Tietoturvallisuuden jaottelu täydennettynä linkeillä aiempiin materiaaleihin

Seuraava kappale, alla olevan pitkän luettelon linkittömät pääkohdat 1–11 ja aivan lopussa oleva selitys ovat samat kuin JOP-hankkeeseen kuuluvan tietoturva-wikin jaottelusivu. Tämän dokumentin tarkoitus on täsmentää jaottelua ja tarjota aineistoa, josta wikiä voi ruveta rakentamaan. Tämä ei onnistu pelkällä kokoamisella, vaan kopioinnissa tarvitaan JOP-määritysten mukaan editointia, merkkausta ja monesti myös pilkkomista, sillä tarjolla oleva aineisto on lyhytsanaisuudessaankin turhan pitkää verkkotekstiksi. Luonnollisesti laadun parantaminen ja sisällön täydentäminen tuovat lisätarvetta pilkkomiselle.

Tällä sivulla tietoturvallisuus (TT) on järjestetty yhdenlaisella logiikalla 11 **luokkaan**. Kukin luokka lohkaisee tietoturvan kentästä vuorollaan jonkin palasen, jota luokkaan kuuluvien aihealueiden osittaiset (ja alustavat) luettelot täsmentävät. Luokkajaon loppupuolella jaettavana oleva kenttä on siis alkua suppeampi ja luokkien otsikot on ymmärrettävä siinä yhteydessä. Monesta alkupuolen aiheesta mennään jälkipuolella paljon syvemmälle – eli senkään puolesta tämä ei ole käsikirjamainen jaottelu. Jaottelun yleistä logiikkaa on selitetty sivun lopussa.

Toisen tason kohdat (merkkinä o) ovat **aihealueita** ja kolmannen tason kohdat (•) **aiheita**. Aiheet on tässä dokumentissa määritelty löyhästi linkeillä TTY:n TT-kursseilta poimittuihin otsikoihin, enimmäkseen ydinsivutasoisiin. Monessa kohdassa useita kurssimateriaalin otsikoita on ryhmitelty samaksi aiheeksi. Vain muutamiin aiheisiin on toistaiseksi lisätty jokin kuvaavampi kokoava nimi, vaikka tavoitteena JOP-määrityksen mukaan on, että vasta aiheiden sisällä on ydinsivuja.

Linkit ovat TT-peruskurssiin (ilman lisämerkintää), jatkokurssin perusosaan, merkintänä (2-A) ja jatko-osaan, (2-B). Näiden kohteina on verkkomateriaalin sivu ja otsikoina ko. sivujen alkuperäiset otsikot (mahdollisesti tiivistettyinä). Verkon tietoturva -kurssin luentomateriaalin viitteinä on [V-TT ja sivunumero] ja Kryptoprotokollat -kurssin materiaalin viitteinä [KryPro]. Jälkimmäisten tarkat kohteet löytyvät muutaman arkin mittaisilta verkkosivuilta. Lisäksi on muutama linkki seminaaritöihin. Täydennyksenä on useita linkittömiä aiheita.

Tästä luettelosta **puuttuu** linkitys TTY:n tarjontaan kuuluviin kursseihin Matemaattinen kryptologia ja Tietoturvallisuuden johtaminen, jotka liittyvät jäsennyksen luokkiin 6 ja 8. Luokkaan 11 liittyy Turvallisen ohjelmoinnin kurssi, jota ei myöskään ole vielä linkitetty tähän. Se tarjoaa luokalle 11 todennäköisesti nykyistä toimivamman jäsennyksen.

1. Tietoturvallisuuden määrittelyä uhkien kautta

Mitä pitää turvata ja miksi, mikä voi mennä vikaan, mikä tai kuka uhkaa, miten uhkia kartoitetaan, mikä on uhkamalli? Yksityiskohtaisia uhkia tulee esille myöhemmissä luokissa.

> *Tietoturvallisuuden yleiset määritelmät (käsitteen sisältö: tietojenkäsittelyrauha, CIA etc), uhkaavat luonnonvoimat, tekniset ongelmat, tahalliset uhkat (hakkerin etiikasta haittaohjelmiin), inhimilliset virheet, hallinnolliset puutteet.*

- Tietoturvauhkien jäsentelyä
  - Yleistä uhkista (mitä tiedolle voi tapahtua); Uhkien jaottelu BSI:n mukaan; Missä tietokoneturva pettää (2-A); Tietoverkon turvaongelmia; Hyökkäysten taksonomia
  - Tietoturvakäsitteen sisältö; Tietoturvapoliittisia määritelmiä (2-A)
  - Uhka-analyysi (2-A); Uhkamalli
- Luonto ja muu ei-tiedollinen tai ulkonainen
  - Ihmisettömiä fyysisiä uhkia; Tuli, vesi, maa, ilma, sähkö, …

- Poikkeusolot, ilkivalta, terrorismi, …
- Virheet tai puutteet, joissa asiaan liittyvä ihminen on osallinen (ks. BSI-luettelot)
  - Inhimillinen taso
  - Tekniikan taso
  - Hallinnon taso
- Pahat ohjelmat
  - Pahat ohjelmat
  - Virusten ominaisuuksia; Virusten anatomiaa (2-B)
  - Hyökkääjän työkaluja (2-A)
  - Epidemiologiaa (2-B); Immunologiaa (2-B)
- Tahalliset uhat (tiedolliset, paitsi "koodiaseet")
  - Tietorikollisuuden piirteitä (alustava wiki-sivu); Hyökkääjät ja hyökkäykset (V-TT s. 4); Hakkerin etiikka
  - Tietomurrot
  - Vakoilu
  - Väärinkäyttö
  - Palvelunesto
  - Roskaposti
  - Identiteettivarkaudet
  - Huijaukset

2. Tietoturvatoimien yleisiä piirteitä

Tietoturvallisuuden yleiset periaatteet, näkökulmat, jaottelut, arkkitehtuurimallit, organisaatiot, standardit, tiedonlähteet, mittaaminen, testaaminen, vakuuttuminen, teoriat, tutkimus.

- Tietoturvatoimien viitekehys ja jaottelu
  - Mitä on tieto ja tietojenkäsittely
  - Tietoturvamekanismien jäsentely: TT-mekanismien yleisesittely; Verkon turvamekanismeja (2-A) ; Erottelumekanismeja (2-A); TT-mekanismien piirteitä (2-A)
  - Tietoturvakäsitteen ulottuvuus (*sisältö* on **Uhkien** kohdalla)
- Yleiskäyttöisiä tai abstrakteja tietoturvaperiaatteita
  - Turvallinen suunnittelu; (ks. myös V-TT s. 11–12); Turvasuunnittelun yleisperiaatteita;
  - Tietoturvasuunnittelun malliratkaisut (2-A)
  - Nimeäminen (2-A); Nimeämisestä hajautetuissa järjestelmissä (2-B)
- Tieto tietoturvasta
  - Päivittäisiä tietoturvatiedon lähteitä
  - Kooste TT-ohjeistoista (2-A)
  - Koulutuksesta (2-A)
  - Tiedostuksesta ja tiedon lähteistä (2-A) ; Tietoturvakatsauksia ja -kampanjoita (2-A)
  - Lähdeaineistoja: Kirjoja ja painatteita suomeksi; Suomalaisia seittiaineistoja; Ulkomaisia seittiaineistoja; Vieraskielisiä kirjoja ja painotuotteita
- Tietoturvan yleisiä standardeja
  - Tietoturvastandardeja
  - BS7799 (2-B)
  - Common Criteria: CC, käyttö (2-B) ; CC, rakenne (2-B) ; CC, toiminnallisuus (versio 2) (2-B); CC, vakuuttavuus (versio 2) (2-B)
  - SSE-CMM (2-B)
- Tietoturvan arviointi (sertifioinnin hallinto on luokassa 6)
  - Miten tietoturvasta voi vakuuttua
  - Turvallisuuden arvostaminen [V-TT s. 20–21]
  - Mittaaminen ja testaaminen
- Tietoturvan tekijät

        - Tietoturva työnä
        - Tietoturvakatsauksia ja -kampanjoita (2-A)
        - Tietoturvayrityksiä (2-A)
        - Tietoturvallisuuden tutkimuksesta (2-B)
    - Tietoturva(politiikan) teoriaa
        - Tietoturvapolitiikan mallinnus (2-A); Perusmallit (2-A)
        - Monitasoinen ja hilamainen luokittelu (2-B); Hilamaiset turvamallit (2-B); Hilamaisten turvamallien kritiikki (2-B)
        - Eheysmalli, Clark-Wilson (2-B)
        - Kiinan muuri (2-B)
        - Politiikkakieliä: Muita politiikkakieliä (2-B)

3. Toteutuvien uhkien käsittely

(Muissa kohdissa tämän jälkeen pääpaino on proaktiivisessa turvallisuudessa.)

Mitä voidaan tehdä, jos uhkaa ei ole osattu tai voitu torjua, vaan se toteutuu? Sitä enemmän mitä paremmin on valmistauduttu.

> *Reagointiin valmistautuminen (suunnittelu, hankinnat, lokit ym.), havainnointi (ml. virustorjunta ja IDS), vaste, toipuminen, jatkuvuus, jäljitys (forensiikka) ja jälkityöt.*

- Tunkeutumisen havainnointi (Tunkeutumisiin reagoinnin prosessi [V-TT s. 41–49])
    - Yleistä suodatuksesta ja tunkeutumisten havainnoinnista
    - Lokitietoja; *Lisää* [V-TT s. 22–25]
    - Miten tunkeutumisen voi havaita; Tunkeutumisten havaitseminen ja hoito (2-A); Tunkeutumisen havainnoinnin tekniikoista (2-B); myös [V-TT s. 26–28 ja Sem-k04]
- Haittaohjelmien torjunta
    - Virusten torjunta (yleisesti ja käytännössä)
    - Haittaohjelmien torjuntaohjelmien periaatteita
- Tietoturvapoikkeaman vaste
    - Tunkeutumisen reagointiprosessin osa …
    - Palveluneston käsittely [Sem-k05]
- Tapahtumien jäljitys
    - Forensiikkaa (2-A); *myös* [Sem-k08]
    - Jälkien tulkintaa ja kokoamista (2-B)
- Selviytyminen
    - Suunnittelu ja valmistautuminen: Vastesuunnitelma; Toipumissuunnitelma (2-A) ; Jatkuvuussuunnitelu
    - Tietojenkäsittelyn vakuuttaminen (2-A)
    - Tunkeutumisen jälkityöt

4. Yhteiskunnan tietoturvaominaisuudet

> Tietosodankäynti (myös yritysten näkökulmasta), strategiat, säännökset (ml. tietorikokset, tekijänoikeudet, tietosuoja), tietoyhteiskunta.

- Tietoturvalaillisesta sääntelystä yleisesti
    - Millaista sääntelyä liittyy tietoon
    - Tietoturvallisuuden poliittisia ulottuvuuksia (2-A)
    - Valtionhallinnon tietoturvallisuusohjeet
    - Vastuu ja tietoturva (2-A)
- Rikoslaki ja tietoturva
    - Tietomurto ynnä muut rikoslaittomuudet

        - Tietorikosten sääntelystä kansainvälisesti [Sem-s07, s 3–7]
    - Henkilön tietojen suoja
        - Yleisesti yksityisyydestä ja tietosuojasta
        - Tietosuojan lainsäädäntö
        - Tietosuojavaltuutettu ja -vastaava
    - Aineettoman omaisuuden jakelu ja suojaus
        - Yleistä tekijänoikeuksista
        - Kopiosuojauksista (2-A)
        - Lisensseistä yleistä (2-A); Oikeuksien luovuttamisia lisensseillä tai muuten (2-A)
        - Vesileimaus (2-A)
    - Sähköinen asiointi
        - Sähköisen asioinnin perusteista; Sähk. asioinnin TT-ohjeet (2-A)
        - Sähköinen henkilökortti
    - Sähköinen kaupankäynti
        - Yleistä e-kaupasta
        - Sähköinen maksaminen
        - Verotuksesta (2-A)
    - Tietoyhteiskunnan tietoturva
        - Kansallinen TT-strategia
        - TT-kulttuuri
        - Tietosodankäynti

5. Yhteisölliset ja yksilölliset tietoturvanäkökulmat

Suoja tiedolta ja huijauksilta, yksityisyyden suoja, käytettävyys, tietoisuus, etiikka ym. inhimilliset tekijät, lisäksi identiteetin ja luottamuksen hallinta.

- Henkilön suoja tiedolta
    - Miltä tiedolta pitää suojautua
    - Seittisisällön suodatus
    - Roskasähköposti; Roskapostin suodatuksesta (2-B); Bayes ja spam (2-B)
- Yksityisyyden toteutusta
    - Evästeet eli selauskuitit
    - Tietokoneen käytön jäljittämisestä
    - Tietojen sanitointi (2-A)
    - Paikannus ja tietosuoja (2-A)
    - Anonymiteetin määrittelyä (2-A); Anonymiteetin toteutusta (2-A); Anonyymi matkaviestintä [KryPro luento 9]
- Inhimillisiä tekijöitä
    - Tietoturvan käytettävyys [Sem-s07]
    - Tietoisuus ja asenteet TT-vaikuttajina [Sem-s08]
    - TT ja etiikka; [Koskinen 99]
- Luottamus
    - Luottamuksen hallintaa (2-B); Verkon turvahallinnan apuvälineitä [V-TT s. 67–69]
    - SPKI/SDSI (2-B)
    - KeyNote (2-B)
- Yhteisöt
    - Yhteistyöverkot [V-TT s. 7–10 ja Sem-k09]
    - Verkkoyhteisöt ja TT; Sosiaalinen VPN [V-TT s. 7–10 ja Sem-k09]

6. Miten turvatoimet valitaan ja hallitaan organisaatiossa?

Hallinnollinen tietoturvallisuus sillä tasolla, jolla puhutaan työntekijöistä, suunnitelmista, euroista yms. mutta ei yleensä biteistä, volteista eikä TCP-porteista.

Strategiat, politiikat, TT:n hallintajärjestelmä, riskien hallinta, henkilöstö, auditointi.

- Tietoturvan rakennusprosessi (≈ mikä on yleensä tarpeellista tehdä)
  - Tietoturva on prosessi; Tietoturvatyön vaiheistus; Yleistä tietoturvan tavoittelusta (2-A); Muuan kokonaismalli turvaprosessista (2-A)
  - Riskianalyysi
  - Tietoturvapolitiikka; myös [V-TT s. 7–10]
- Tietoturvallisuuden hallintajärjestelmä (≈ miten huolehditaan että tarpeellinen tehdään)
  - TT-strategiatyö
  - TT-riskien hallinta
  - TT-politiikan luominen ja toimeenpano
  - TT-suunnitelmien luonti ja toimeenpano
  - Yhteydenpito ja sopimukset
  - Lainmukaisuuden hallinta
  - Resurssienkäytön hallinta
- Henkilöstö
  - Henkilöstöturvallisuus yleisesti
  - Työhön otettavan henkilöstön taustan tarkistukset
  - Työsuhteen päättyminen
  - Valvontaa ja huolenpitoa
  - Turvallisuushenkilöstö; [V-TT s. 13 – 14]
- TT:n arviointi yrityksessä
  - Auditointi [V-TT s. 50–51]
  - Sertifiointi

7. Millainen on tietoturvallinen tapa käyttää ja operoida tietoja ja järjestelmiä?

Käyttöturvallisuus, tietoaineistojen turvallisuus ja muita hyviä käytäntöjä.

Pääsynvalvonta, salasanojen käyttö, lokien keruu, kahdennus (ml. varmuuskopiointi), tiedon elinkaareen liittyvät käsittelyohjeet (mm. milloin salataan/tai allekirjoitetaan sähköposti), erityisiä järjestelmiä kuten terveydenhuolto, viranomaisjärjestelmät.

- Tietoaineistoista
  - Eheystarkasteluja
  - Käytöstä poistettu tieto: Jäännöstieto; Tietojäämistöistä
  - Tietoaineistojen luokituksesta; Tietoaineistojen luokittelun lähtökohtia (2-A) ; Viranomaisaineistojen turvaluokitus ja -merkintä (2-A)
  - Tietoaineistojen käsittelyohjeisto (2-A) ; Henkilöstön ohje ja hyvät tavat (2-A)
  - Verkkotalletuksen turvamenettelyjä (2-A)
- Kahdennukset
  - Varmuuskopioinnista yleisesti; Varmuuskopioinnin suorittaminen (2-A)
  - Muu kahdennus (kuin varmennus)
  - RAID-tekniikka (2-A)
- Käyttäjä
  - Turvallista tiedostojen käyttöä
  - Tietokoneen käytön jälkeen
  - Jälkien peittämisestä
- Pääsynvalvonta
  - Pääsynvalvonnan määrittelyä; Pääsyoikeuksien esittäminen
  - Rooliperustainen pääsynvalvonta (2-B)
  - Käyttäjähallinto (2-A); myös [V-TT s. 52–53]
  - SQL:n pääsynvalvonta (2-A); SQL-injektio
  - Piilokanavat (2-B)

- TT-käytäntöjä joissain tärkeissä tietojärjestelmissä
  - Terveydenhuollon tietoturva ([Sem-k09])
  - Julkisten palvelujen TT-käytäntöjä: koulut, kirjastot, KELA, Yle ym.
  - Viranomaisjärjestelmät: pelastus, poliisi, oikeuslaitos, eduskunta, armeija ym.

8. Kryptologiset menetelmät

Algoritmit, toteutukset, murtaminen, protokollat (ml. autentikointi eri muodoissaan), avaintenhallinta, erikoiset järjestelmät kuten äänestys.

- Avainten hallinnointi
  - Avaimiakin pitää hallinnoida; Avaintenhallinnan peruskäsitteet (2-A); Avainten käytön kontrolli (2-A)
  - Key Escrow (2-A)
  - Julkisen avaimen varmenne; Varmennejärjestelmä, PKI (2-A); Varmennejärjestelmän käytäntöjä (2-A); X.509, varmennestandardi (2-A)
  - Varmennepolitiikka (2-A)
  - Sulkulistan tekniikoita (2-A)
  - Yksilökohtaista kryptologiaa (2-B); *Tarkemmin:* Identiteettipohjainen julkinen avain [KryPro luento 9]
  - Avaintenhallinta ryhmäviestinnässä [KryPro luento 11]
- Yleistä kryptoalgoritmeista
  - Johdanto kryptoalgoritmeihin; Diffuusio ja konfuusio
  - Kryptohierarkia [KryPro luento 12]; Kryptoprimitiivit (2-A)
  - Satunnaisluvuista (2-A)
  - Murtaminen ja algoritmien turvallisuus (2-A); Kryptoanalyysin mekanismeja (2-B)
  - Tiedon piilottaminen (2-A)
  - Kryptokvantteja (2-B)
- Symmetrisiä salausalgoritmeja
  - Johdanto symmetriseen salaukseen; Lohkosalauksen toteutuksesta (2-A)
  - Tärkeitä symmetrisiä salausmenetelmiä
  - DES (2-A)
  - AES (2-A)
  - Vuosalaus (2-A)
- Yksisuuntaista kryptografiaa
  - Tarkistussumma ja yksisuuntainen tiivistefunktio
  - Kryptografinen tiivistefunktio (2-A)
- Epäsymmetrisiä algoritmeja
  - Julkisen avaimen kryptografian idea; Allekirjoituksen idea; Epäsymmetristen algoritmien käytöstä; Digitaalisen allekirjoituksen tekniikkaa (2-A)
  - Modulaarista aritmetiikkaa (2-A); Modulo-algoritmeja (2-A)
  - RSA (2-A)
  - ElGamal (2-A); ElGamal allekirjoittajana (2-A)
  - NTRU-algoritmi (2-A)
  - Sokea allekirjoitus (2-A); Puolisokea allekirjoitus (2-A)
- Kryptoalgoritmien toteuttamista
  - Lohkoalgoritmien moodit (2-A); Uusia kryptomoodeja (2-A)
  - Kryptoalgoritmien formaatteja (2-A)
  - Kryptosysteemien standardeista (2-A)
  - Kryptomoduuleista ja -kirjastoista (2-A); Krypto-ohjelmoinnista (2-A)
- Yleistä kryptografisista protokollista
  - Kryptoprotokollan käsite; Kryptoprotokollan olemuksesta (2-A); Arviointiperusteita ja luokittelua [KryPro luento 11]
  - Suunnitteluperiaatteita [KryPro luento 4 ja 5]; *Täydennystä* [KryPro luento 12]

        - Aikaleimauksesta (2-A)
    - Autentikointi
        - Autentikoinnin perusteet; Tiedettyyn perustuva autentikointi (2-A)
        - Salasana-autentikointi: Salasanojen valinta- ja käyttöohjeita; Näennäinen haaste-vaste -menetelmä; Kertakäyttösalasanat (2-A); Salasanajärjestelmän toteuttamisesta (2-A); Salasanojen tallennuksen tekniikka (2-A)
        - Autentikoinnin protokollista (2-A); Haaste-vaste -menetelmä yleisesti; Haaste-vaste epäsymmetrisellä tiedolla (2-A); Perusprotokollat [KryPro luento 2]
        - Salasanojen vahvistaminen (2-B); Tarkemmin [KryPro luento 5]
        - Autentikointipuu [KryPro luento 3]
    - Avaintenvaihto
        - Avaimesta sopimisen tavat
        - Diffie-Hellman -avaintenvaihto (2-A)
    - Erikoisia protokollia
        - Salaisuuden jakaminen (2-A)
        - Bittiin sitoutuminen (2-A); Rahanheitto (ja korttipeli) [KryPro luento 6]
        - Erityisiä allekirjoituksia (2-A); Kieltämätön allekirjoitus (2-B)); Allekirjoitusten luokittelua [KryPro luento 8]
        - Äänestysprotokolla (2-A); *Tarkemmin* [KryPro luento 6]
        - Bittikäteinen (2-A); Jäljittyvä anonyymi bittikäteinen (2-B); Anonyymin bittikäteisen laajennuksia [KryPro luento 3]
        - Kaupankäynnin ja maksamisen protokollista; Yleistä [KryPro luento 3]; Reilu vaihto [KryPro luento 9B ja 8B]; Mikromaksaminen [KryPro luento 3]; Huutokauppa [KryPro luento 7]
        - Valtuuttamisen protokollia [KryPro luento 8 ja 8B]
        - Vedonlyönti [KryPro luento 10]
        - Unohtava tiedonsiirto ja salattu myynti (2-B); *Tarkemmin* [KryPro luento 7 ja 7B]
        - Nollatieto; Haaste-vaste nollatiedolla (2-A); Hieman ZK-todistuksista [KryPro luento 8]
    - Protokollien verifiointi
        - Yleistä verifioinnista
        - Logiikka [KryPro luento 9B]
        - Prosessialgebra [KryPro luento 9B ja 11B]
        - Ranta-avaruudet [KryPro luento 12B]

9. Fyysisiä ja laitteistoihin liittyviä tietoturvanäkökulmia

Kulunvalvonta, laitetilat, sähkönsaanti, peukaloinnin torjunta, biometriikka, turvalaitteet, luotetut arkkitehtuurit, kriittiset järjestelmät ja teollisuusautomaatio, hajasäteily.

- Fyysisiin uhkiin varautumista tai fyysistä varautumista uhkiin
    - Tuli
    - Vesi ja muut aineet
    - IT-laitetilojen turvallisuussuosituksen fysiikkaa (2-A)
    - Kulunvalvontaa (2-A)
    - Sähkön laatu ja saanti (2-A)
    - Hajasäteily (2-A)
- Peukaloinnin sietokyky
    - Fyysisen pääsyn rajoittaminen
    - Kopiointi ja väärentäminen
    - Laitteistojen turvallisuudesta
    - Toimikortti; Toimikortin turvallisuudesta
    - PUF (2-B)
    - Luotettu tietojenkäsittely ja isoveli (2-A)
- Turvakriittisten laitteiden tietoturva (sulautetut ohjelmistot ovat luokassa 11)
    - Liikennevälineet

        - Sairaalat
        - Teollisuus
    - Biometriikka

10. Tietoverkon ja liikkuvan tiedon turvaaminen

Tietoverkko on kaikenlaisen tietojenkäsittelyn pohjalla nykyään. Tässä hyödynnetään vahvasti edellä olevia tietoja, etenkin kryptologiaa. Monet asiat ovat siten jatkotasolla, mutta perustasolle laaditaan niitä varten tähänkin kontekstiin johdantosivuja.

> *Langallisen / langattoman yritysverkon / runkoverkon / satunnaisverkon turvallinen rakenne (laitteineen) ja hallinnointi; suodatus; protokollien TT ja käytännön TT-protokollat (esim. HTTP ja SSL) ; erityiset järjestelmät kuten p2p, digi-tv, WLAN, Bluetooth, 3G, RFID. Haavoittuvuustestaus.*

- Tietoverkon tietoturva
    - Kooste [V-TT s. 58–60]
    - Verkkoturvan opiskelusta ja harjoittelusta [Sem-k08]
- Verkkokerroksen turvamekanismi
    - IPsec: Yleistä IPSecistä; IPSec: ESP ja AH (2-A); IPSec, kokonaisuus ja arviointia (2-A); IPSec: IKE (v1), vaiheet (2-A); IPSec: IKE (v1), autentikointitavat (2-A) ; IPSecin toteuttamisesta (2-A)
    - HIP (2-B)
- Autentikointitoteutuksia
    - Kertakirjautuminen; Bittipasseista Kerberokseen (2-A)
    - Kerberoksen toiminta (2-A); Kerberos-lippuja (2-B); Kerberoksen toimialueista (2-B)
    - AAA (2-A)
    - Langattoman pääsyn autentikointi [KryPro luento 12]
- Etäkäyttö; myös [V-TT s. 54–56]
    - VPN ja etätyö; Liikkuva käyttäjä [Huhtanen 08]
    - Yleistä etäyhteyksistä; VPN-tunneloinnin toteutuksesta (2-A)
    - Yleistä SSH:sta; SSH (2-A)
- Langaton viestintä
    - Langattomuus
    - Matkapuhelimen tietoturvasta; GSM-autentikoinnista ja -salauksesta (2-A)
    - WLAN (2-A); *myös* [V-TT s. 73–74];
- Samoiluturvaa (WWW)
    - Seittiselailun turvakysymyksiä
    - Selaajan tietoturva
    - SSL: Yleistä SSL:stä; SSL ja verkkokauppa; SSL-protokolla (2-A); SSL-kättely (2-A)
    - Seittipalvelimen turvallisuus (2-A); *myös* [V-TT s. 32–35]
- Sähköposti
    - Sähköpostin tietoturvakysymyksiä; Vastauksia verkon ylläpitäjän kannalta [V-TT s. 29–31]
    - PGP yleisesti; PGP:n algoritmit ja niiden käyttö (2-A); PGP:n avainrenkaat (2-A)
- Hajautetut järjestelmät
    - DNS [V-TT s. 73]
    - CORBA-turvallisuus (2-A)
    - Web services -turvallisuudesta (2-A)
    - P2P-turvallisuudesta (2-B)
- Tietoverkon rakenteet
    - Yleistä palomuureista; Lisää palomuureista (2-A); *ja lisää* [V-TT s. 36–40]
    - Internetin infrastruktuurin turvaaminen (2-A); ISP-näkökulma [V-TT s. 64–66 ja 70]
    - Turvallisen tietoverkon rakenne (2-A) ; Haavoittuvuustestaus [Sem-k08]

- Tietoverkon turvaaminen (2-A); Verkon toimilaitteet ja niiden turvaaminen [V-TT s. 15–19]
- Turvallisuus päästä päähän
- Reititys ([V-TT s. 57 ja 71–72])
- Verkonhallinta [V-TT s. 57 ja 61]
- Satunnaisverkot ja liikkuva tietoliikenne [Sem-k07]

11. "Paikallaan pysyvän" tietojenkäsittelyn turvaaminen

Tietokannat, ohjelmistot, käyttöjärjestelmä, ohjelmointi, sulautetut järjestelmät.

- Tietokannat
  - Tietokantojen olemuksesta
  - Luottamuksellisuus tietokannoissa; Luottamuksellisuuden mekanismeja (2-A)
  - Eheys tietokannassa (2-A)
  - Monitasoisuus tietokannassa (2-B)
- Ohjelmien tekeminen
  - Ihan oikeat ohjelmat; Ohjelmien virheistä; Ohjelmien todistamisesta ja todentamisesta (2-B)
  - Tietoturvallinen ohjelma (2-A); Ohjelmistojen turvan käsitteitä ja vakuuttumista (2-B); Ohjelmiston kehityksen menettelyjä (2-A); Perussääntöjä ohjelmoijille; Kohti konkreettisia ohjelmointiohjeita (2-A); Tietoturvallinen ohjelma, yksi peukalosäännöstö (2-A)
  - Liittymä turvapalveluihin, GSS-API (2-A)
  - Java-kielen turvallisuudesta (2-A)
  - Liikkuvat agentit, mobiili koodi (2-B)
  - Koodin hämäännyttäminen (2-B)
- Ohjelmien käyttäminen
  - Ohjelmien käytön turvanäkökulmia; Ohjelmien käynnistämisestä; Ohjelmien vaaroihin varautumista; Kääreohjelmat (2-A)
  - Ohjelmiston saatavuuden turvaaminen (2-A)
  - Liikkuvien agenttien turvamekanismeja (2-B)
- Käyttöjärjestelmien perusteita
  - Käyttöjärjestelmien olemuksesta (2-A); Käyttöjärjestelmä erottelijana ja yhdistäjänä (2-A)
  - Prosesseja käyttöjärjestelmissä (2-A)
  - Muistinhallintaa (2-A)
  - Tiedostojärjestelmistä (2-A)
  - Käyttöjärjestelmä laitteiden ohjaajana (2-A)
- Käyttöjärjestelmät ja tietoturva
  - Käyttöjärjestelmän turvatehtävistä TCB:hen; TCB ja käyttöjärjestelmä sen osana (2-A); Datan ja ohjelman erottelu (2-A)
  - Turvakäyttöjärjestelmien perusteita (2-A); Turvakäyttöjärjestelmiä (2-A); EROSista Coyotos-hankkeeseen (2-A)
  - Kryptografisia tiedostojärjestelmiä (2-A)
  - Käyttäjäläheistä käyttöjärjestelmää; esim. Unix (2-A) ; Turvajärjestelyjä Windows NT:ssä (2-A)
- Sulautetut järjestelmät

Jaottelun selitystä

Kaksi ensimmäistä luokkaa, uhkat ja TT-toimet, kokoavat sellaisia aiheita, jotka kuuluisivat useampaan kuin yhteen myöhemmistä luokista. Sama pätee jossain määrin myös 3. luokassa, jossa tosin käsitellään useita reaktiivisia turvatoimia, jotka liittyvät vain yhteen myöhemmistä luokista. Seuraavien kahden luokan (4 ja 5)

tarkoitus on lohkaista TT-kentästä palaset sekä ylhäältä yhteiskunnan että alhaalta yksilön ja heidän yhteisöjensä näkökulmista. Kumpaankin on sijoitettu jonkin verran myös aihealueita, joita voisi yhtä hyvin lähestyä yritysnäkökulmasta 6. luokassa. Kyseistä hallinnollisen tietoturvan luokkaa on muillakin em. sijoitteluilla pyritty pitämään kohtuullisen kokoisena. Lisäksi se on rajattu mahdollisimman epätekniseksi.

Luokka 7 saattaa olla kaikkein erikoisin, sillä siinä on pantu rinnakkain käyttötoimintojen ja aineistojen turvallisuus ja yhdistetty näihin muita informaatioon ja tietojärjestelmiin liittyviä käytäntöjä. Tähän on päädytty lähtemällä tiedon ja tietojärjestelmien tavanomaisesta käytöstä, jossa käyttäjät ja ylläpitäjät joutuvat soveltamaan turvallisuutta edistäviä menettelyjä. Osa niistä on melko itsenäisiä turvamekanismeja kuten salasanat tai salaus, ja ne lohkaisevat osia (perustasolla) hieman myöhemmistä luokista, lähinnä kryptologiasta. Luokat 8 ja 9 lienevät selkeimmät tässä jaottelussa. Edellinen käsittelee kutakuinkin kaiken kryptologian ja jälkimmäinen kaiken ”kouriintuntuvan” paitsi henkilöt, joskin heistäkin biologian. Viimeiset kaksi luokkaa (10 ja 11) edustavat jäljellä olevaa tietoteknistä turvallisuutta siten, että edellinen keskittyy sellaiseen, missä liike tietoverkon eri osien välillä on oleellisempaa kuin jälkimmäisessä.