ *web-vastaava*

verkonhallinta

en network management

1) tietoverkon ylläpito ja sen tietoliikenteen valvonta

2) verkon ylläpidosta, kehittämisestä ja valvonnasta vastaava toiminto

▲ *hallinta, tietoverkko* ♣ ▶ *tietoliikenneturvallisuus, ylläpito* ▼ *jäljityspaketti, pakettisuodatin, SNMP, telehallintaverkko, verkkoanalysointi, verkkovastaava*

verkonhallintaohjelmisto

en network management software

ohjelmisto, jonka avulla seurataan, havaitaan ja raportoidaan vikatilanteita verkossa

▲ *hallinta, lähiverkko, ohjelmisto* ▶ *monitori, seurain*

vesileima

kts. *piiloleima*

vianjäljitys

en fault trace

vikojen sattumisesta kertovan tiedon keruu ja tallennus

▲ *vika*

vierasverkko

en extranet; partnernet

asiakkaille ja yhteistyökumppaneille avattu osa organisaation tietoverkosta

▲ *Internet, verkko* ♣ ▶ *harmaa vyöhyke, oma-verkko*

viestintämarkkinalaki

en Communications Market Act

laki (393/2003) sisältää säädöksiä muun muassa viestintäalan kilpailusta, kuluttajansuojasta, viranomaisasettelystä ja vaihtolovelvollisuudesta

▲ *laki, tietotekniikkaoikeus* ▶ *televiestinnän tietosuojalaki* ▼ *tietoliikenneturvallisuus*

viestintärikos

en communications crime

turvallista ja luottamuksellista viestintää vaarantava teko, esimerkiksi viestintäsalaisuuden loukkaus tai tietoliikenteen häirintä

Suomessa kriminalisoidut viestintärikokset on koottu rikoslain 38 lukuun.

▲ *rikos* ▶ *tietoliikenneturvallisuus, tietotekniikka-rikos, tietoverkkorikos* ▼ *salakuuntelu, tietoliikenteen häirintä, viestintäsalaisuuden loukkaus*

viestintäsalaisuuden loukkaus

en breach of communications secrecy

tahallinen tai tahaton viestinnän luottamuksellisuuden rikkoutuminen tai vaarantuminen

Rikoslain 38:3 §mukaan rikoksia ovat muun muassa oikeudeton

- tiedon hankkiminen suojatusta sähköisestä viestistä

- salakuuntelu teknisen laitteen avulla

- tiedon hankkiminen televerkossa välitettävänä olevasta puhelusta tai muusta televiestistä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta.

▲ *loukkaus, oikeudenloukkaus, salassapitorikkomus, tietoturvaloukkaus, viestintärikos* ▶ *salaisuus*

Viestintävirasto

en Finnish Communications Regulatory Authority

viestinnän alan hallintoviranomainen Suomessa

▲ *viranomainen* ▶ *CERT, hallinto, verkkotunnuslaki*

viestitiedustelu

en communications intelligence

sähköisessä sodankäynnissä vastustajan viestintään kohdistuva tiedustelu

▲ *signaalitiedustelu* ♣, *tiedustelu* ▶ *mittaustiedustelu* ▼ *Echelon***viiteseurain**

en reference monitor

ohjelmisto, joka rekisteröi tietojen ja ohjelmien saantia koskevat pyynnöt ja valtuuttaa niiden käytön

▲ *käyttöoikeus, seurain, valtuus***vika**

en fault

tila, jossa (tavallisesti laitteen) normaali toiminta on estynyt

▲ *käytettävyyks (1)* ▶ *esto, etähuolto, häirintä, häiriö, virhe (1), virhe (2), virhetilanne* ▼ *levyrikko, vianjäljitys, vikasietoinen***vikakynnys**

en fault threshold

erikoistoiimiin johtava vikojen määrän, taajuuden tai laadun vähimmäismäärä

▲ *käytettävyyks (1)* ▶ *liipaisin***vikasietoinen**

en fault tolerant

toimintakykynsä vioista huolimatta ainakin osittain säilyttävä

▲ *käytettävyyks (1), ominaisuus, vika* ▶ *katastrofisietoinen, sitkeys, vastustuskykyinen***vikataajuus**

en error rate

vikojen lukumäärä aikayksikössä

viranomainen

en (public) authority

valtion, kunnan tai eduskunnan tiettyä tehtävää itsenäisesti hoitamaan perustama organisaatio tai lain tai asetuksen perusteella julkista tehtävää hoitava yhteisö, laitos, säätiö tai yksityishenkilö

Julkisuuslain mukaan viranomaisia ovat mm. ministeriö, valtion tai kunnan virasto tai laitos, valtion liikelaitos, tuomioistuin, eduskunnan virasto tai laitos, Suomen Pankki, Kansaneläkelaitos, kunnan tilintarkastaja, sekä valtion viranomaisen tai tuomioistuimen asettama lautakunta, neuvotelukunta, komitea, toimikunta ja työryhmä.

▶ *julkisuuslaki, luotettu taho, normi, perusrekisteri* ▼ *ENISA, hallinnon sähköinen asiointi, Huoltovarmuuskeskus, Puolustuslaidollinen suunnittelukunta, SFS, tietosuojalautakunta, tietosuojavaltuutettu, tunnushallintokeskus, VAHTI, Viestintävirasto, viranomaisen asiakirja, VIRVE, yhteispalvelupiste***viranomaisen asiakirja**

en official document

viranomaisen hallussa oleva asiakirja, jonka viranomaisen tai sen palveluksessa oleva on laatinut tai joka on toimitettu viranomaiselle asian käsittelyä varten sen tehtäviin kuuluvassa asiassa

Viranomaisen asiakirjoja eivät kuitenkaan ole virkamiehen laatimat muistiinpanot tai sisäistä koulutusta varten hankitut asiakirjat.

▲ *asiakirja, viranomainen* ▶ *erittäin salainen, luottamuksellinen, salassa pidettävä tieto, turvallisuus***viranomaiskortti**

en civil service card

sähköinen henkilökortti, jota henkilö käyttää viranomaisena

▲ *kortti, sähköinen henkilökortti* ▶ *roolivarmenne, viranomaiskäyttö***viranomaiskäyttö**

en restricted use

tiedon tai asiakirjan saatavuuden rajoittaminen asiaa käsitteleviin viranomaisiin sillä perusteella, että paljastuminen saattaisi heikentää viranomaisen toimintaedellytyksiä

▲ *käyttö (1), turvallisuus* ▶ *julkinen, luottamuksellinen, salainen, viranomaiskortti***viranomaispääsy**

en lawful access

ulkopuolisen, esimerkiksi valvontaviranomaisen laillinen mahdollisuus saada haltuunsa salakirjoitettua tietoa vastaava ilmiteksti tai salakirjoituksessa käytetyt salausavaimet

▲ *pääsy, vara-avainjärjestelmä* ▶ *tarkastusoikey, valvonta, varmennehallinto* ▼ *Clipper chip***virhe (1)**

en error

suureen lasketun tai mitatun arvon ja todellisen tai teoreettisesti oikean arvon välinen ero

▲ *oikeellisuus* ▶ *vika* ▼ *muistivuoto, virhetilanne, ylivuoto***virhe (2)**

en mistake

ihmisen tai tietokoneen suorittama toimenpide, joka tai jonka tulos ei ole sovittujen sääntöjen tai tarkoituksen mukainen

▲ *sääntö* ▶ *tarkistaa (1), testata, varmiste, vika, virhetilanne* ▼ *perkaus, rakenteinen virheenhallinta, tarkastaa (1)***virhelopetus**

en abort (s);abend

ohjelman suorituksen lopettaminen odottamattomassa virhetilanteessa

▶ *jatkoaloitus, kaatua, kumota, uudelleenaloitus*

virheryöppy

en error burst

tiedonsiirrossa syntyvä virheiden kasautuma

▶ *syklinen ylimäärävarmistus*

virhetilanne

en error condition

viasta tai virheestä aiheutunut epänormaali tilanne tietokoneen, tietoverkon, käyttöjärjestelmän tai ohjelman toiminnassa

▲ *tilanne, virhe (1)* ▶ *toipuminen, vika, virhe (2)*

viruksentorjuntaohjelma

en virus protection software; anti-virus program ohjelma, joka pyrkii havaitsemaan tietokoneeseen tai datansiirtolaitteeseen tulleen viruksen tai muun tuholaisohjelman ja torjumaan sen

▲ *ohjelma, turvaohjelma ♣* ▶ *tietomurtohälytin, virus ♣, virustutka*

virus ♣

en computer virus; virus

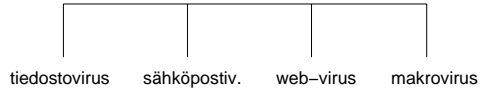
ohjelmaan tai dataan kätkeyty haittaohjelma, joka leviää tietokoneessa muihin ohjelmiin ja tietoverkossa muihin tietokoneisiin monistamalla itseään siten, että monistetut virukset edelleen monistuvat

Virusia on tuhansia lajeja, joista eräät paljastumisen vaikeuttamiseksi muuttavat jatkuvasti muotoaan. Viruksen ja madon ero: kts. *mato ♣*.

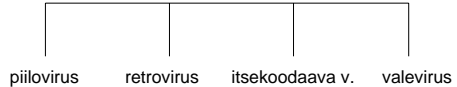
▲ *haittaohjelma ♣, monistuva ohjelma, tuholaisohjelma ♣* ▶ *bakteeri, epidemia, eristää, mato ♣, tartunta, troijanhevonen, viruksentorjuntaohjelma* ▼ *itsekoodaava virus, käynnistyslohkovirus, lataus, liipaisin, loisohjelma, makrovirus, piilovirus, retrovirus, sähköpostivirus, tiedostovirus, valevirus, web-virus*

Virustyyppiä

leviämistavan mukaan



toimintatavan mukaan



virustutka

en virus scanner

ohjelma, jonka tarkoituksena on havaita ja eristää tietokoneeseen tunkeutuneet virukset ja madot

▲ *turvaohjelma ♣* ▶ *monitori, seurain, tietomurtohälytin, viruksentorjuntaohjelma*

virusvalhe

en virus hoax

aiheeton, yleensä pelottelu- tai häirintätarkoituksessa lähetetty virusvaroitus

▶ *disinformaatio, valevirus, virusvaroitus*

virusvaroitus

en virus alert

tietoverkon turvallisuudesta huolehtivan viranomaisen tai muun luotettavan tahon lähettämä viesti, jossa käyttäjiä varoitetaan liikkeellä olevasta viruksesta

▲ *tietoliikenneturvallisuus* ▶ *CERT, haittaohjelma ♣, tietomurtohälytin, virusvalhe*

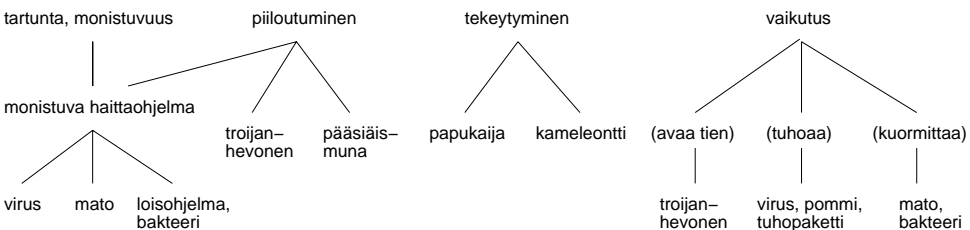
VIRVE

viranomaisverkko

Suomen turvallisuus-, pelastus- ja terveydenhoitoviranomaisten yhteinen valtakunnallinen TETRA-standardia käyttävä matkaviestintäverkko

▲ *viranomainen* ▶ *TETRA*

Haitta- ja tuholaisohjelmia jonkin ominaispiirteensä mukaan



VPDN

virtual private dial-up network

Internet-verkkoon tarvittaessa muodostettava yksityisverkko, jonka välityksellä etäkäyttäjät voivat saada valintayhteyden organisaation palvelimeen

▲ *Internet* ► *yksityisverkko*

VPN-verkko

en virtual private network

avoimeen verkkoon tiettyjen käyttäjien välille muodostettu suljettu aliverkko, jonka sisäinen liikenne on suojattu avoimen verkon muilta käyttäjiltä

▲ *tietoverkko* ♣, *verkko* ♣ ► *palomuri* ♣, *suljettu verkko*, *yksityisverkko*

VRK

Väestörekisterikeskus

Väestörekisterikeskus on muiden tehtäviensä ohella myös valtionhallinnon varmennusviranomaisen

▼ *kansalaisvarmenne*

välikohtaus

kts. *turvallisuushäiriö*

välipalvelin

en proxy (server)

tietoverkon ja paikallisen järjestelmän välissä oleva palvelin, joka voi toimia esimerkiksi tietojen hakua nopeuttavana välivarastona tallettamalla hakutuloksia välimuistiinsa, tai turvapalvelimena

▲ *palvelin* ► *NAT*, *palomuri* ♣, *turvapalvelin*

välistöhyökkäys

en man-in-the-middle attack

verkossa hyökkäys, jossa kahden viestijän väliin tunkeutuu näiden huomaamatta kolmas osapuoli, joka sieppaa viestit ja saattaa aiheuttaa vahinkoa muuttamalla tai poistamalla viestejä, urkkimalla salaussavaimia tai korvaamalla pyydetyn julkisen avaimen omalla julkisella avaimellaan

▲ *aktiivinen hyökkäys* ► *kaapata*, *tekeytyminen*

välivedos

en checkpoint record

ajon kestäessä otettu vedos mahdollista jatkoaloitusta varten

▲ *vedostaa* ► *jatkoalitus*

väsytyshyökkäys

en brute force attack

väsytystekniikkaa käyttävä hyökkäys

▲ *hyökkäys*, *väsytystekniikka* ► *kevyt salaus*, *sanakirjahyökkäys*

väsytystekniikka

en brute force technique; exhaustive search

kaikkien mahdollisten avainten tai salasanojen systemaattinen kokeilu salakirjoituksen avaamiseksi tai salasanan löytämiseksi

▲ *murtaa*, *salauksen ratkonta* ► *laskennallisesti murtovarma*, *murto-ohjelma* ▼ *väsytyshyökkäys*

W**Wassenaar-järjestely**

en Wassenaar arrangement

kansainvälinen sopimus kaksikäyttötuotteiden vientivalvonnan toimeenpanosta, johon Suomi on liittynyt

► *kaksikäyttötuote*

web-palvelin

en Web server

web-sivuja HTTP-käytännön mukaisesti selaimille toimittava ohjelma

▲ *palvelin*

web-selain

en Web browser

Internet-verkon käyttäjän verkkoasemassa oleva selain, joka noutaa, tulkitsee ja esittää web-sivuja ja valvoo sovelmien suoritusta

► *sovelma*

web-suodatin

en Web filter

ohjelma, joka rajoittaa pääsyä web-osoitteisiin tai -palveluihin annettujen kriteerien mukaisesti tai estää tietynlaisten sivujen näytön

▲ *suodatin* ► *pakettisuodatin*, *PICS*, *roskapostisuodatin*

web-vastaava

en webmaster

henkilö, joka huolehtii web-palvelujen, web-sivustojen ja palvelinohjelmien ylläpidosta

▲ *hallinta*, *vastaava* ► *verkkovastaava*

web-virus

en Web virus

virus, joka tarttuu selaimen käyttäjän käydessä saastuttavalla web-sivulla

▲ *virus* ♣ ► *sähköpostivirus*, *tiedostovirus*

WEP

Wired Equivalent Privacy

standardoitu langattoman verkon yhteyskäytäntö, joka salakirjoitusta käyttämällä pyrkii lankaverkon tarjoamaan tietoturvallisuuden tasoon

▲ *turvakäytäntö*, *yhteyskäytäntö*

Windows-pommi

en blue bomb; WinNuke

viesti, joka aiheuttaa vastaanottavan verkkoase-
man Windows-järjestelmän kaatumisen

▲ *pommi* ► *tuhopaketti*

WP 29

Working Party 29

Euroopan Unionin henkilötietodirektiivin
(2002/58/EC) mukainen kansallisista tietosuoja-
viranomaisista koostuva asiantuntijaelin

▲ *järjestö* ► *EESSI, tietosuojavaikuttettu, WPISP*

WPISP

Working Party on Information Security and Pri-
vacy

OECD:n tietotekniikkakomitean työryhmä, jonka
tehtäväalueena ovat tietoturvallisuus ja tietosuoja

▲ *järjestö* ► *salakirjoituspolitiikka, WP 29*

WPKI

wireless PKI

langaton julkisen avaimen järjestelmä

▲ *PKI*

X

X.509

ITU:n suositus menetelmistä ja tukipalveluista,
joiden avulla voidaan toteuttaa julkisen avaimen
järjestelmän mukaisia varmenne-, todennus- ja
muuta tietoturvaa lisääviä palveluja

▲ *julkisen avaimen järjestelmä*

Y

yhdistelmäsalaus

en hybrid encryption

salakirjoitus, jossa käytetään osin symmetristä ja
osin epäsymmetristä salakirjoitusta

▲ *salaus* ► *epäsymmetrinen salaus, symmetri-
nen salaus ♣*

yhteispalvelupiste

en joint service point

paikka, jossa on tarjolla kahden tai useamman
viranomaisen palveluja

▲ *palvelu, sähköinen asiointi, viranomainen*
► *toiminto-osoite*

yhteys

▼ *esto, etäyhteys, eväste, käytäntö, piiloyhteys*

yhteysavain

kts. *kerta-avain*

yhteykäytäntö

en communication protocol

säännöstö, joka määrittelee datayhteydellä käy-
tettävät yhteydenpitotavat, koodin sekä siirto-,
ohjaus- ja toipumismenettelyt

▲ *käytäntö* ► *avoin verkko, turvakäytäntö*
▼ *FTPS, IDAP, SSH, SSL, SSMTP, TLS, WEP*

yksilöidä

en identify

sama kuin *tunnistaa*

► *leimata* ▼ *henkilötunnus, tunnistus, tunnus*

yksinkertainen tunnistus

kts. *kevyt tunnistus*

yksisuuntainen salausalgoritmi

en one-way encryption algorithm

salausalgoritmi, jolle ei ole tunnettua avausalgo-
ritmia

Algoritmin käyttö perustuu salaustulosten vertai-
luun.

▲ *avata (2), salausalgoritmi*

yksityinen avain

en private key

epäsymmetrisessä salauksessa, esimerkiksi jul-
kisen avaimen menetelmässä käyttäjälle kuulu-
vasta avainparista se avain, jonka hän pitää hal-
lussaan ja salassa

▲ *avain, epäsymmetrinen salaus, julkisen avai-
men menetelmä ♣, salausavain ♣* ► *julkisen*
avain, salainen avain

yksityisverkko

en private network

käyttävän yhteisön omassa hallinnassa oleva tie-
toverkko

▲ *tietoverkko ♣, verkko ♣* ► *avoin verkko, oma-
verkko, suljettu verkko, VPDN, VPN-verkko*

yksityisyyden loukkaus

en infringement of privacy; privacy violation

yksityisyyden suojaa koskevien oikeuksien vas-
tainen toiminta

▲ *loukkaus, oikeudenloukkaus, yksityisyys* ► *ar-
kaluonteinen tieto, tietosuoja ♣*

yksityisyyden suoja

en privacy protection

Suomen perustuslain 10 §:ssä suojattu oikeushy-
vä

▲ *yksityisyys* ▼ *henkilötietolaki*

yksityisyys

en privacy

1) luonnollisen henkilön oikeus tai käytännön mahdollisuus suojautua ulkopuoliselta puuttumiselta

2) oikeus tai käytännön mahdollisuus määrätä itseään koskevien henkilötietojen käytöstä

3) oikeus tulla arvioituksi oikeiden ja oleellisten henkilötietojen perusteella

Suomessa yksityisyyttä suojaavia säädöksiä on erityisesti henkilötietolaissa ja rikoslain 24 luvussa.

▲ *oikeus, ominaisuus* ▶ *arkaluonteinen tieto, henkilötunnus, luottamuksellisuus* ▼ *yksityisyyden loukkaus, yksityisyyden suoja*

ylikuuluminen

en crosstalk

tiedon tarkoittamaton jäljentyminen kanavalta toiselle

▶ *salakuuntelu*

ylimäärä

en redundancy

pienimmän tarvittavan ylittävä laitteiden tai tiedon esityksen alkiodien määrä

▲ *varmistus (2)* ▶ *ylivuoto* ▼ *ylimäärävarmistus*

ylimäärävarmistus

en redundancy checking

ylimäärän käyttö vikojen tai virheiden vaikutuksen vähentämiseksi

▲ *ylimäärä* ▶ *jakojäännösvarmistus, kaikuvarmistus* ▼ *syklinen ylimäärävarmistus*

ylin varmentajakts. *varmennusorganisaatio*

▲ *varmentaja* ▶ *juurivarmenne*

ylivuoto

en overflow

1) virhe (1), joka syntyy luvun itseisarvon ylittäessä käytettävän esitystarkkuuden salliman suurimman arvon

2) virhe, joka syntyy kun ohjelma yrittää tallentaa muistialueeseen enemmän tietoa kuin tiedolle varattu muistitila sallii

▲ *virhe (1)* ▶ *muistivuoto, ylimäärä*

ylläpidettävyys

en maintainability

(järjestelmään, suunnitelmaan, tietokantaan, laitteistoon) sisäänrakennettu mahdollisuus tehdä joustavasti muutoksia ja lisäyksiä

▲ *ominaisuus, ylläpito*

ylläpito

en maintenance

tarpeelliseksi havaittujen muutosten tai korjausten tekeminen (ohjelmaan, järjestelmään, tiedostoon, sanastoon)

▲ *käytettävyys (1)* ▶ *eheys, huolto (1), käyttöturvallisuus, turmeltuminen, verkonhallinta* ▼ *systemin kunnossapito, ylläpidettävyys*

yrittysalaisuus

en business secret

yrittäjän toimintaan liittyvä asiakirja, suunnitelma tai muu tieto, jonka joutuminen ulkopuoliselle saattaa aiheuttaa vahinkoa yrittäjälle

▲ *salaisuus* ▶ *luottamuksellisuus, yrittäjävakoilu*

yrittäjävakoilu

en business espionage

yrittäjän luottamuksellisuutta pitämien tietojen oikeudeton hankkiminen tai jäljentäminen, esimerkiksi tunkeutumalla ulkopuolisilta suojattuun yrittäjän tietojärjestelmään

Rikoslain 30:4 § koskee yrittäjävakoilun rangaistavuutta.

▲ *oikeus, tietorikos* ▶ *Echelon, (käyttäjän) manipulointi, paljastus, tiedustelu, urkintatekniikka, yrittäjäsalaisuus*

Ä**älykortti**kts. *toimikortti***äänentunnistus**

en voice recognition

henkilön automaattinen tunnistaminen hänen äänensä ja puhetapansa perusteella

▲ *biotunnistus, tunnistaa (2), tunnistus* ▶ *puheentunnistus, puhujan tunnistus, salasanatunnistus*

ENGLANTI–SUOMI -SANASTO

A

abend virhelopetus

▶ *abort (s), abort (v), checkpoint restart, crash, restart*

abort (s) virhelopetus

▶ *abend, checkpoint restart, crash, restart*

abort (v) kumota

▶ *abend*

abuse

▼ *computer abuse, data abuse*

accept hyväksyä

▶ *validate*

acceptance test hyväksymistarkastus

▶ *accreditation, assessment, evaluation (1)*

access (s) pääsy

▲ *information system* ▶ *availability, cracking, data trespass, public* ▼ *access control, accessibility, lawful access, remote access, right of access, trap door*

access authority käsittelyvaltuus

▲ *authorization, usage rights* ▶ *access right*

access control pääsynvalvonta

▲ *access (s), control (1), information security, supervision* ▶ *access right, piggybacking, tailgating* ▼ *access control software, passage control, physical access control*

access control software pääsynvalvontaohjelmisto

▲ *access control, software, user*

access provider yhteyspalvelun tuottaja

access right käyttöoikeus; pääsyvaltuus

▲ *right, use, utilization* ▶ *access authority, access control, authority, authorization, usage rights* ▼ *reference monitor*

accessibility saavutettavuus

▲ *access (s), property* ▶ *availability, network scan, reliability*

accountability tilivelvollisuus

▶ *audit (s)*

accreditation akkreditointi

▲ *trusted (third) party* ▶ *acceptance test, assessment, authorization, certification, evaluation (1), validation*

accreditation scheme akkreditointijärjestelmä

▲ *certificate authority, public key infrastructure* ▶ *certification hierarchy*

accuracy oikeellisuus

▲ *property* ▶ *anomaly, integrity, modulo N checking, reliability, residue checking, validity* ▼ *error, revise, verify*

acknowledgement kuittaus

▶ *confirmation*

act

▼ *Act on Electronic Commerce, Act on Online Government Services, Act on Privacy in Telecommunications, Act on the Openness of Government Activities, Archives Act, Coercive Measures Act, Communications Market Act, Electronic Signatures Act, Emergency Powers Act, Personal Data Act*

Act on Electronic Commerce verkkokauppalaaki

▲ *act, computer law* ▶ *Act on the Openness of Government Activities*

Act on Online Government Services verkkoasiointilaki

▲ *act, computer law* ▶ *electronic government, online government*

Act on Privacy in Telecommunications televiestinnän tietosuojalaki

▲ *act, computer law, information security, information security law* ▶ *Communications Market Act, extraordinary circumstances*

Act on the Openness of Government Activities julkisuuslaki

▲ *act, computer law* ▶ *Act on Electronic Commerce, (public) authority, privacy law* ▼ *classified information*

active attack aktiivinen hyökkäys

▲ *attack* ▶ *passive attack* ▼ *crack, cracking, data driven attack, data trespass, DoS attack, impersonation, leapfrog attack, man-in-the-middle attack, masquerading, saturation attack, spoofing*

address hijacking osoitteen kaappaus

▲ *cybercrime, hijacking, network crime* ▶ *impersonation, masquerading, session hijacking, spoofing*

administrative and organizational information security hallinnollinen tietoturvallisuus

▲ *information security* ▶ *data security, software security*

administrative domain verkkoalue

▲ *information network* ▼ *domain name, naming authority*

administrator pääkäyttäjä (1)

▶ *authorized user, superuser* ▼ *network administrator, system administrator*

agreement

▼ *backup system agreement, key agreement protocol, nondisclosure agreement*

AH *authentication header*
todennusnimiö

algorithm algoritmi
▼ *compression function, encryption algorithm, hash function, one-way encryption algorithm*

alternate route varareitti
▲ *contingency plan*

analysis
▼ *cryptanalysis, forensic, risk analysis, threat analysis, vulnerability analysis*

ankle biter alokasurtautuja
► *cracker, script kiddie*

anomaly poikkeavuus
► *accuracy, security incident*

anonymity server anonyymipalvelin
▲ *server* ► *unidentified use*

anonymous file transfer anonyymi tiedoston-siirto

anonymous FTP anonyymi FTP

anonymous use anonyymikäyttö
▲ *identification, recognition, use* ► *anonymous user identity, unidentified use* ▼ *anonymous user ID*

anonymous user ID anonyymitunnus
▲ *anonymous use, user ID* ► *pseudonym*

anonymous user identity nimimerkki
▲ *identifier, identity, user* ► *anonymous use*

anti-virus program viruksentorjuntaohjelma
▲ *program, security monitor, tiger* ► *computer virus, intrusion detection system, virus, virus protection software, virus scanner*

applet sovelma
► *Web browser*

archive (s) arkisto
► *data, document, material* ▼ *backup archive, security archive, working archive*

Archives Act arkistolaki
▲ *act, data security*

assessment arviointi
► *acceptance test, accreditation, audit (s), evaluation (1), information security norm, quality, review (s)* ▼ *certify*

assurance
▼ *information security assurance, technical assurance*

assure varmistaa
► *authenticate, ensure, information security assurance, safeguard, seal (v), verify* ▼ *audit trail, backup, backup copy, call-back (1), check symbol, checking, control (2), dump (v), duplex (v), error control*

asymmetric encryption epäsymmetrinen salaus

▲ *encryption* ► *hybrid encryption, symmetric encryption* ▼ *elliptical curve cryptography, private key, public key, public key method*

asynchronous stream cipher itsetahdistava jonosalaus

▲ *stream cipher* ► *synchronous stream cipher*

attack hyökkäys

▲ *computer abuse, computer crime, information system* ► *bastion host, corruption, intrusion, penetration, perpetrator, secure host, spyware*
▼ *active attack, brute force attack, data driven attack, dictionary attack, DoS attack, impersonation, IP spoofing, masquerading, MITMA, passive attack, saturation attack, spoofing, war dialing, war driving*

audit (s) tarkastus (2); tilintarkastus

► *accountability, assessment, control (1), evaluation (1), inspection, review (s), supervision, trusted (third) party* ▼ *auditor, information audit, systems audit*

audit (v) tarkastaa (2)
▼ *auditability*

audit trail kirjausketju

▲ *assure, back up, check (v), ensure, inspect, secure (v), trail* ► *integrity, traceability*

auditability tarkastettavuus

▲ *audit (v), property* ► *checking, error control, identifiability, reliability, repeatability, traceability, verifiability*

auditor tarkastaja; tilintarkastaja

▲ *audit (s), check (v), inspect* ▼ *systems auditor*

authenticate todentaa

► *assure, back up, check (v), ensure, secure (v), verify* ▼ *authentication, verifiability, verification*

authentication todennus

▲ *authenticate, verify* ► *certification, identification, introduction, log-in, password, recognition, sign-on, testing, verification* ▼ *challenge-response method, credential(s), password identification, signature (1), strong authentication, token, weak authentication*

authentication data todennustiedot

▲ *data, identification, recognition* ► *challenge-response method*

authentication key todennusavain

▲ *key* ► *dual use key*

authentication server notaaripalvelin

▲ *network notary, security server, server* ▼ *time stamp server*

authenticity aituus

▲ *property* ► *certificate, challenge-response method, credential(s), identification, integrity, nonrepudiation, recognition, validity*

authority valtuus

▲ use, utilization ▶ access right, authorization, system owner ▼ authorization, authorization terminal, authorized user, certificate authority, credential(s), master card, reference monitor, smart key, usage rights

(public) authority viranomainen

▶ Act on the Openness of Government Activities, norm, trusted (third) party ▼ certificate authority, data protection ombudsman, electronic government, naming authority, official document, online government, privacy commissioner

authorization käyttövaltuudet; valtuutus

▲ authority ▶ access right, accreditation, authority, usage rights, validation ▼ access authority, unauthorized user

authorization terminal varmennuspäätte

▲ authority, secure device, trusted device

authorize oikeuttaa; valtuuttaa

▶ certify ▼ unauthorized

authorized user valtuutettu käyttäjä

▲ authority, user ▶ administrator, root, superuser, unauthorized user

availability käytettävyys (1)

▲ property, quality, use, utilization ▶ access (s), accessibility, information security, management, operation(s), protection, reliability, robustness, serviceable, usability ▼ back up, backup, backup copy, backup file, backup hardware, backup site, backup system, bypass procedure, check (v), contamination, contingency planning, continuity plan, corruption, crash, denial of service, deny, downtime, failure, fallback system, fault, fault threshold, fault tolerant, go down, hazard, information security risk, inhibit, interference, maintenance, malfunction, no-break power supply, recovery, recovery plan, resilient, resistant, secure (v), security of supply, service, standby, threat, unavailability, uninterrupted power supply, watchdog timer

B

back door takaportti

▶ entrap, trap door

back up varmistaa

▲ availability, reliability ▶ authenticate, check (v), information security assurance, inspect, monitor (v), revise, seal (v), secure (v), supervise, verify ▼ audit trail, backup, backup copy, call-back (1), check symbol, checking, control (2), dump (v), duplex (v), error control

backup varmuuskopio; varmuuskopiointi

▲ assure, availability, back up, backup copy, check (v), ensure, secure (v) ▶ backup archive, backup copy, safety copy, standby ▼ backup file, IT backup

backup archive varmuusarkisto

▲ archive (s) ▶ backup, backup copy, security archive, working archive

backup copy varmuuskopio

▲ assure, availability, back up, check (v), copy, ensure, secure (v) ▶ backup, backup archive, safety copy ▼ backup, backup file

backup file varmistustiedosto

▲ availability, backup, backup copy ▶ mirror database

backup hardware varalaitteisto

▲ availability ▶ backup site, backup system agreement, contingency plan, standby

backup premises varatila

▶ backup site

backup site varakeskus

▲ availability, IT backup ▶ backup hardware, backup premises, backup system agreement, contingency plan ▼ cold site

backup system varajärjestelmä

▲ availability, information system, IT backup, reliability, system ▶ failure, fallback system, malfunction

backup system agreement varakonesopimus

▲ agreement, contingency plan ▶ backup hardware, backup site

bacterium (pl bacteria) bakteeri

▲ replicator, rogue program ▶ computer virus, flooding, memory leak, parasite, parasitic virus, virus, worm

bandwidth throttling kuormanrajoitus

baseline security perusturvallisuus

▲ information security, security ▶ extraordinary circumstances, information security plan ▼ level C security

bastion host verkkolinnake

▲ host ▶ attack, robustness, secure host, vulnerability

be compromised vaarantua

▲ compromise (v) ▶ control failure, security incident

be contaminated saastua

▶ quarantine (v)

biometric identification biotunnistus

▲ identification, recognize ▶ characteristic, electronic identification, feature, password identification ▼ speaker identification, speaker recognition, voice recognition

block cipher lohkosalaus

▲ *cipher, cryptography, encryption* ▶ *stream cipher* ▼ *symmetric block cipher*

blue bomb Windows-pommi

▲ *bomb* ▶ *ping of death, WinNuke*

bomb pommi

▲ *malicious program, rogue program* ▶ *crash, ping of death* ▼ *blue bomb, letter bomb, logic bomb, mail bombing, time bomb*

boot sector virus käynnistyslohkovirus

▲ *virus*

breach (s) aukko; murto

▶ *infringement, intrusion* ▼ *security breach*

breach (v) murtaa

▶ *break (v), crack, decipher, decrypt* ▼ *brute force technique, exhaustive search*

break (v) murtaa

▶ *breach (v), crack, decipher, decrypt* ▼ *brute force technique, exhaustive search*

brute force attack väsytyshyökkäys

▲ *attack, brute force technique, exhaustive search* ▶ *dictionary attack, weak encryption*

brute force technique väsytystekniikka

▲ *breach (v), break (v), crack, cryptanalysis, technique* ▶ *computationally secure, cracker, cracking program, exhaustive search* ▼ *brute force attack*

bug vika; virhe

▶ *error* ▼ *debug, debugging, Web bug*

business espionage yritysvakoilu

▶ *business secret, illegal disclosure, intelligence (2), social engineering, spyware*

business secret yrityssalaisuus

▲ *secret (s)* ▶ *business espionage, confidentiality*

bypass procedure ohitusmenettely

▲ *availability* ▶ *recovery procedure*

C

C2W *command and control warfare* johtamissodankäynti

▶ *information warfare*

CA *certificate authority*

varmentaja; varmenneviranomainen

call-back (1) vastakutsu

▲ *assure, back up, check (v), ensure, remote access, remote login, secure (v)* ▶ *challenge-response method*

card

▼ *chip card, electronic identity card, identification card, master card, smart card*

case processing asiankäsitely

▶ *workflow*

catastrophe katastrofi

▲ *failure, malfunction* ▶ *disaster, exceptional situation, extraordinary circumstances, recovery plan* ▼ *disaster resistant*

copyrightware suodatusohjelma

▲ *filter, ware*

certificate turvallisuustodistus; varmenne

▲ *information security, public key infrastructure, trusted (third) party* ▶ *authenticity, check symbol, electronic government, electronic identification, online government, stamp (s)* ▼ *certificate authority, certification, cross-border recognition of certificates, digital signature, multiple certificate environment, personal certificate, PKI certificate, public key certificate, qualified certificate, revocation list, root certificate, server certificate*

certificate administration varmennehallinto

▲ *certificate authority, public key infrastructure* ▶ *certification hierarchy, certification service, lawful access* ▼ *escrow*

certificate authority varmentaja

▲ *authority, (public) authority, certificate, public key infrastructure* ▶ *certificate directory, key distribution center, trusted (third) party* ▼ *accreditation scheme, certificate administration, certification hierarchy, certification service*

certificate directory varmennehakemisto

▶ *certificate authority, directory service*

certificate path varmennepolku

certificate policy varmennepoliittikka

▲ *information security policy* ▶ *cryptography policy*

certification varmentaminen

▲ *certificate, computer law* ▶ *accreditation, authentication, control (2), electronic signature, stamp (v), verification* ▼ *certification service*

certification hierarchy varmennusorganisaatio

▲ *certificate authority* ▶ *accreditation scheme, certificate administration* ▼ *multiple certificate environment, root certificate*

certification service varmennepalvelu

▲ *certificate authority, certification, service* ▶ *certificate administration* ▼ *multiple certificate environment*

certify sertifioida; todistaa

▲ *assessment, evaluation (1)* ▶ *authorize, validate*

challenge-response method haastemenetelmä

▲ *authentication, verification* ▶ *authentication data, authenticity, call-back (1), passphrase, password identification*

chameleon kameleontti

▲ *malicious program, rogue program* ▶ *self-encrypting virus, self-garbling virus*

characteristic tuntomerkki

▲ *identification, recognition* ▶ *biometric identification, feature, identifier, label, stamp (s)*

check (s) tarkastus (1); varmistus (2)

▲ *security* ▶ *checking, inspection* ▼ *cyclic redundancy checking, error-checking code, error-detecting code, redundancy*

check (v) tarkastaa (1); varmistaa

▲ *availability, error, integrity, mistake, reliability, validity* ▶ *authenticate, back up, information security assurance, inspect, monitor (v), revise, seal (v), secure (v), supervise, test (v), testing, verify* ▼ *audit trail, auditor, backup, backup copy, call-back (1), check symbol, checking, control (2), dump (v), duplex (v), error control, right to inspect, self-checking code*

check(mark) rastitus

▶ *checking, inspection* ▼ *cyclic redundancy checking*

check bit varmistusbitti

▲ *check symbol*

check character varmistusmerkki

▲ *check symbol*

check digit varmistusnumero

▲ *check symbol*

check(ing) sequence varmistus

▶ *check symbol*

check symbol varmistus

▲ *assure, back up, check (v), ensure, secure (v)* ▶ *certificate, check(ing) sequence, hash value, message digest, mistake, seal (s)* ▼ *check bit, check character, check digit, checksum, proof total*

checking varmistus (2)

▲ *assure, back up, check (v), ensure, secure (v)* ▶ *auditability, check (s), check(mark), error control* ▼ *echo checking, error-checking code, error-detecting code, modulo N checking, redundancy, redundancy checking, residue checking*

checkout testaus

▶ *testing*

checkpoint varmistuskohta

▲ *operation(s)*

checkpoint record välivedos

▲ *dump (v)* ▶ *checkpoint restart*

checkpoint restart jatkoaloitus

▲ *operation(s)* ▶ *abend, abort (s), checkpoint record, rerun, restart*

checksum varmistussumma

▲ *check symbol* ▶ *proof total*

chip card toimikortti

▲ *card* ▶ *smart card, smart key* ▼ *electronic identity card, master card*

CIIP *critical information infrastructure protection* yhteiskunnan elintärkeiden tietoteknisten perusrakenteiden suojaaminen

▲ *II*

CIP *critical infrastructure protection*

yhteiskunnan elintärkeiden perusrakenteiden suojaaminen

cipher salakirjoitusmenetelmä

▲ *cryptology* ▼ *block cipher, decipher, deciphering, stream cipher*

ciphertext salateksti

▲ *cryptography, encryption, text* ▶ *clear text, encrypted text, plaintext*

CISA *Certified Information Systems Auditor*

kansainvälisesti hyväksytty atk-tarkastaja

classification luokitus

▲ *classify* ▶ *taxonomy* ▼ *priority classification, security classification*

classification of data tietojen luokitus

▲ *data, data security, information security* ▶ *public* ▼ *priority classification, secret (a), security classification*

classified information turvaluokiteltava tieto

▲ *Act on the Openness of Government Activities, data, material, security classification* ▶ *secret (a)*

classify luokitella

▼ *classification, security classification, taxonomy*

clear text selväkieliteksti

▲ *text* ▶ *ciphertext, cryptography, encrypted text, encryption, plaintext*

closed network suljettu verkko

▲ *network* ▶ *open network, private network, virtual private network* ▼ *local area network*

code koodi

▶ *cryptography, key, password* ▼ *country code, decode, error-checking code, error-correcting code, error-detecting code, PIN code, self-checking code*

code of conduct eettiset ohjeet

▲ *rule* ▶ *code of ethics, computer abuse, norm*

code of ethics eettiset ohjeet

▲ *rule* ▶ *code of conduct, computer abuse, norm*

coded representation koodiesitys

Coercive Measures Act pakkokeinolaki

▲ *act, computer law* ► *control (1), lawful interception, remote surveillance, supervision, telemonitoring, (legal) wiretapping*

cold site kylmä varakeskus

▲ *backup site*

collapse kaatua

► *go down*

command-and-control warfare johtamisso-dankäynti

▲ *control (1), cyberwarfare, information warfare, warfare* ► *electronic warfare*

commandeer kaapata

► *distributed denial of service attack, hijack, impersonation, intercept, man-in-the-middle attack, masquerading, spoofing, theft of identity* ▼ *cybersquatting, zombie*

communication protocol yhteyskäytäntö

▲ *protocol* ► *open network, security protocol*

communications crime viestintärikos

▲ *crime* ► *computer crime, cybercrime, network crime, telecommunications security* ▼ *eavesdropping, wiretapping*

communications intelligence viestitiedustelu

▲ *intelligence (2), signals intelligence* ► *electronic intelligence*

Communications Market Act viestintämarkkinalaki

▲ *act, computer law* ► *Act on Privacy in Telecommunications* ▼ *telecommunications security*

compression function tiivistysfunktio

▲ *algorithm, hash value, message digest* ► *hash function*

compromise (s) vaarantuminen

▲ *information security*

compromise (v) vaarantaa

▲ *computer crime, hazard, threat* ► *risk* ▼ *be compromised*

computationally secure laskennallisesti murtovarma

► *brute force technique, cracker, cracking program, exhaustive search, key, strong encryption*

computer abuse tietotekniikan väärinkäyttö

▲ *abuse* ► *code of conduct, code of ethics, computer crime, data abuse* ▼ *attack*

computer crime tietotekniikkarikollisuus; tietotekniikkarikos

▲ *crime, infringement, violation of right* ► *communications crime, computer abuse, computer law, cybercrime, data abuse, infringement, network crime, violation of right* ▼ *attack, compromise (v), computer sabotage, computer-assisted forgery, computer-assisted fraud, cracking, data protection crime, data trespass, denial of service, interference, piracy, theft of identity*

computer law tietotekniikkaoikeus

▲ *law* ► *computer crime, information law* ▼ *Act on Electronic Commerce, Act on Online Government Services, Act on Privacy in Telecommunications, Act on the Openness of Government Activities, certification, Coercive Measures Act, Communications Market Act, copyright, copyright law, Electronic Signatures Act, information security law, Personal Data Act*

computer sabotage atk-sabotaasi

▲ *computer crime, damage, hazard, threat*

computer security laitteistoturvallisuus

▲ *information security, physical security, security* ► *data security, facilities security, software security, telecommunications security*

computer system tekninen tietojärjestelmä

▲ *system* ► *data processing system, employee monitoring*

computer virus virus

▲ *malicious program, replicator, rogue program* ► *anti-virus program, bacterium (pl bacteria), epidemic, infection, quarantine (v), Trojan horse, virus, virus protection software, worm* ▼ *parasite, parasitic virus, payload, trigger (s)*

computer-assisted forgery tietokoneavusteinen väärennys

▲ *computer crime* ► *document*

computer-assisted fraud tietokoneavusteinen petos

▲ *computer crime* ▼ *salami technique*

confidential luottamuksellinen

► *official document, public, (in the) public domain, restricted use, secret (a), security classification, sensitive data* ▼ *confidentiality, illegal disclosure*

confidentiality luottamuksellisuus

▲ *confidential, quality* ► *business secret, information security, integrity, privacy* ▼ *trusted (third) party*

confirmation kuittaus

► *acknowledgement*

congestion esto

► *data network, deny, fault, inhibit, suppress, unavailability* ▼ *DoS attack, saturation attack*

contamination saastuminen

▲ *availability* ► *corruption, damage, data tampering, infection, interference*

contingency plan varautumissuunnitelma

▲ *contingency planning* ► *backup hardware, backup site, continuity plan* ▼ *alternate route, backup system agreement, preparedness plan, recovery plan*

contingency planning varautuminen

▲ *availability, preparedness* ► *failure, malfunction* ▼ *contingency plan, preparedness planning*

continuity plan jatkuvuussuunnitelma

▲ *availability* ▶ *contingency plan, failure, information security plan, malfunction, security of supply, vital application* ▼ *preparedness plan, recovery plan*

control (1) ohjaus; valvonta

▲ *monitor (v), supervise* ▶ *audit (s), Coercive Measures Act, filtering, interference, lawful access, management, monitoring, rule, supervision, system owner* ▼ *access control, command-and-control warfare, control failure, information management, passage control, physical access control, quality control, remote surveillance, tele-monitoring*

control (2) varmistus (1)

▲ *assure, back up, check (v), ensure, secure (v)* ▶ *certification, revise* ▼ *error control, passage control*

control (v) tarkkailla; valvoa

▶ *monitor (v)* ▼ *data controller*

control failure valvontakatko

▲ *control (1), failure, supervision* ▶ *be compromised, security incident*

cookie eväste; kuitti

▶ *Web beacon*

copy

▼ *backup copy, pirate copy, safety copy*

copyright tekijänoikeus

▲ *computer law, information law, right* ▼ *copyright law, piracy, pirate copy*

copyright law tekijänoikeuslaki

▲ *computer law, copyright, law*

correct (v) korjata; oikaista

▶ *debug, test (v)* ▼ *error-correcting code*

corruption turmeltuminen

▲ *availability, integrity* ▶ *attack, contamination, data tampering, degradation, disk crash, fragmentation, head crash, maintenance*

country code maatunnus

▲ *code* ▶ *country domain name* ▼ *fi root*

country domain name maatunnus

▲ *domain name* ▶ *country code* ▼ *fi root*

covert channel piiloyhteys

▶ *trap door*

crack murtaa; murtautua

▲ *active attack* ▶ *breach (v), break (v), decipher, decrypt, hack (v), intrusion, penetration, piggybacking, tailgating* ▼ *brute force technique, cracker, cracking, cyberhacker, data trespass, exhaustive search*

cracker murtautuja; murto-ohjelma

▲ *crack, cracking, data trespass, intrusion, penetration* ▶ *ankle biter, brute force technique, computationally secure, cracking program, cyberhacker, dictionary attack, exhaustive search, hacker, perpetrator, phreaking, rogue program, root kit, samurai, script kiddie, security monitor, tiger, trap (s), white hat*

cracking tietomurto

▲ *active attack, computer crime, crack, information security breach* ▶ *access (s), data trespass, eavesdropping, hacking, impersonation, intrusion, intrusion detection system, masquerading, penetration, probe (s), spoofing, wiretapping* ▼ *cracker, cracking program, loophole, root kit, security breach, war dialing*

cracking program murto-ohjelma

▲ *cracking, data trespass, program* ▶ *brute force technique, computationally secure, cracker, dictionary attack, exhaustive search, rogue program, root kit, security monitor, tiger*

crash kaatua

▲ *availability, reliability* ▶ *abend, abort (s), bomb, fail soft (v), go down, nuke* ▼ *disk crash, head crash*

CRC *cyclic redundancy check*

syklinen ylimäärävarmistus

credential(s) valtuustieto

▲ *authentication, authority, verification* ▶ *authenticity*

credibility luotettavuus; uskottavuus

crime

▼ *communications crime, computer crime, cyber-crime, data protection crime, network crime*

cross-border recognition of certificates var-

menteiden vastavuoroinen hyväksyntä

▲ *certificate, recognition*

crosstalk ylikuuluminen

▶ *eavesdropping, wiretapping*

cruft ohjelmajäte

▶ *residual data, residue*

cryptanalysis salauksen ratkonta

▲ *analysis, cryptography, decipher, decrypt, encryption* ▶ *cryptology, deciphering, decryption* ▼ *brute force technique, dictionary attack, exhaustive search*

cryptographic key salausavain

▲ *cryptography, encryption, key* ▶ *dual use key, encryption algorithm, encryption key* ▼ *key escrow (system), key management, key recovery, keyholder, one-time key, private key, public key, secret key*

cryptography salakirjoitus; salaustekniikka
 ▶ *clear text, code, cryptology, dual use product, encrypt, encryption, information security technology, plaintext, security protocol, steganography*
 ▼ *block cipher, ciphertext, cryptanalysis, cryptographic key, cryptology, cryptoprocessor, cryptosystem, digital envelope, elliptical curve cryptography, encrypted message, encrypted text, encryption algorithm, encryption key, encryption product, forensic cryptography, steganography, stream cipher*

cryptography policy salakirjoituspolitiikka
 ▲ *information security policy* ▶ *certificate policy*
 ▼ *encryption product, escrow, key escrow (system)*

cryptology salaustutkimus
 ▲ *cryptography, encryption* ▶ *cryptanalysis, cryptography* ▼ *cipher*

cryptoprocessor salaussuoritin
 ▲ *cryptography* ▶ *encryption algorithm*

cryptosystem salausjärjestelmä
 ▲ *cryptography, system*

CSP *certification service provider*
 varmentaja, varmennepalvelujen tuottaja

cyber terrorism verkkoterrorismi
 ▲ *cybercrime, netwar, network crime, network-centric warfare*

cybercrime tietoverkkorikos
 ▲ *crime, information network* ▶ *communications crime, computer crime, network crime* ▼ *address hijacking, cyber terrorism, cybersquatting, eavesdropping, intercept, session hijacking, wiretapping*

cyberhacker murtautuja
 ▲ *crack, intrusion, penetration* ▶ *cracker, hacker, perpetrator, samurai, script kiddie, trap (s), white hat*

cybersquatting nimenvaltaus
 ▲ *commandeer, cybercrime, domain name, hijack, network crime* ▶ *domain name grabbing, unauthorized user*

cyberwarfare tietosodankäynti
 ▲ *warfare* ▶ *information warfare, vulnerability*
 ▼ *command-and-control warfare, disinformation, electronic warfare, information systems warfare, infrastructure warfare, interference, netwar, network-centric warfare, signals intelligence*

cyclic redundancy checking CRC-varmistus; syklinen ylimäärävarmistus
 ▲ *check (s), check(mark), redundancy, redundancy checking* ▶ *error burst*

D

damage vahinko
 ▶ *contamination, disclaimer, hazard, information security risk, infringement, physical security, risk, security archive, threat, violation of right* ▼ *computer sabotage*

data aineisto
 ▶ *archive (s), data security, material, pirate copy*
 ▼ *authentication data, classification of data, classified information, personal data, residual data, sensitive data, test data*

data abuse tietojen väärinkäyttö
 ▲ *abuse* ▶ *computer abuse, computer crime*
 ▼ *data diddling*

data controller rekisterinpitäjä
 ▲ *control (v)* ▶ *registrar*

data diddling tiedon peukalointi
 ▲ *data abuse* ▶ *data tampering*

data driven attack datapohjainen hyökkäys
 ▲ *active attack, attack* ▶ *macro virus, rogue program*

data haven tietovalkama
 ▶ *privacy protection, sensitive data*

data leakage tietovuoto
 ▲ *information risk* ▶ *data seepage, illegal disclosure*

data network dataverkko
 ▲ *net, network* ▶ *congestion, information network* ▼ *tunneling*

data processing system tekninen tietojärjestelmä
 ▲ *system* ▶ *computer system, employee monitoring*

data protection crime tietosuojarikos
 ▲ *computer crime, crime, privacy protection*

data protection law henkilötietolaki
 ▲ *law, privacy, protection*

data protection ombudsman tietosuojavaltuutettu
 ▲ *(public) authority, privacy protection, protection*
 ▶ *Personal Data Act, privacy commissioner*

data protection policy tietosuojapolitiikka
 ▲ *policy* ▶ *information security policy, privacy protection policy*

data protection software suojausohjelmisto
 ▲ *privacy protection, protection, software* ▶ *security architecture, security monitor, tiger*

data security aineistoturvallisuus

▲ *information security, security* ▶ *administrative and organizational information security, computer security, data, facilities security, material, software security* ▼ *Archives Act, classification of data*

data seepage tietovuoto

▲ *information risk* ▶ *data leakage, illegal disclosure*

data subject rekisteröity

▲ *person register* ▶ *register object, right to inspect*

data tampering tiedon peukalointi

▲ *interference, tamper* ▶ *contamination, corruption, data diddling, forge, integrity*

data trespass tietomurto

▲ *active attack, computer crime, crack, information security breach* ▶ *access (s), cracking, eavesdropping, hacking, impersonation, intrusion, intrusion detection system, masquerading, penetration, probe (s), spoofing, wiretapping* ▼ *cracker, cracking program, loophole, root kit, security breach, war dialing*

DDoS *distributed denial of service*

hajautettu palvelunestohyökkäys

▲ *DoS*

debug korjata virheet; perata

▲ *bug* ▶ *correct (v)*

debugging perkaus

▲ *bug, mistake* ▶ *test (v), testing*

decipher avata (2)

▲ *cipher, encrypt* ▶ *breach (v), break (v), crack, decrypt* ▼ *cryptanalysis, deciphering, decryption, one-way encryption algorithm*

deciphering koodin avaaminen

▲ *cipher, decipher, decrypt* ▶ *cryptanalysis, decryption*

decode avata (1)

▲ *code*

decoy syötti; täky

▶ *trap (s)*

decrypt avata (2)

▲ *encrypt* ▶ *breach (v), break (v), crack, decipher* ▼ *cryptanalysis, deciphering, decryption, one-way encryption algorithm*

decryption koodin avaaminen

▲ *decipher, decrypt* ▶ *cryptanalysis, deciphering*

defensive information security puolustautuva tietoturvallisuus

▲ *information security, information security policy* ▶ *proactive information security*

defragment eheyttää

▶ *fragmentation, memory leak*

degradation rappeutuminen; taantuminen

▶ *corruption*

demilitarized zone harmaa vyöhyke

▶ *extranet, firewall, partnernet*

denial of service palvelun esto

▲ *availability, computer crime, service* ▶ *deny, inhibit, unavailability* ▼ *distributed denial of service attack*

deny estää

▲ *availability* ▶ *congestion, denial of service, inhibit, suppress*

derf salakäyttö

▶ *unauthorized user, war driving*

desk checking pöytätestaus

▲ *testing*

diagnostic (a) vianmääritys-; virheenmääritys-

dictionary attack sanakirjahyökkäys

▲ *attack, cryptanalysis* ▶ *brute force attack, cracker, cracking program*

digital certificate varmenne

digital envelope salauskuori

▲ *cryptography, encryption*

digital fingerprint piiloleima

▲ *steganography* ▶ *digital watermark, pirate copy*

digital signature digitaalinen allekirjoitus

▲ *certificate, signature (1)* ▶ *electronic signature, qualified certificate, seal (s), secure e-mail*

digital watermark piiloleima

▲ *steganography* ▶ *digital fingerprint, pirate copy*

DII *Defense Information Infrastructure*

USA:n puolustusvoimain tietojärjestelmä

▲ *II*

directory service hakemistopalvelu

▲ *network service, service* ▶ *certificate directory, public key infrastructure* ▼ *revocation list*

disaster katastrofi

▲ *failure, malfunction* ▶ *catastrophe, exceptional situation, extraordinary circumstances, recovery plan* ▼ *disaster resistant*

disaster resistant katastrofisietoinen

▲ *catastrophe, disaster, resistant* ▶ *fault tolerant, resilient, resistant*

disclaimer vastuunrajausilmoitus

▶ *damage, legal notice, privacy statement*

disclosure

▼ *illegal disclosure, nondisclosure agreement*

discretionary access control harkinnanvarainen pääsynvalvonta

disinformation disinformaatio

▲ *cyberwarfare, information warfare* ▶ *impersonation, masquerading, spoofing, virus hoax*

disk crash levyrikko

▲ *crash, fault* ▶ *corruption, head crash*

distributed denial of service attack hajautettu palvelunestohyökkäys

▲ *denial of service* ▶ *commandeer, hijack, leapfrog attack, zombie*

DMZ demilitarized zone

harmaa vyöhyke

document asiakirja

▶ *archive (s), computer-assisted forgery, log (s)*
▼ *electronic document, official document*

domain name verkkotunnus

▲ *administrative domain* ▼ *country domain name, cybersquatting, domain name grabbing, fi root*

domain name grabbing verkkotunnuksen kaappaus

▲ *domain name* ▶ *cybersquatting*

dongle tonkeli

▲ *security module* ▶ *hardware key, key chip, smart key* ▼ *USB key*

DoS denial of service

palvelun esto

▼ *DDoS*

DoS attack palvelunestohyökkäys

▲ *active attack, attack, congestion, rogue program* ▶ *flooding, interference, ping of death, saturation attack* ▼ *mail bombing*

downtime häiriöaika

▲ *availability*

dual use key kaksikäyttöavain

▲ *key* ▶ *authentication key, cryptographic key, encryption key*

dual use product kaksikäyttötuote

▲ *encryption product* ▶ *cryptography, encryption algorithm, Wassenaar arrangement*

due care principle huolellisuusperiaate

dump (v) vedostaa

▲ *assure, back up, check (v), ensure, secure (v)*
▶ *duplex (v), mirror (v), replicate* ▼ *checkpoint record*

dumpster diving pengonta

▲ *intelligence (2)* ▶ *residual data, residue, scavenging, shredder, spyware*

duplex (v) kahdentaa

▲ *assure, back up, check (v), ensure, secure (v)*
▶ *dump (v), mirror (v), replicate*

dynamic password dynaaminen salasana

▲ *password* ▶ *session key*

E

e-mail virus sähköpostivirus

▲ *virus* ▶ *file infector virus, macro virus, Web virus*

eavesdropping salakuuntelu

▲ *communications crime, cybercrime, intelligence (2), network crime, spyware* ▶ *cracking, crosstalk, data trespass, employee monitoring, intercept, key logger, lawful interception, probe (s), remote surveillance, telemonitoring, wiretapping, (legal) wiretapping*

echo checking kaikuvarmistus

▲ *checking* ▶ *feedback error control, modulo N checking, redundancy checking, repeater, residue checking*

electromagnetic pulse sähkömagneettinen pulssi

▲ *electronic warfare* ▶ *high energy laser, high power microwave weapon, scattered electromagnetic radiation*

electronic commerce verkkoasiointi

▲ *network service* ▶ *public key infrastructure*
▼ *front end system, multi-use smart card*

electronic document sähköinen asiakirja

▲ *document* ▶ *electronic signature*

electronic government hallinnon sähköinen asiointi

▲ *(public) authority* ▶ *Act on Online Government Services, certificate, online government* ▼ *electronic identity card*

electronic identification sähköinen tunnistus

▲ *identification* ▶ *biometric identification, certificate, password identification, public key method*
▼ *electronic identity card, strong authentication, weak authentication*

electronic identity card sähköinen henkilökortti

▲ *card, chip card, electronic government, electronic identification, identity, online government, smart card* ▶ *multi-use smart card*

electronic intelligence mitaustiedustelu

▲ *intelligence (2), signals intelligence* ▶ *communications intelligence*

electronic signature sähköinen allekirjoitus

▲ *signature (1)* ▶ *certification, digital signature, electronic document, Electronic Signatures Act, personal certificate, qualified certificate*

Electronic Signatures Act allekirjoituslaki

▲ *act, computer law, information security law*
▶ *electronic signature, trusted (third) party*

electronic warfare sähköinen sodankäynti
 ▲ *cyberwarfare, information warfare, warfare*
 ▶ *command-and-control warfare, smart weapon*
 ▼ *electromagnetic pulse, high energy laser, high power microwave weapon, signals intelligence*

ELINT *electronic intelligence*
 sähköinen tiedustelu

elliptical curve cryptography elliptinen salaustekniikka
 ▲ *asymmetric encryption, cryptography*

Emergency Powers Act valmiuslaki
 ▲ *act, information security law* ▶ *extraordinary circumstances*

employee monitoring tekninen valvonta
 ▲ *monitoring* ▶ *computer system, data processing system, eavesdropping, lawful interception, wiretapping, (legal) wiretapping*

encrypt salakirjoittaa; salata
 ▲ *protection* ▶ *cryptography, encryption, scramble, suppress* ▼ *decipher, decrypt*

encrypted message salasanoma
 ▲ *cryptography, encryption, steganography*

encrypted text salateksti
 ▲ *cryptography, encryption, text* ▶ *ciphertext, clear text, plaintext*

encrypting file system salaava tiedostojärjestelmä
 ▲ *system*

encryption salakirjoitus; salaus
 ▶ *clear text, cryptography, encrypt, plaintext, security protocol, steganography* ▼ *asymmetric encryption, block cipher, ciphertext, cryptanalysis, cryptographic key, cryptology, digital envelope, encrypted message, encrypted text, encryption algorithm, encryption key, encryption product, encryptor, end-to-end encryption, hybrid encryption, one-way encryption algorithm, stream cipher, strong encryption, symmetric encryption, weak encryption*

encryption algorithm salausalgoritmi
 ▲ *algorithm, cryptography, encryption* ▶ *cryptographic key, cryptoprocessor, dual use product, encryption key* ▼ *one-way encryption algorithm, strong encryption algorithm*

encryption key salausavain
 ▲ *cryptography, encryption, key* ▶ *cryptographic key, dual use key, encryption algorithm* ▼ *key escrow (system), key management, key recovery, keyholder, one-time key, private key, public key, secret key*

encryption product salaustuote
 ▲ *cryptography, cryptography policy, encryption* ▼ *dual use product*

encryptor salain
 ▲ *encryption*

end-to-end encryption läpialaus
 ▲ *encryption* ▶ *security protocol*

ensure varmistaa
 ▶ *assure, authenticate, information security assurance, safeguard, seal (v), secure (v), verify*
 ▼ *audit trail, backup, backup copy, call-back (1), check symbol, checking, control (2), dump (v), duplex (v), error control*

entrap ansoittaa
 ▲ *trap (s)* ▶ *back door, honeypot, trap door*

epidemic epidemia
 ▲ *malicious program, rogue program* ▶ *computer virus, infection, virus*

error virhe (1)
 ▲ *accuracy* ▶ *bug, fault, mistake* ▼ *check (v), error condition, memory leak, overflow, structured error handling*

error burst virheryöppy
 ▶ *cyclic redundancy checking*

error condition virhetilanne
 ▲ *error* ▶ *fault, mistake, recovery*

error control varmistus (2)
 ▲ *assure, back up, check (v), control (2), ensure, secure (v)* ▶ *auditability, checking* ▼ *error-checking code, error-detecting code, redundancy*

error rate vikataajuus

error-checking code itsevarmistava koodi
 ▲ *check (s), checking, code, error control* ▶ *error-correcting code, error-detecting code*

error-correcting code itsekorjaava koodi
 ▲ *code, correct (v), revise* ▶ *error-checking code, error-detecting code*

error-detecting code itsevarmistava koodi
 ▲ *check (s), checking, code, error control* ▶ *error-checking code, error-correcting code*

escrow turvatalletus
 ▲ *certificate administration, cryptography policy, information security* ▶ *key escrow (system), key recovery, trusted (third) party*

evaluation (1) arviointi
 ▶ *acceptance test, accreditation, assessment, audit (s), information security norm, quality, review (s)* ▼ *certify*

evidence todistusaineisto

EW *electronic warfare*
 sähköinen sodankäynti

exceptional situation erityistilanne
 ▶ *catastrophe, disaster, extraordinary circumstances*

exhaustive search väsytystekniikka

▲ *breach (v), break (v), crack, cryptanalysis*
 ▶ *brute force technique, computationally secure, cracker, cracking program* ▼ *brute force attack*

exposure altistus

▶ *risk, vulnerability*

extranet vierasverkko

▲ *net* ▶ *demilitarized zone, intranet, partnernet*

extraordinary circumstances poikkeusolot

▶ *Act on Privacy in Telecommunications, baseline security, catastrophe, disaster, Emergency Powers Act, exceptional situation, full preparedness, priority classification, security of supply* ▼ *preparedness plan*

F

facilities security laitteistoturvallisuus

▲ *information security, physical security, security*
 ▶ *computer security, data security, software security, telecommunications security*

fail soft (a) joustavasti varmistettu

▶ *fault tolerant, resilient*

fail soft (v) sietää häiriötä

▶ *crash, robustness*

failsafe ehdottomasti varmistettu

▶ *resistant, robustness*

failure häiriö

▲ *availability, reliability* ▶ *backup system, contingency planning, continuity plan, fallback system, fault, malfunction* ▼ *catastrophe, control failure, disaster, standby*

fallback system varajärjestelmä

▲ *availability, information system, IT backup, reliability, system* ▶ *backup system, failure, malfunction*

fault vika

▲ *availability* ▶ *congestion, error, error condition, failure, interference, malfunction, mistake, tele-maintenance* ▼ *disk crash, fault tolerant, fault trace, head crash*

fault threshold vikakynnys

▲ *availability* ▶ *trigger (s)*

fault tolerant vikasietoinen

▲ *availability, fault, property, tolerant* ▶ *disaster resistant, fail soft (a), resilient, resistant, robustness*

fault trace vianjäljitys

▲ *fault*

feature tunto-merkki

▲ *identification, recognition* ▶ *biometric identification, characteristic, identifier, label, signature (2), stamp (s)*

feedback error control kaikuvarmistus

▶ *echo checking, modulo N checking, redundancy checking, repeater, residue checking*

fi root fi-juuri

▲ *country code, country domain name, domain name, root* ▶ *naming authority*

file infector virus tiedostovirus

▲ *virus* ▶ *e-mail virus, infection, macro virus, parasite, parasitic virus, Web virus*

filter suodatin

▲ *protection* ▶ *firewall, screen (v), security monitor, tiger* ▼ *copyright, packet filter, spam filter, Web filter*

filtering suodatus

▲ *information security* ▶ *control (1), monitoring, supervision*

finger (v) tunnustella

▲ *spyware* ▶ *ping (v), ping packet, port scan*

firewall palomuuuri

▲ *security server* ▶ *demilitarized zone, filter, packet filter, proxy (server), virtual private network*

firewall segment palomuurilohko

FIRST *Forum of Incident Response and Security Teams*

kansainvälinen tietoturvajärjestö

▶ *response team*

flooding hukuttaminen

▶ *bacterium (pl bacteria), DoS attack, saturation attack* ▼ *mail bombing*

forensic oikeuslääketieteellinen; oikeustutkinnallinen

▲ *analysis, law*

forensic cryptography oikeudellinen salakirjoitustutkimus

▲ *cryptography, law*

forge väärentää

▶ *data tampering, tamper*

fragmentation pirstoutuminen

▲ *integrity* ▶ *corruption, defragment*

front end system palvelujärjestelmä

▲ *electronic commerce, online service, system*

full preparedness täysvalmius

▶ *preparedness* ▶ *extraordinary circumstances*

functional address toiminto-osoite

G

garble salakirjoittaa; sekoittaa
 ▶ *hash value* ▼ *self-garbling virus*

go down kaatua
 ▲ *availability* ▶ *collapse, crash*

H

hack (v) hakata (näppäimistöä); murtautua järjestelmään
 ▶ *crack*

hacker hakkeri
 ▲ *user* ▶ *cracker, cyberhacker, hacking, hactivist, samurai, script kiddie, white hat*

hacking hakkerointi
 ▲ *use, utilization* ▶ *cracking, data trespass, hacker, netwar, network-centric warfare*

hactivist haktivisti
 ▶ *hacker*

hardware key tonkeli
 ▲ *key, security module* ▶ *dongle, key chip, smart key* ▼ *USB key*

hash function tiivistysfunktio
 ▲ *algorithm, hash value, message digest* ▶ *compression function*

hash total sekasumma
 ▲ *hash value, message digest*

hash value tiiviste
 ▶ *check symbol, garble, message digest* ▼ *compression function, hash function, hash total*

hazard riskialtius; uhka
 ▲ *availability* ▶ *damage, perpetrator, preparedness, risk, security, threat, vulnerability* ▼ *compromise (v), computer sabotage*

head crash levyrikko
 ▲ *crash, fault* ▶ *corruption, disk crash*

HEL *high energy laser*
 suurenergialaser

high energy laser suurenergialaser
 ▲ *electronic warfare* ▶ *electromagnetic pulse, high power microwave weapon*

high power microwave weapon suuritehoinen mikroaaltose
 ▲ *electronic warfare* ▶ *electromagnetic pulse, high energy laser*

hijack kaapata
 ▶ *commandeer, distributed denial of service attack, impersonation, intercept, man-in-the-middle attack, masquerading, spoofing, theft of identity, zombie* ▼ *cybersquatting, zombie*

hijacking kaappaus
 ▼ *address hijacking, session hijacking*

hoax
 ▼ *virus hoax*

hoax virus valevirus
 ▲ *virus* ▶ *stealth virus, virus hoax*

honeypot houkutuslintu
 ▲ *security monitor, tiger, trap (s)* ▶ *entrap, impersonation, masquerading, mockingbird, spoofing*

host verkkoasema
 ▲ *information network* ▼ *bastion host, secure host*

HTTP *Hypertext Transfer Protocol*
 verkkosivujen siirtokäytäntö

hybrid encryption yhdistelmäsalaus
 ▲ *encryption* ▶ *asymmetric encryption, symmetric encryption*

I

ICT *information and communication technologies*
 tieto- ja viestintäteknikka, tvt

identifiability tunnistettavuus
 ▲ *identify, property* ▶ *auditability, verifiability*

identification tunnistus
 ▲ *identify* ▶ *authentication, authenticity, introduction, log-in, recognition, sign-on, verification*
 ▼ *anonymous use, authentication data, biometric identification, characteristic, electronic identification, feature, identification card, password identification, personal identification number, speaker identification*

identification card henkilökortti
 ▲ *card, identification, recognition*

identifier tunniste; tunnus
 ▲ *identify* ▶ *characteristic, feature, key, label, signature (1), stamp (s), unidentified use*
 ▼ *anonymous user identity, password, user identifier*

identify tunnistaa (1); yksilöidä
 ▶ *stamp (v)* ▼ *identifiability, identification, identifier, label, personal identification number, recognition, unidentified use*

identity henkilöllisyys; identiteetti
 ▼ *anonymous user identity, electronic identity card, theft of identity*

IDS intrusion detection system
tietomurtohälytin

II information infrastructure
tietotekninen perusrakenne
▼ CIIP, DII

illegal luvaton
▲ rule ► legal, unauthorized, X-rated ▼ pirate copy

illegal disclosure paljastus
▲ confidential, disclosure ► business espionage, data leakage, data seepage, unauthorized user

impersonation tekeytyminen
▲ active attack, attack ► address hijacking, commandeering, cracking, data trespass, disinformation, hijack, honeypot, IP spoofing, man-in-the-middle attack, masquerading, mockingbird, piggybacking, rogue program, session hijacking, social engineering, spoofing, tailgating

infection tartunta
► computer virus, contamination, epidemic, file infector virus, virus, worm

information audit tietojenkäsittelyn tarkastus
▲ audit (s) ► information security audit, systems audit

information infrastructure tietotekniset perusrakenteet
▲ infrastructure ► rule

information law tieto-oikeus
▲ law ► computer law ▼ copyright

information management tietohallinto
▲ control (1), management ► information security, risk management, security management ▼ password management

information network tietoverkko
▲ net, network ► data network, service network, value added network ▼ administrative domain, cybercrime, host, intranet, local area network, network crime, network management, network service, open network, private network, remote access, remote login, server, virtual private network

information risk tietoriski
▲ risk ► information security, information security risk, risk management ▼ data leakage, data seepage, residual data, residue

information security tietoturvallisuus
▲ security ► availability, confidentiality, information management, information risk, information systems security, integrity, privacy protection, vulnerability ▼ access control, Act on Privacy in Telecommunications, administrative and organizational information security, baseline security, certificate, classification of data, compromise (s), computer security, data security, defensive information security, escrow, facilities security, filtering, information security architecture, information security assurance, information security law, information security risk, intrusion, IT security, operations security, penetration, personnel security, physical security, premises security, proactive information security, public key infrastructure, secret (a), software security, telecommunications security, violation of information security

information security architecture tietoturva-arkkitehtuuri
▲ information security, security architecture ► information security guidelines, information security policy

information security assurance tietojen turvaaminen
▲ assurance, information security ► assure, back up, check (v), ensure, secure (v)

information security audit tietoturvatarkastus
▲ information security norm ► information audit, systems audit ▼ loophole, risk analysis, security breach

information security breach tietoturvaloukkaus
▲ security breach ► infringement, security incident, violation of right ▼ cracking, data trespass

information security guidelines tietoturvalinjaukset
▲ information security policy ► information security architecture, information security planning ▼ information security manual

information security law tietoturva-oikeus
▲ computer law, information security, law ▼ Act on Privacy in Telecommunications, Electronic Signatures Act, Emergency Powers Act, Personal Data Act

information security manual tietoturvakäsikirja; tietoturvaohjeisto
▲ information security guidelines, information security norm

information security norm tietoturvanormi
▲ norm ► assessment, evaluation (1), information security policy, information security standard ▼ information security audit, information security manual, systems audit

information security plan tietoturvasuunnitelma
 ▶ *baseline security, continuity plan, information security planning*

information security planning tietoturvasuunnittelu
 ▶ *information security guidelines, information security plan* ▼ *threat analysis*

information security policy tietoturvapoliittikka
 ▲ *policy, security, security policy* ▶ *data protection policy, information security architecture, information security norm, information security standard, privacy protection policy* ▼ *certificate policy, cryptography policy, defensive information security, information security guidelines, proactive information security, risk management, security management*

information security risk tietoturvariski
 ▲ *availability, information security, risk* ▶ *damage, information risk* ▼ *scattered electromagnetic radiation*

information security standard tietoturvastandardi
 ▲ *standard* ▶ *information security norm, information security policy*

information security strategy tietoturvastrategia

information security technology tietoturva-tekniikka
 ▲ *technology* ▶ *cryptography, privacy enhancing technology, spyware*

information service tiedotuspalvelu
 ▲ *network service, online service, service*

information system tietojärjestelmä
 ▲ *system* ▶ *systems auditor* ▼ *access (s), attack, backup system, fallback system, system administrator, system description, use, user, utilization*

information systems security tietoturvallisuus
 ▶ *information security, IT security*

information systems warfare tietojärjestelmä-sodankäynti
 ▲ *cyberwarfare, information warfare* ▶ *netwar, network-centric warfare*

information warfare tietosodankäynti
 ▲ *warfare* ▶ *C2W, cyberwarfare, vulnerability* ▼ *command-and-control warfare, disinformation, electronic warfare, information systems warfare, infrastructure warfare, interference, netwar, network-centric warfare, signals intelligence*

infrastructure perusrakenne
 ▼ *information infrastructure, infrastructure warfare, public key infrastructure*

infrastructure warfare infrastruktuurisodankäynti
 ▲ *cyberwarfare, information warfare, infrastructure, warfare*

infringement oikeudenloukkaus
 ▶ *breach (s), computer crime, damage, information security breach, interference, session hijacking, violation of right* ▼ *computer crime, infringement of privacy, privacy violation*

infringement of privacy yksityisyyden loukkaus
 ▲ *infringement, privacy, violation of right* ▶ *privacy protection, privacy violation, sensitive data*

inhibit estää
 ▲ *availability* ▶ *congestion, denial of service, deny, suppress*

insider threat sisäinen uhka
 ▲ *threat* ▶ *outside threat*

inspect tarkastaa (1)
 ▲ *integrity, mistake, validity* ▶ *back up, check (v), revise, secure (v), test (v), testing* ▼ *audit trail, auditor, right to inspect*

inspection tarkastus (1)
 ▶ *audit (s), check (s), check(mark)*

integrity eheys
 ▲ *property, quality* ▶ *accuracy, audit trail, authenticity, confidentiality, data tampering, information security, maintenance, nonrepudiation, reliability, usability, validity* ▼ *check (v), corruption, fragmentation, inspect*

intelligence (1) älykkyys

intelligence (2) tiedustelu
 ▶ *business espionage, monitoring, probe (s), spyware* ▼ *communications intelligence, dumpster diving, eavesdropping, electronic intelligence, ping packet, port scan, scan (s), scanning, scavenging, signals intelligence, wiretapping*

intercept siepata
 ▲ *cybercrime, network crime, spyware* ▶ *commandeer, eavesdropping, hijack, lawful interception, scattered electromagnetic radiation, wiretapping, (legal) wiretapping* ▼ *key logger*

interference häirintä; puuttuminen
 ▲ *availability, computer crime, cyberwarfare, information warfare* ▶ *contamination, control (1), DoS attack, fault, infringement, protection, saturation attack, violation of right* ▼ *data tampering, tamper*

intranet omaverkko
 ▲ *information network, net* ▶ *extranet, partner-net, private network*

introduction esittäytyminen
 ▲ *log-in, login, sign-on, user* ▶ *authentication, identification, recognition, verification*

intrusion tunkeutuminen

▲ *information security* ▶ *attack, breach (s), crack, cracking, data trespass, loophole, penetration, security breach, unauthorized user* ▼ *cracker, cyberhacker, intrusion detection system*

intrusion detection system tietomurtohälytin

▲ *intrusion, monitor (s), penetration, security monitor, system, tiger* ▶ *anti-virus program, cracking, data trespass, security alert, trap (s), virus alert, virus protection software, virus scanner*

IP spoofing verkko-osoitteen väärentäminen

▲ *attack, spoofing* ▶ *impersonation, masquerading, spoofing*

IPSec IP Security

IP-verkon tietoturvastandardi

IT backup tietotekniikan varmistus

▲ *backup* ▼ *backup site, backup system, fallback system*

IT security tietotekniikan turvallisuus; tietoturvallisuus

▲ *information security, security* ▶ *information systems security, operations security, physical security, software security*

IW *information warfare*

tietosodankäynti

J

junk mail roskaposti

▶ *spam (s)*

K

key avain

▶ *code, computationally secure, identifier* ▼ *authentication key, cryptographic key, dual use key, encryption key, hardware key, one-time key, private key, public key, secret key, session key, smart key, USB key*

key agreement protocol avaintenvaihtokäytäntö

▲ *agreement, protocol, security protocol, symmetric encryption*

key chip avainpiiri

▲ *security module* ▶ *dongle, hardware key, pirate copy*

key distribution center avainten jakelukeskus

▲ *key management* ▶ *certificate authority*

key escrow (system) vara-avainjärjestelmä

▲ *cryptographic key, cryptography policy, encryption key* ▶ *escrow, key recovery, recovery* ▼ *lawful access*

key logger näppäinloki

▲ *intercept, spyware* ▶ *eavesdropping, scattered electromagnetic radiation, wiretapping*

key management avaintenhallinta

▲ *cryptographic key, encryption key, management* ▶ *keyholder* ▼ *key distribution center*

key management system avaintenhallintajärjestelmä

key recovery avaimen palautus

▲ *cryptographic key, encryption key, recovery* ▶ *escrow, key escrow (system)*

keyholder avaimenhaltija

▲ *cryptographic key, encryption key* ▶ *key management*

L

label tunnistee

▲ *identify* ▶ *characteristic, feature, identifier, signature (1), stamp (s), unidentified use*

law

▼ *computer law, copyright law, data protection law, forensic, forensic cryptography, information law, information security law, nondisclosure agreement, privacy law, sunshine law*

lawful access viranomaispääsy

▲ *access (s), key escrow (system)* ▶ *certificate administration, control (1), right to inspect, supervision*

lawful interception telekuuntelu

▲ *spyware* ▶ *Coercive Measures Act, eavesdropping, employee monitoring, intercept, remote surveillance, telemonitoring, wiretapping, (legal) wiretapping*

leapfrog attack koukkaus

▲ *active attack* ▶ *distributed denial of service attack, zombie*

legal juridinen; luvallinen; sallittu

▶ *illegal*

legal notice ehtoilmoitus

▶ *disclaimer, nondisclosure agreement*

letter bomb kirjepommi

▲ *bomb*

level C security C-tason turvallisuus

▲ *baseline security, security classification*

liability vahinkovastuu

local area network lähiverkko

- ▶ *closed network, information network, network*
- ▶ *remote access, remote connection, telework*
- ▼ *network management software*

lock (out) suojata

log (s) loki

- ▶ *document, monitor (s), operation(s), security incident*

log-in sisäänkirjaus

- ▶ *authentication, identification, recognition, sign-on, verification*
- ▼ *introduction, single sign-on*

logic bomb ehdollinen pommi

- ▶ *bomb, malicious program*
- ▼ *trigger (s)*

login sisäänkirjaus

- ▼ *introduction, remote login, single sign-on*

loophole tietoturva-aukko

- ▶ *cracking, data trespass, information security audit, systems audit, vulnerability*
- ▶ *intrusion, penetration, protection, security breach, trap door*
- ▼ *trap door*

M

macro virus makrovirus

- ▶ *virus*
- ▶ *data driven attack, e-mail virus, file infector virus*

mail bombing sähköpostipommitus

- ▶ *bomb, DoS attack, flooding, saturation attack*

maintainability ylläpidettävyys

- ▶ *maintenance, property*
- ▶ *serviceable*

maintenance huolto (1); ylläpito

- ▶ *availability*
- ▶ *corruption, integrity, malfunction, network management, operation(s), operations security, service*
- ▼ *maintainability, purging, system maintenance, telemaintenance*

malfunction häiriö; toimintahäiriö

- ▶ *availability, reliability*
- ▶ *backup system, contingency planning, continuity plan, failure, fallback system, fault, maintenance, recovery, service*
- ▼ *catastrophe, disaster, standby*

malicious code tuholaisohjelma

- ▶ *rogue program*

malicious program tuholaisohjelma

- ▶ *program*
- ▶ *ping of death, replicator, rogue program, security monitor, tiger*
- ▼ *bomb, chameleon, computer virus, epidemic, logic bomb, mockingbird, payload, time bomb, Trojan horse, virus, worm*

malware haittaohjelma; tuholaisohjelma

- ▶ *ware*
- ▶ *rogue program*

man-in-the-middle attack välistävetohyökkäys

- ▶ *active attack*
- ▶ *commandeer, hijack, impersonation, masquerading, spoofing*

management hallinta; hallinto

- ▶ *availability, control (1), system owner*
- ▼ *information management, key management, network management, quality management, risk management, security management, telecommunications management network, webmaster*

mandatory access control pakollinen pääsyalvonta

masquerading tekeytyminen

- ▶ *active attack, attack*
- ▶ *address hijacking, commandeer, cracking, data trespass, disinformation, hijack, honeypot, impersonation, IP spoofing, man-in-the-middle attack, mockingbird, piggybacking, rogue program, session hijacking, social engineering, spoofing, tailgating*

master card valtuuskortti

- ▶ *authority, card, chip card, smart card*

material aineisto

- ▶ *archive (s), data, data security, pirate copy*
- ▼ *classified information*

memory leak muistihukka; muistivuoto

- ▶ *error*
- ▶ *bacterium (pl bacteria), defragment, overflow*

message digest tiiviste

- ▶ *check symbol, hash value*
- ▼ *compression function, hash function, hash total*

MIME Multipurpose Internet Mail Extensions

eräs laajennettu sähköpostin koodaustapa

mimic matkia

- ▶ *spoofing*

mirror (s,a) toisio-

- ▶ *tandem*
- ▼ *mirror database, mirror file, mirror server, mirror site*

mirror (v) toisintaa

- ▶ *dump (v), duplex (v), replicate, replicator*

mirror database toisiokanta

- ▶ *mirror (s,a)*
- ▶ *backup file, mirror site*

mirror file toisiotiedosto

- ▶ *mirror (s,a)*
- ▶ *mirror server*

mirror server toisiopalvelin

- ▶ *mirror (s,a), server*
- ▶ *mirror file, mirror site*

mirror site toisiosivusto

- ▶ *mirror (s,a)*
- ▶ *mirror database, mirror server*

mistake virhe (2)

- ▶ *rule*
- ▶ *check symbol, error, error condition, fault, revise, test (v)*
- ▼ *check (v), debugging, inspect, structured error handling*

MITMA man-in-the-middle

välistävetohyökkäys

- ▶ *attack*

mockingbird papukaija

▲ *malicious program, rogue program* ▶ *honeypot, impersonation, masquerading, spoofing*

modulo N checking jakojäännösvarmistus

▲ *checking* ▶ *accuracy, echo checking, feedback error control, redundancy checking, residue checking*

monitor (s) seurain

▶ *log (s), network management software, remote surveillance, telemaintenance, telemonitoring, virus scanner* ▼ *intrusion detection system, network analyzer, packet sniffer, reference monitor, security monitor, sniffer, watchdog timer*

monitor (v) tarkkailla; valvoa

▶ *back up, check (v), control (v), secure (v), sniff, supervise* ▼ *control (1), supervision, telemonitoring*

monitoring tarkkailu

▶ *control (1), filtering, intelligence (2), supervision* ▼ *employee monitoring, passage control, physical access control*

multi-use smart card monitoimikortti

▲ *electronic commerce, network service, smart card, use* ▶ *electronic identity card*

multiple certificate environment monivarmenneympäristö

▲ *certificate, certification hierarchy, certification service*

N

name server nimipalvelin

▲ *server*

naming authority tunnushallintokeskus

▲ *administrative domain, (public) authority* ▶ *fi root*

net verkko

▶ *network* ▼ *data network, extranet, information network, intranet, partnet*

netwar verkkosodankäynti

▲ *cyberwarfare, information warfare* ▶ *hacking, information systems warfare, network-centric warfare* ▼ *cyber terrorism*

network verkko

▶ *net* ▼ *closed network, data network, information network, local area network, open network, private network, service network, telecommunications management network, value added network, virtual private network*

network administrator verkkovastaava

▲ *administrator, network management* ▶ *webmaster*

network analyzer verkkoanalysaattori

▲ *monitor (s), network management* ▶ *network trace, packet filter, packet sniffer, sniffer*

network crime tietoverkkorikos

▲ *crime, information network* ▶ *communications crime, computer crime, cybercrime* ▼ *address hijacking, cyber terrorism, cybersquatting, eavesdropping, intercept, session hijacking, wiretapping*

network management verkonhallinta

▲ *information network, management* ▶ *maintenance, telecommunications security* ▼ *network administrator, network analyzer, packet filter, packet sniffer, telecommunications management network, trace packet*

network management software verkonhallintaohjelmisto

▲ *local area network* ▶ *monitor (s)*

network notary verkkonotaari

▲ *trusted (third) party* ▶ *nonrepudiation, time stamp service* ▼ *authentication server, notarization, notary services*

network scan verkkoskannaus

▲ *scan (s)* ▶ *accessibility, ping packet, port scan*

network service verkkopalvelu

▲ *information network, service* ▶ *telemaintenance, telework* ▼ *directory service, electronic commerce, information service, multi-use smart card, Robinson list, time stamp service*

network trace verkkojälki

▶ *network analyzer, packet sniffer, trace packet, user profile*

network-centric warfare verkkosodankäynti

▲ *cyberwarfare, information warfare, warfare* ▶ *hacking, information systems warfare, netwar* ▼ *cyber terrorism*

no-break power supply katkoton tehonsyöttö

▲ *availability, operations security* ▶ *uninterrupted power supply*

nondisclosure agreement vaitiolosopimus

▲ *agreement, disclosure, law* ▶ *legal notice*

nonrepudiation kiistämättömyys

▲ *quality, repudiate* ▶ *authenticity, integrity, network notary, secure e-mail, stamp (s), time stamp*

norm normi

▲ *rule* ▶ *(public) authority, code of conduct, code of ethics, standard* ▼ *information security norm*

notarization notarointi

▲ *network notary* ▼ *time stamp*

notary services notaaripalvelut

▲ *network notary*

nuke tuhota

▶ *crash*

O

official document viranomaisen asiakirja
 ▲ (public) authority, document ▶ confidential, security classification, top secret

one-time key kerta-avain
 ▲ cryptographic key, encryption key, key ▶ one-time pad, session key

one-time pad kertasalain
 ▲ stream cipher ▶ one-time key

one-way encryption algorithm yksisuuntainen salausalgoritmi
 ▲ algorithm, decipher, decrypt, encryption, encryption algorithm

online government hallinnon sähköinen asiointi
 ▲ (public) authority ▶ Act on Online Government Services, certificate, electronic government ▼ electronic identity card

online service sähköinen asiointi
 ▲ service ▼ front end system, information service

open network avoin verkko
 ▲ information network, network ▶ closed network, communication protocol, private network, service network, value added network

operation(s) käyttö (2)
 ▶ availability, log (s), maintenance, service ▼ checkpoint, checkpoint restart, operations security, restart, time-out

operations security käyttöturvallisuus
 ▲ information security, operation(s), security ▶ IT security, maintenance, physical security ▼ no-break power supply, uninterrupted power supply

OPSEC operations security
 käyttöturvallisuus

OTA over the air
 langattomasti

outside threat ulkoinen uhka
 ▲ threat ▶ insider threat

overflow ylivuoto
 ▲ error ▶ memory leak, redundancy

P

packet
 ▼ ping packet, trace packet

packet filter pakettisuodatin
 ▲ filter, network management ▶ firewall, network analyzer, packet sniffer, sniffer, spam filter, Web filter

packet sniffer nuuskin; verkkoanalysoija
 ▲ monitor (s), network management, sniff, sniffer ▶ network analyzer, network trace, packet filter, ping packet, root kit, sniffer

parasite loisohjelma
 ▲ computer virus, rogue program, virus ▶ bacterium (pl bacteria), file infector virus, parasitic virus

parasitic virus loisohjelma
 ▲ computer virus, rogue program, virus ▶ bacterium (pl bacteria), file infector virus, parasite

partnet vierasverkko
 ▲ net ▶ demilitarized zone, extranet, intranet

passage control kulunvalvonta
 ▲ access control, control (1), control (2), monitoring, physical security, premises security, supervision ▶ physical access control

passive attack passiivinen hyökkäys
 ▲ attack ▶ active attack ▼ sniff, trap door

passphrase salalause
 ▶ challenge-response method, password

password salasana
 ▲ identifier ▶ authentication, code, passphrase, theft of identity, user, verification ▼ dynamic password

password identification salasanatunnistus
 ▲ authentication, identification, verification ▶ biometric identification, challenge-response method, electronic identification, voice recognition

password management salasanahallinto
 ▲ information management

patch (v) paikata

payload lataus
 ▲ computer virus, malicious program, rogue program, virus ▶ trigger (s)

PEM privacy enhanced mail
 tietosuojattu sähköposti

penetration tunkeutuminen
 ▲ information security ▶ attack, crack, cracking, data trespass, intrusion, loophole, security breach, unauthorized user ▼ cracker, cyberhacker, intrusion detection system

perpetrator hyökkääjä
 ▶ attack, cracker, cyberhacker, hazard, threat

person register henkilörekisteri
 ▶ Personal Data Act, registrar ▼ data subject, personal file description, register object

personal certificate henkilövarmenne
 ▲ certificate ▶ electronic signature

personal data henkilötieto
 ▲ data ▼ privacy protection

Personal Data Act henkilötietolaki

▲ *act, computer law, information security law, privacy protection* ► *data protection ombudsman, person register, privacy commissioner* ▼ *personal file description, registrar, sensitive data*

personal file description rekisteriseloste

▲ *person register, Personal Data Act, system description* ► *privacy statement*

personal identification number henkilötunnus

▲ *identification, identify, recognition* ► *privacy, user identifier*

personnel security henkilöstöturvallisuus

▲ *information security, security*

PET *privacy enhancing technology*
tietosuojatekniikka

PGP *pretty good privacy*

eräs julkisen avaimen menetelmä

phreaking puhelinverkkoon murtautuminen

► *cracker, war dialing*

physical access control kulunvalvonta

▲ *access control, control (1), monitoring, physical security, premises security, supervision* ► *passage control*

physical security fyysinen turvallisuus

▲ *information security, security* ► *damage, IT security, operations security* ▼ *computer security, facilities security, passage control, physical access control, premises security*

piggybacking peesaus

► *access control, crack, impersonation, masquerading, spoofing, tailgating*

PIN *personal identification number*

henkilökohtainen tunnus; henkilötunnus

PIN code PIN-koodi

▲ *code*

PING *packet Internet groper*

eräs yhteyskäytäntö

▲ *spyware*

ping (v) lähettää tiedustelupaketti

► *finger (v)*

ping command ping-komento

► *ping packet*

ping of death tuhopaketti

► *blue bomb, bomb, DoS attack, malicious program, ping packet, saturation attack, WinNuke*

ping packet tiedustelupaketti

▲ *intelligence (2), packet, scan (s), scanning* ► *finger (v), network scan, packet sniffer, ping command, ping of death, probe (s), root kit, security monitor, sniffer, tiger*

piracy piratismi

▲ *computer crime, copyright*

pirate copy laitton kopio

▲ *copy, copyright, illegal, unauthorized* ► *data, digital fingerprint, digital watermark, key chip, material, skim*

pixel beacon piilojäljite

▲ *spyware, Web beacon* ► *Web bug*

PKA *public key architecture*

julkisen avaimen järjestelmä

PKI *public key infrastructure*

julkisen avaimen järjestelmä

▼ *wireless PKI*

PKI certificate PKI-varmenne

▲ *certificate*

plaintext selväkieliteksti

► *ciphertext, clear text, cryptography, encrypted text, encryption*

policy

▼ *data protection policy, information security policy, privacy protection policy, security policy*

port scan porttipyyhkäisy; porttiskannaus

▲ *intelligence (2), probe (s), scan (s)* ► *finger (v), network scan, vulnerability scan*

positioning paikannus

positioning system paikannusjärjestelmä

▲ *system*

premises security toimitilaturvallisuus

▲ *information security, physical security, security* ▼ *passage control, physical access control*

preparedness valmius

► *hazard, threat* ▼ *contingency planning, full preparedness, standby*

preparedness plan valmiussuunnitelma

▲ *contingency plan, continuity plan, extraordinary circumstances*

preparedness planning valmiussuunnittelu

▲ *contingency planning* ► *priority classification*

preventive measures ennaltaehkäisy

▲ *proactive information security* ► *vulnerability*

priority classification tärkeysluokitus

▲ *classification, classification of data* ► *extraordinary circumstances, preparedness planning, protection profile* ▼ *vital application*

privacy yksityisyys

▲ *property* ► *confidentiality, personal identification number, sensitive data* ▼ *data protection law, infringement of privacy, privacy protection, privacy violation*

privacy commissioner tietosuojavaltutettu

▲ *(public) authority, privacy protection* ► *data protection ombudsman, Personal Data Act*

privacy enhancing technology tietosuojatekniikka

▲ *privacy protection, technology* ▶ *information security technology*

privacy law tietosuojalaki

▲ *law* ▶ *Act on the Openness of Government Activities*

privacy protection tietosuojaja; yksityisyyden suoja

▲ *personal data, privacy, protection* ▶ *data haven, information security, infringement of privacy, privacy violation, user profile* ▼ *data protection crime, data protection ombudsman, data protection software, Personal Data Act, privacy commissioner, privacy enhancing technology*

privacy protection policy tietosuojapolitiikka

▲ *policy* ▶ *data protection policy, information security policy*

privacy statement tietosuojaseloste

▲ *disclaimer, personal file description, system description*

privacy violation yksityisyyden loukkaus

▲ *infringement, privacy, violation of right* ▶ *infringement of privacy, privacy protection, sensitive data*

private key yksityinen avain

▲ *asymmetric encryption, cryptographic key, encryption key, key, public key method* ▶ *public key, secret key*

private network yksityisverkko

▲ *information network, network* ▶ *closed network, intranet, open network, virtual private network* ▼ *virtual private network*

proactive information security ennakoiva tietoturvasuus

▲ *information security, information security policy* ▶ *defensive information security, security management* ▼ *preventive measures*

probe (s) luotaus

▶ *cracking, data trespass, eavesdropping, intelligence (2), ping packet, scan (s), scanning, wiretapping* ▼ *port scan, vulnerability scan*

processor käsittelijä

(data) processor tietojenkäsittelijä

professional ethics ammattietiikka

profile

▼ *protection profile, user profile*

program

▼ *anti-virus program, cracking program, malicious program, rogue program*

proof total varmistussumma

▲ *check symbol* ▶ *checksum*

property ominaisuus

▶ *quality, standard* ▼ *accessibility, accuracy, auditability, authenticity, availability, fault tolerant, identifiability, integrity, maintainability, privacy, public, quality of service, reliability, repeatability, resilient, resistant, robustness, traceability, usability, verifiability, vulnerability*

protection suojaus

▶ *availability, interference, loophole, risk, security, security breach* ▼ *data protection law, data protection ombudsman, data protection software, encrypt, filter, privacy protection, protection profile, quarantine (v), virus protection software*

protection profile turvaprofiili

▲ *profile, protection* ▶ *priority classification*

protocol käytäntö

▼ *communication protocol, key agreement protocol, security protocol*

proxy (server) välipalvelin

▲ *server* ▶ *firewall, security server* ▼ *reverse proxy*

pseudonym peitenimi

▲ *user identifier* ▶ *anonymous user ID*

public julkinen

▲ *property* ▶ *access (s), classification of data, confidential, (in the) public domain, restricted use, secret (a)*

(in the) public domain julkinen

▶ *confidential, public, restricted use, secret (a)*

public key julkinen avain

▲ *asymmetric encryption, cryptographic key, encryption key, key* ▶ *private key, secret key* ▼ *public key infrastructure*

public key certificate julkisen avaimen varmenne

▲ *certificate* ▶ *root certificate*

public key infrastructure julkisen avaimen järjestelmä

▲ *information security, infrastructure, public key* ▶ *directory service, electronic commerce, trusted (third) party* ▼ *accreditation scheme, certificate, certificate administration, certificate authority, revocation list, time stamp service*

public key method julkisen avaimen menetelmä

▲ *asymmetric encryption* ▶ *electronic identification, strong authentication* ▼ *private key*

purging puhdistus

▲ *maintenance, service* ▶ *residual data, residue*

Q

qualified certificate laatuvarmenne
 ▲ *certificate* ► *digital signature, electronic signature*

quality laatu
 ► *assessment, evaluation (1), property* ▼ *availability, confidentiality, integrity, nonrepudiation, quality management, quality of service, validity, verifiability*

quality control laadunvarmistus
 ▲ *control (1)* ► *quality management*

quality management laadunhallinta
 ▲ *management, quality* ► *quality control*

quality of service palvelutaso
 ▲ *property, quality, service*

quarantine (s) karanteeni

quarantine (v) eristää
 ▲ *protection* ► *be contaminated, computer virus, rogue program, trap (s), virus*

R

RAID *redundant arrays of inexpensive disks*
 eräs vikasietoinen levymuistijärjestelmä

recognition tunnistus
 ▲ *identify* ► *authentication, authenticity, identification, introduction, log-in, sign-on, verification*
 ▼ *anonymous use, authentication data, characteristic, cross-border recognition of certificates, feature, identification card, personal identification number, speaker recognition, speech recognition, voice recognition*

recognize tunnistaa (2)
 ▼ *biometric identification, speaker identification, speaker recognition, speech recognition, voice recognition*

recovery palautus; toipuminen
 ▲ *availability* ► *error condition, key escrow (system), malfunction, reliability* ▼ *key recovery*

recovery plan toipumissuunnitelma
 ▲ *availability, contingency plan, continuity plan*
 ► *catastrophe, disaster*

recovery planning toipumissuunnittelu

recovery procedure toipumismenettely
 ► *bypass procedure*

redundancy ylimäärä
 ▲ *check (s), checking, error control* ► *overflow* ▼ *cyclic redundancy checking, redundancy checking*

redundancy checking ylimäärävarmistus
 ▲ *checking, redundancy* ► *echo checking, feedback error control, modulo N checking, residue checking* ▼ *cyclic redundancy checking*

reference monitor viiteseurain
 ▲ *access right, authority, monitor (s)*

register object rekisteröity
 ▲ *person register* ► *data subject, right to inspect*

registrar rekisterinpitäjä
 ▲ *Personal Data Act* ► *data controller, person register, system owner*

registry henkilörekisteri; rekisteri
 ► *roster*

reliability luotettavuus
 ▲ *property* ► *accessibility, accuracy, auditability, availability, integrity, recovery, robustness, secure (a), security, verifiability* ▼ *back up, backup system, check (v), crash, failure, fallback system, malfunction, seal (s), secure (v), trusted (third) party*

remote access etäkäyttö; etäyhteys
 ▲ *access (s), information network, use, utilization*
 ► *local area network, remote connection, remote login, telework* ▼ *call-back (1), remote job entry*

remote connection etäyhteys
 ► *local area network, remote access, telework*

remote job entry töiden etäsyöttö
 ▲ *remote access, remote login*

remote login etäkäyttö
 ▲ *information network, login, use, utilization* ► *remote access, telework* ▼ *call-back (1), remote job entry*

remote procedure call etäkutsu

remote surveillance televalvonta
 ▲ *control (1), spyware, supervision* ► *Coercive Measures Act, eavesdropping, lawful interception, monitor (s), telemaintenance, telemonitoring, wiretapping, (legal) wiretapping*

remote work etätö
 ▲ *work* ► *telecommuting*

repeatability uusittavuus
 ▲ *property* ► *auditability, rerun, traceability, verifiability*

repeater toistin
 ▲ *revise* ► *echo checking, feedback error control*

replicate toisintaa
 ► *dump (v), duplex (v), mirror (v), replicator*

replicator monistuva ohjelma
 ► *malicious program, mirror (v), replicate, rogue program* ▼ *bacterium (pl bacteria), computer virus, virus, worm*

repudiate kiistää

▼ *nonrepudiation*

rerun uusinta-ajo

▶ *checkpoint restart, repeatability*

residual data jäännöstieto

▲ *data, information risk* ▶ *cruff, dumpster diving, purging, residue, scavenging* ▼ *shredder*

residue jäännöstieto

▲ *information risk* ▶ *cruff, dumpster diving, purging, residual data, scavenging* ▼ *shredder*

residue checking jakojäännösvarmistus

▲ *checking* ▶ *accuracy, echo checking, feedback error control, modulo N checking, redundancy checking*

resilient vastustuskykyinen

▲ *availability, property* ▶ *disaster resistant, fail soft (a), fault tolerant, resistant, robustness, tolerant*

resistant vastustuskykyinen

▲ *availability, property* ▶ *disaster resistant, failsafe, fault tolerant, resilient, robustness* ▼ *disaster resistant*

response team (tieto)turvapartio

▶ *FIRST*

restart uudelleenaloitus

▲ *operation(s)* ▶ *abend, abort (s), checkpoint restart*

restricted use viranomaiskäyttö

▲ *security classification, use* ▶ *confidential, public, (in the) public domain, secret (a)*

retrovirus retrovirus

▲ *virus* ▶ *stealth virus*

reverse proxy turvapalvelin

▲ *proxy (server)*

review (s) katselmus

▶ *assessment, audit (s), evaluation (1)*

revise tarkistaa (1)

▲ *accuracy* ▶ *back up, check (v), control (2), inspect, mistake, secure (v)* ▼ *error-correcting code, repeater*

revocation list sulkulista

▲ *certificate, directory service, public key infrastructure* ▶ *Robinson list*

right

▼ *access right, copyright, usage rights, violation of right*

right of access pääsyoikeus; tarkastusoikeus

▲ *access (s)* ▶ *right to inspect*

right to inspect tarkastusoikeus

▲ *check (v), inspect* ▶ *data subject, lawful access, register object, right of access*

risk riski

▶ *compromise (v), damage, exposure, hazard, protection, security, threat, vulnerability* ▼ *information risk, information security risk*

risk analysis riskianalyysi

▲ *analysis, information security audit, risk management, systems audit* ▶ *threat analysis, vulnerability analysis*

risk management riskienhallinta

▲ *information security policy, management* ▶ *information management, information risk, vulnerability* ▼ *risk analysis*

Robinson list kieltolista

▲ *network service* ▶ *revocation list*

robustness sitkeys

▲ *property* ▶ *availability, bastion host, fail soft (v), failsafe, fault tolerant, reliability, resilient, resistant, secure host, vulnerability*

rogue program haittaohjelma; tuholaisohjelma

▲ *program* ▶ *cracker, cracking program, data driven attack, impersonation, malicious code, malicious program, malware, masquerading, quarantine (v), replicator, spoofing, virus alert* ▼ *bacterium (pl bacteria), bomb, chameleon, computer virus, DoS attack, epidemic, mockingbird, parasite, parasitic virus, payload, saturation attack, time bomb, Trojan horse, virus, worm*

root pääkäyttäjä (2)

▶ *authorized user* ▼ *fi root*

root certificate juurivarmenne

▲ *certificate, certification hierarchy* ▶ *public key certificate*

root kit murtopakki

▲ *cracking, data trespass* ▶ *cracker, cracking program, packet sniffer, ping packet, sniffer, Trojan horse*

roster henkilökisteri; rekisteri

▶ *registry*

RPC *remote procedure call*

etäkutsu

rule sääntö

▶ *control (1), information infrastructure, standard* ▼ *code of conduct, code of ethics, illegal, mistake, norm, unauthorized*

S

S/MIME *Secure MIME*

turvallisempi MIME-sähköposti

safeguard suojata; turvata; turvatakuu

▶ *assure, ensure, secure (v)*

safety copy turvakopio

▲ *copy* ▶ *backup, backup copy, security archive*

salami technique siivuteknikka

▲ *computer-assisted fraud, technique*

samurai valkolakki

▶ *cracker, cyberhacker, hacker, security monitor, tiger, white hat*

saturation attack palvelunestohyökkäys

▲ *active attack, attack, congestion, rogue program* ▶ *DoS attack, flooding, interference, ping of death* ▼ *mail bombing*

scan (s) skannaus

▲ *intelligence (2)* ▶ *probe (s), scanning* ▼ *network scan, ping packet, port scan, vulnerability scan*

scanning skannaus

▲ *intelligence (2)* ▶ *probe (s), scan (s)* ▼ *ping packet*

scattered electromagnetic radiation hajasäteily

▲ *information security risk* ▶ *electromagnetic pulse, intercept, key logger, signals intelligence*

scavenging pengonta

▲ *intelligence (2)* ▶ *dumpster diving, residual data, residue, shredder, spyware*

scramble sekoittaa

▶ *encrypt*

screen (v) seuloa; valikoida

▶ *filter*

script kiddie skriptari

▶ *ankle biter, cracker, cyberhacker, hacker*

seal (s) sinetti

▲ *reliability* ▶ *check symbol, digital signature*

seal (v) sinetöidä

▶ *assure, back up, check (v), ensure, secure (v)*

secrecy salassapito**secret (a)** salainen

▲ *classification of data, information security, security classification* ▶ *classified information, confidential, public, (in the) public domain, restricted use, sensitive data* ▼ *top secret*

secret (s) salaisuus

▼ *business secret*

secret key salainen avain

▲ *cryptographic key, encryption key, key* ▶ *private key, public key, symmetric encryption*

secure (a) suojattu; turvallinen

▶ *reliability*

secure (v) varmistaa

▲ *availability, reliability* ▶ *authenticate, back up, check (v), ensure, information security assurance, inspect, monitor (v), revise, safeguard, seal (v), supervise, trusted, verify* ▼ *audit trail, back-up, backup copy, call-back (1), check symbol, checking, control (2), dump (v), duplex (v), error control*

secure device varmalaitte

▶ *security module, trusted device* ▼ *authorization terminal*

secure e-mail turvaposti

▶ *digital signature, nonrepudiation*

secure host verkkolinnake

▲ *host* ▶ *attack, bastion host, robustness, vulnerability*

secure router turvareititin**security** turvallisuus

▶ *hazard, protection, reliability, risk, threat* ▼ *baseline security, check (s), computer security, data security, facilities security, information security, information security policy, IT security, operations security, personnel security, physical security, premises security, security policy, software security, technical assurance, telecommunications security*

security alert hälytysviesti

▶ *intrusion detection system, security incident*

security architecture turva-arkkitehtuuri

▶ *data protection software* ▼ *information security architecture, security mechanism*

security archive turva-arkisto

▲ *archive (s)* ▶ *backup archive, damage, safety copy, working archive*

security awareness turvallisuustietoisuus

▶ *security culture, security policy*

security breach tietoturva-aukko

▲ *breach (s), cracking, data trespass, information security audit, systems audit, vulnerability* ▶ *intrusion, loophole, penetration, protection, trap door* ▼ *information security breach, trap door*

security classification turvaluokitus

▲ *classification, classification of data, classify* ▶ *confidential, official document* ▼ *classified information, level C security, restricted use, secret (a), security marking, top secret*

security culture turvallisuuskulttuuri

▶ *security awareness, security policy*

security incident turvallisuushäiriö

▶ *anomaly, be compromised, control failure, information security breach, log (s), security alert*

security management turvallisuusjohtaminen
 ▲ *information security policy, management* ▶ *information management, proactive information security*

security marking turvamerkintä
 ▲ *security classification*

security mechanism turvallisuusmekanismi
 ▲ *security architecture*

security module turvamoduuli
 ▶ *secure device, trusted device* ▼ *dongle, hardware key, key chip, smart key, token, USB key*

security monitor turvaohjelma
 ▲ *monitor (s)* ▶ *cracker, cracking program, data protection software, filter, malicious program, ping packet, samurai, spam filter, spam trap, tiger, vulnerability, white hat* ▼ *anti-virus program, honeypot, intrusion detection system, trap (s), virus protection software, virus scanner*

security of supply huoltovarmuus
 ▲ *availability* ▶ *continuity plan, extraordinary circumstances*

security policy turvallisuuspolitiikka
 ▲ *policy, security* ▶ *security awareness, security culture* ▼ *information security policy*

security protocol turvakäytäntö
 ▲ *protocol* ▶ *communication protocol, cryptography, encryption, end-to-end encryption* ▼ *key agreement protocol*

security server turvapalvelin
 ▲ *server* ▶ *proxy (server)* ▼ *authentication server, firewall*

segregation of duties tehtävien eriyttäminen

self-checking code itsevarmistava koodi
 ▲ *check (v), code*

self-encrypting virus itsekoodaava virus
 ▲ *virus* ▶ *chameleon, self-garbling virus, stealth virus*

self-garbling virus itsekoodaava virus
 ▲ *garble, virus* ▶ *chameleon, self-encrypting virus, stealth virus*

sensitive data arkaluonteinen tieto
 ▲ *data, Personal Data Act* ▶ *confidential, data haven, infringement of privacy, privacy, privacy violation, secret (a)*

server palvelin
 ▲ *information network* ▼ *anonymity server, authentication server, mirror server, name server, proxy (server), security server, time stamp server, Web server*

server certificate palvelinvarmenne
 ▲ *certificate*

service huolto (1); palvelu
 ▲ *availability* ▶ *maintenance, malfunction, operation(s)* ▼ *certification service, denial of service, directory service, information service, network service, online service, purging, quality of service, time stamp service*

service network palveluverkko
 ▲ *network* ▶ *information network, open network, value added network*

serviceable käyttökuntoinen
 ▶ *availability, maintainability, usability*

session hijacking istunnon kaappaus
 ▲ *cybercrime, hijacking, network crime* ▶ *address hijacking, impersonation, infringement, masquerading, spoofing, violation of right*

session key kertatunnus
 ▲ *key* ▶ *dynamic password, one-time key*

shredder silppuri
 ▲ *residual data, residue* ▶ *dumpster diving, scavenging*

sign-on sisäänkirjaus
 ▶ *authentication, identification, log-in, recognition, verification* ▼ *introduction, single sign-on*

signals intelligence signaalitiedustelu
 ▲ *cyberwarfare, electronic warfare, information warfare, intelligence (2)* ▶ *scattered electromagnetic radiation* ▼ *communications intelligence, electronic intelligence*

signature (1) allekirjoitus
 ▲ *authentication, verification* ▶ *identifier, label*
 ▼ *digital signature, electronic signature*

signature (2) (erikois)piirre; tekotapa
 ▶ *feature*

single sign-on kertakirjaus
 ▲ *log-in, login, sign-on*

skim kuoria
 ▶ *pirate copy, unauthorized user*

smart card toimikortti
 ▲ *card* ▶ *chip card, smart key* ▼ *electronic identity card, master card, multi-use smart card*

smart key toimiaivain
 ▲ *authority, key, security module* ▶ *chip card, dongle, hardware key, smart card* ▼ *token, USB key*

smart weapon täsmäase
 ▶ *electronic warfare*

sniff nuuskia
 ▲ *passive attack, spyware* ▶ *monitor (v), supervise* ▼ *packet sniffer, sniffer*

sniffer nuuskin
 ▲ *monitor (s), sniff* ▶ *network analyzer, packet filter, packet sniffer, ping packet, root kit* ▼ *packet sniffer*

social engineering (käyttäjän) manipulointi

▶ *business espionage, impersonation, masquerading, spoofing, theft of identity, user, user profile*

software

▼ *access control software, data protection software, virus protection software*

software security ohjelmistoturvallisuus

▲ *information security, security* ▶ *administrative and organizational information security, computer security, data security, facilities security, IT security, telecommunications security*

SPAM *spiced ham*

roskaposti

▼ *UCE*

spam (s) roskaposti

▶ *junk mail*

spam (v) lähettää roskapostia

spam filter roskapostisuodatin

▲ *filter* ▶ *packet filter, security monitor, tiger, Web filter*

spam trap roskapostiansa

▲ *trap (s)* ▶ *security monitor, tiger*

spamdexing roskaindeksointi

speaker identification puhujan tunnistus

▲ *biometric identification, identification, recognize* ▶ *speaker recognition, speaker verification, speech recognition, voice recognition*

speaker recognition puhujan tunnistus

▲ *biometric identification, recognition, recognize* ▶ *speaker identification, speaker verification, speech recognition, voice recognition*

speaker verification puhujan todennus

▲ *verification* ▶ *speaker identification, speaker recognition*

speech recognition puheentunnistus

▲ *recognition, recognize* ▶ *speaker identification, speaker recognition, voice recognition*

spoofing tekeytyminen

▲ *active attack, attack* ▶ *address hijacking, commandeer, cracking, data trespass, disinformation, hijack, honeypot, impersonation, IP spoofing, man-in-the-middle attack, masquerading, mock-ingbird, piggybacking, rogue program, session hijacking, social engineering, tailgating* ▼ *IP spoofing, mimic*

spyware urkintatekniikka

▲ *ware* ▶ *attack, business espionage, dumpster diving, information security technology, intelligence (2), scavenging, user profile* ▼ *eavesdropping, finger (v), intercept, key logger, lawful interception, PING, pixel beacon, remote surveillance, sniff, telemonitoring, Web bug, wiretapping, (legal) wiretapping*

SSO *single sign-on*

kertakirjaus

▶ *USERID*

stamp (s) leima

▶ *certificate, characteristic, feature, identifier, label, nonrepudiation* ▼ *time stamp*

stamp (v) leimata

▶ *certification, identify*

standard standardi

▶ *norm, property, rule* ▼ *information security standard*

standby valmiustila; varallaolo

▲ *availability, failure, malfunction, preparedness* ▶ *backup, backup hardware*

stealth virus piilovirus

▲ *virus* ▶ *hoax virus, retrovirus, self-encrypting virus, self-garbling virus*

steganography piilokirjoitus

▲ *cryptography* ▶ *cryptogram, encryption* ▼ *digital fingerprint, digital watermark, encrypted message*

stream cipher jonosalaus

▲ *cipher, cryptography, encryption* ▶ *block cipher* ▼ *asynchronous stream cipher, one-time pad, synchronous stream cipher*

strong authentication vahva tunnistus

▲ *authentication, electronic identification* ▶ *public key method, strong encryption, weak authentication*

strong encryption vahva salaus

▲ *encryption* ▶ *computationally secure, strong authentication, weak encryption*

strong encryption algorithm vahva salausalgoritmi

▲ *encryption algorithm*

structured error handling rakenteinen virheenhallinta

▲ *error, mistake* ▶ *testing*

sunshine law asiakirjajulkisuuslaki

▲ *law*

superuser pääkäyttäjä (1)

▲ *user* ▶ *administrator, authorized user*

supervise valvoa

▶ *back up, check (v), monitor (v), secure (v), sniff* ▼ *control (1), supervision*

supervision valvonta

▲ *monitor (v), supervise* ▶ *audit (s), Coercive Measures Act, control (1), filtering, lawful access, monitoring* ▼ *access control, control failure, passage control, physical access control, remote surveillance, telemonitoring*

supervisory ohjaus-; valvonta-

suppress pimittää

▶ *congestion, deny, encrypt, inhibit*

symmetric block cipher symmetrinen lohkosalaus

▲ *block cipher*

symmetric encryption symmetrinen salaus

▲ *encryption* ▶ *asymmetric encryption, hybrid encryption, secret key* ▼ *key agreement protocol*

synchronous stream cipher tahdistettu jonosalaus

▲ *stream cipher* ▶ *asynchronous stream cipher*

system

▼ *backup system, computer system, cryptosystem, data processing system, encrypting file system, fallback system, front end system, information system, intrusion detection system, positioning system*

system administrator järjestelmä vastaava

▲ *administrator, information system*

system description järjestelmäseloste

▲ *information system* ▶ *privacy statement* ▼ *personal file description*

system maintenance systeemin kunnossapito

▲ *maintenance*

system owner järjestelmän omistaja

▶ *authority, control (1), management, registrar*

systems audit tietoturvatarkastus

▲ *audit (s), information security norm* ▶ *information audit, information security audit* ▼ *loophole, risk analysis, security breach*

systems auditor atk-tarkastaja

▲ *auditor* ▶ *information system*

T

tailgating peesaus

▶ *access control, crack, impersonation, masquerading, piggybacking, spoofing*

tamper peukaloida; puuttua (häiritsevästi); väärentää

▲ *interference* ▶ *forge* ▼ *data tampering*

tandem kahdennettu; kaksois-

▶ *mirror (s,a)*

taxonomy luokitus

▲ *classify* ▶ *classification*

technical assurance tekninen turvaaminen

▲ *assurance, security*

technique

▼ *brute force technique, salami technique*

technology

▼ *information security technology, privacy enhancing technology*

telecommunications management network telehallintaverkko

▲ *management, network, network management*

telecommunications security tietoliikenneturvallisuus

▲ *Communications Market Act, information security, security* ▶ *communications crime, computer security, facilities security, network management, software security* ▼ *virus alert*

telecommuting etätyö

▶ *remote work, telework*

telemaintenance etähuolto

▲ *maintenance* ▶ *fault, monitor (s), network service, remote surveillance, telemonitoring*

telemonitoring televalvonta

▲ *control (1), monitor (v), spyware, supervision* ▶ *Coercive Measures Act, eavesdropping, lawful interception, monitor (s), remote surveillance, telemaintenance, wiretapping, (legal) wiretapping*

telework etätyö

▲ *work* ▶ *local area network, network service, remote access, remote connection, remote login, telecommuting*

test (v) testata

▶ *check (v), correct (v), debugging, inspect, mistake* ▼ *testing*

test data testiaineisto

▲ *data*

testing testaus

▲ *test (v)* ▶ *authentication, check (v), check-out, debugging, inspect, structured error handling, verification* ▼ *desk checking*

text

▼ *ciphertext, clear text, encrypted text*

theft of identity identiteettivarkaus

▲ *computer crime, identity* ▶ *commandeer, hijack, password, social engineering*

threat uhka

▲ *availability* ▶ *damage, hazard, perpetrator, preparedness, risk, security, vulnerability* ▼ *compromise (v), computer sabotage, insider threat, outside threat*

threat analysis uhka-analyysi

▲ *analysis, information security planning* ▶ *risk analysis, vulnerability analysis*

tiger turvaohjelma

▶ *cracker, cracking program, data protection software, filter, malicious program, ping packet, samurai, security monitor, spam filter, spam trap, vulnerability, white hat* ▼ *anti-virus program, honeypot, intrusion detection system, trap (s), virus protection software, virus scanner*

time bomb aikapommi

▲ *bomb, malicious program, rogue program*
▶ *watchdog timer*

time stamp aikaleima

▲ *notarization, stamp (s)* ▶ *nonrepudiation*

time stamp server aikaleimapalvelin

▲ *authentication server, server*

time stamp service aikaleimapalvelu

▲ *network service, public key infrastructure, service, trusted (third) party* ▶ *network notary*

time-out aikakatkaus

▲ *operation(s)* ▶ *watchdog timer*

TLD *top level domain (name)*

ylätason verkkoalue tai -tunnus

token poletti

▲ *authentication, security module, smart key, verification*

tolerant sietoinen; sietävä

▶ *resilient* ▼ *fault tolerant*

top secret erittäin salainen

▲ *secret (a), security classification* ▶ *official document*

trace packet jäljityspaketti

▲ *network management, packet* ▶ *network trace, traceability*

traceability jäljitettävyys

▲ *property* ▶ *audit trail, auditability, repeatability, trace packet*

trail jälki; ketju

▼ *audit trail*

trap (s) ansa

▲ *security monitor, tiger* ▶ *cracker, cyberhacker, decoy, intrusion detection system, quarantine (v)*
▼ *entrap, honeypot, spam trap*

trap door salaovi

▲ *access (s), loophole, passive attack, security breach* ▶ *back door, covert channel, entrap, loophole, security breach, Trojan horse*

trigger (s) liipaisin

▲ *computer virus, logic bomb, virus* ▶ *fault threshold, payload*

Trojan horse troijanhevonen

▲ *malicious program, rogue program* ▶ *computer virus, root kit, trap door, virus*

trusted luotettava; uskottu

▶ *secure (v)*

trusted device varmlaite

▶ *secure device, security module* ▼ *authorization terminal*

trusted (third) party luotettu taho

▲ *confidentiality, reliability* ▶ *audit (s), (public) authority, certificate authority, Electronic Signatures Act, escrow, public key infrastructure* ▼ *accreditation, certificate, network notary, time stamp service*

TTP *trusted third party*

luotettu taho

tunneling tunnelointi

▲ *data network*

U

UCE *unsolicited commercial e-mail*

mainosroskaposti

▲ *SPAM*

unauthorized luvaton

▲ *authorize, rule* ▶ *illegal* ▼ *pirate copy*

unauthorized user luvaton käyttäjä

▲ *authorization, usage rights, user* ▶ *authorized user, cybersquatting, defr, illegal disclosure, intrusion, penetration, skim, war driving*

unavailability käytettävyyden estyminen

▲ *availability* ▶ *congestion, denial of service*

unidentified use tunnisteen käyttö

▲ *identify, use* ▶ *anonymity server, anonymous use, identifier, label*

uninterrupted power supply katkoton tehonsyöttö

▲ *availability, operations security* ▶ *no-break power supply*

usability käytettävyys (2); käyttökelpoisuus

▲ *property* ▶ *availability, integrity, serviceable*

usage rights käyttövaltuudet

▲ *authority, right* ▶ *access right, authorization*
▼ *access authority, unauthorized user*

USB key USB-avain

▲ *dongle, hardware key, key, security module, smart key*

use käyttö (1)

▲ *information system* ▶ *utilization* ▼ *access right, anonymous use, authority, availability, hacking, multi-use smart card, remote access, remote login, restricted use, unidentified use*

user käyttäjä

▲ *information system* ▶ *password, social engineering* ▼ *access control software, anonymous user identity, authorized user, hacker, introduction, superuser, unauthorized user*

user ID käyttäjätunnus

▼ *anonymous user ID*

user identifier käyttäjätunnus

▲ *identifier* ▶ *personal identification number*
▼ *pseudonym*

user profile käyttäjäprofiili

▲ *profile* ▶ *network trace, privacy protection, social engineering, spyware*

USERID *user ID*

käyttäjätunnus

▶ *SSO*

utilization käyttö (1)

▲ *information system* ▶ *use* ▼ *access right, authority, availability, hacking, remote access, remote login*

V

validate osoittaa kelvolliseksi

▶ *accept, certify, verify*

validation kelpuus

▲ *validity* ▶ *accreditation, authorization*

validity kelpoisuus

▲ *quality* ▶ *accuracy, authenticity, integrity, verifiability* ▼ *check (v), inspect, validation*

value added network palveluverkko

▲ *network* ▶ *information network, open network, service network*

verifiability todennettavuus

▲ *authenticate, property, quality, verify* ▶ *auditability, identifiability, reliability, repeatability, validity*

verification todennus

▲ *authenticate, verify* ▶ *authentication, certification, identification, introduction, log-in, password, recognition, sign-on, testing* ▼ *challenge-response method, credential(s), password identification, signature (1), speaker verification, token*

verify tarkistaa (2); todentaa

▲ *accuracy* ▶ *assure, authenticate, back up, check (v), ensure, secure (v), validate* ▼ *authentication, verifiability, verification*

violation of information security tietoturvaloukkaus

▲ *information security*

violation of right oikeudenloukkaus

▲ *right* ▶ *computer crime, damage, information security breach, infringement, interference, session hijacking* ▼ *computer crime, infringement of privacy, privacy violation*

virtual private network VPN-verkko

▲ *information network, network, private network*
▶ *closed network, firewall, private network*

virus virus

▲ *malicious program, replicator, rogue program*
▶ *anti-virus program, bacterium (pl bacteria), computer virus, epidemic, infection, quarantine (v), Trojan horse, virus protection software, worm*
▼ *boot sector virus, e-mail virus, file infector virus, hoax virus, macro virus, parasite, parasitic virus, payload, retrovirus, self-encrypting virus, self-garbling virus, stealth virus, trigger (s), Web virus*

virus alert virusvaroitus

▲ *telecommunications security* ▶ *intrusion detection system, rogue program, virus hoax*

virus hoax virusvalhe

▲ *hoax* ▶ *disinformation, hoax virus, virus alert*

virus protection software viruksentorjuntaohjelma

▲ *protection, security monitor, software, tiger*
▶ *anti-virus program, computer virus, intrusion detection system, virus, virus scanner*

virus scanner virustutka

▲ *security monitor, tiger* ▶ *anti-virus program, intrusion detection system, monitor (s), virus protection software*

vital application elintärkeä sovellus

▲ *priority classification* ▶ *continuity plan*

voice recognition äänentunnistus

▲ *biometric identification, recognition, recognize*
▶ *password identification, speaker identification, speaker recognition, speech recognition*

VPN *virtual private network*

vulnerability haavoittuvuus

▲ *property* ▶ *bastion host, cyberwarfare, exposure, hazard, information security, information warfare, preventive measures, risk, risk management, robustness, secure host, security monitor, threat, tiger* ▼ *loophole, security breach*

vulnerability analysis haavoittuvuustutkimus

▲ *analysis* ▶ *risk analysis, threat analysis*

vulnerability scan haavoittuvuusskannaus

▲ *probe (s), scan (s)* ▶ *port scan*

W

war dialing modeemiyökkäys

▲ *attack, cracking, data trespass* ▶ *phreaking, war driving*

war driving loiskäyttö

▲ *attack* ▶ *derf, unauthorized user, war dialing*

ware tietoteknistä välinettä kuten valmistohjelmistoa tarkoittava pääte

▼ *copyrightware, malware, spyware*

warfare

▼ *command-and-control warfare, cyberwarfare, electronic warfare, information warfare, infrastructure warfare, network-centric warfare*

Wassenaar arrangement Wassenaar-järjestely

▶ *dual use product*

watchdog timer vahtiajastin

▲ *availability, monitor (s)* ▶ *time bomb, time-out*

weak authentication kevyt tunnistus

▲ *authentication, electronic identification*
▶ *strong authentication, weak encryption*

weak encryption kevyt salaus

▲ *encryption* ▶ *brute force attack, strong encryption, weak authentication*

Web beacon verkkojäljite

▶ *cookie* ▼ *pixel beacon, Web bug*

Web browser web-selain

▶ *applet*

Web bug piilojäljite

▲ *bug, spyware, Web beacon* ▶ *pixel beacon*

Web filter web-suodatin

▲ *filter* ▶ *packet filter, spam filter*

Web server web-palvelin

▲ *server*

Web virus web-virus

▲ *virus* ▶ *e-mail virus, file infector virus*

webmaster web-vastaava

▲ *management* ▶ *network administrator*

white hat valkolakki

▶ *cracker, cyberhacker, hacker, samurai, security monitor, tiger*

WinNuke Windows-pommi

▶ *blue bomb, ping of death*

wireless PKI langaton julkisen avaimen järjestelmä

▲ *PKI*

wiretapping salakuuntelu

▲ *communications crime, cybercrime, intelligence (2), network crime, spyware* ▶ *cracking, crosstalk, data trespass, eavesdropping, employee monitoring, intercept, key logger, lawful interception, probe (s), remote surveillance, telemonitoring*

(legal) wiretapping telekuuntelu

▲ *spyware* ▶ *Coercive Measures Act, eavesdropping, employee monitoring, intercept, lawful interception, remote surveillance, telemonitoring*

work

▼ *remote work, telework*

workflow asiankäsittely

▶ *case processing*

working archive käyttöarkisto

▲ *archive (s)* ▶ *backup archive, security archive*

worm mato

▲ *malicious program, replicator, rogue program*
▶ *bacterium (pl bacteria), computer virus, infection, virus*

X

X-rated alaikäisiltä kielletty

▶ *illegal*

Z

zombie kaapattu verkoasema; orja

▲ *commandeer, hijack* ▶ *distributed denial of service attack, hijack, leapfrog attack*

VM:n ja VAHTI:n tietoturvaohjeita (<http://www.vm.fi/vahti>)

- Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003
- Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003
- Suositus turvallisen etäkäytön arkkitehtuurista, VAHTI 2/2003
- Tunnistaminen valtionhallinnon verkkopalveluissa, VM 6/01/2003
- Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003
- Arkaluonteisten kansainvälisten aineistojen käsittelyohje, VAHTI 4/2002
- Etätyön tietoturvaohje, VAHTI 3/2002
- Tietoteknisten laittilojen turvallisuussuositus, VAHTI 1/2002
- Tietotekniikan turvallisuus ja toiminnan varmistaminen, VM ja PTS, 2002
- Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001
- Tietotekniikkahankintojen tietoturvallisuustarkistuslista, VAHTI 6/2001
- Sähköpostin ja lokitietojen käsittely, VAHTI 5/2001
- Sähköisten palveluiden ja asiointin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001
- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje, VAHTI 4/2000
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999

- Suositus toimitilaturvallisuuden huomioonottamisesta valtionhallinnossa, VM 1/01/99
- Tietoturvallisuuden tulosohjaus ja kehittämisvälineet, VAHTI 2/1997

VAHTI



VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin: (09) 160 01
Telefaksi: (09) 160 33123
www.vm.fi

4/2003
VALTIONHALLINNON
TIETOTURVAKÄSITTEISTÖ

ISSN 1455-2566
ISBN 951-804-404-8