TTY / TIE / Jukka Koskinen

TLT-3101 Tietoturvallisuuden perusteet
Tentti I 24.5.2013 EI LASKINTA !

Merkitse vastauksesi oheiselle lomakkeelle. Sille pitää kirjoittaa nimi ja opiskelijanumero, joka pitää merkitä myös rastimalla ao. numeromerkit. Tätä tehtäväpaperia ei tarvitse palauttaa. Tee luonnokset ja korjaukset mieluummin tälle paperille kuin lomakkeelle! Tentin jälkeen voit silloin myös helpommin verrata vastauksiasi kurssisivulta löytyvään oikeaan riviin sekä aikanaan tuloslistassa julkaistaviin vastauksiin, jotka on luettu lomakkeeltasi.

Kussakin tehtävässä on vain yksi oikea vastaus. Oikeasta vastauksesta tulee 1 piste. Jos rasteja ei ole yhtään tai niitä on enemmän kuin yksi, tehtävästä tulee 0 pistettä. Väärä vastaus vähentää pistetiliä 1/3 pisteellä.

---

1. **Tietoturvapolitiikka on määritelmän mukaan johdon hyväksymä näkemys joistakin asioista: Mitkä kolme seuraavista parhaiten kuvaavat näitä asioita (TT=tietoturva)? (i) TT-käsitteen merkitys (ii) TT:n päämäärät, (iii) TT-suunnitelma, (iv) TT:n periaatteet, (v) TT:n toteutuksen yleispiirteet, (vi) TT:n toteutuksen yksityiskohdat, (vii) TT-mekanismit.**
   a. ( ) i, iii, v
   b. (X) ii, iv, v
   c. ( ) i, iii, vi
   d. ( ) ii, iv, vii

2. **Oletetaan, että olet keksinyt seittipalveluun salasanan unohtamisen varalle turvakysymyksen "Ystävä Unkarissa?", jonka vastaus "Dorottya" sinun on helppo muistaa. Kaikki seuraavista ovat turvallisuuden kannalta varsin heikkoja modifikaatioita, mutta mikä on *heikoin*?**
   a. ( ) "Ystävä Unkarissa? Siirrä pari(ttomat)." ja "(Fotovtâa)"
   b. ( ) "Ystävä Unkarissa? Kasvattele vokaaleita." ja "D6r2ttYA"
   c. (X) "Ystävä Unkarissa? t=7" ja "Doro77ya"
   d. ( ) "Ystävä Unkarissa? Pisteytä oot." ja "Do..ro:ttya"

3. **Tietoon ja sen turvaamiseen liittyvää sääntelyä jaotellaan materiaalissa kolmeen näkökulmaan. Vaihtoehdoissa on tiivistäen mainittu nämä näkökulmat ja yksi muu. Mikä se on?**
   a. ( ) Mistä tietoturvarauhan häirinnän muodoista voi lain mukaan saada rangaistuksen?
   b. (X) Suojataanko tietoa ihmisiltä vai toisinpäin?
   c. ( ) Miten hyvin tietoturvan rakentajan täytyy hoitaa tehtävänsä, jotta hän ei joutuisi vastuuseen mahdollisista tietoturvaongelmista?
   d. ( ) Onko lainsäädäntö tietoyhteiskunnan kehityksen tasalla?

4. **Kaikilla seuraavista on jotain tekemistä redundanssin kanssa. Millä on vähiten tekemistä eheyden tai saatavuuden suojaamiseen käytettävän toisteisuuden kanssa?**
   a. ( ) datasta laskettu tiivistefunktio
   b. (X) entropia
   c. ( ) metatieto eli tieto tiedosta
   d. ( ) varmuuskopio

5. **Jos sähköisen viranomaisasioinnin vaiheet jaotellaan kolmeen, niin ne ovat**
   a. ( ) aikomus - oikeuksien tarkistus - päätös.
   b. ( ) vireillepano - käsittely - päätöksen tiedoksianto.
   c. (X) oikeuksien tarkistus - palvelun toteuttaminen - lokitietojen kirjaaminen.
   d. ( ) tuotteiden valinta - maksaminen - toimitus.

6. **Tutki väitettä: Kryptoalgoritmit ovat joko symmetrisiä salausalgoritmeja tai epäsymmetrisiä salaus- tai allekirjoitusalgoritmeja. Se on**
   a. ( ) epätosi, mutta steganografian eli piilokirjoituksen mukaan ottaminen tekisi väitteestä toden.
   b. ( ) epätosi, koska luettelosta puuttuu sellaisia algoritmeja, joissa ei käytetä avainta.
   c. ( ) epätosi, mutta kryptografisesti vahvojen satunnaislukujen mukaan ottaminen tekisi väitteestä toden.
   d. (X) tosi, koska perinteisen salauksen rinnalle tullut digitaalinen allekirjoitus tapahtuu salauksen tapaisella algoritmilla, joka ei ole symmetrinen.

7. **Mikä seuraavista on tyypillistä tarkistussummille, jotka on tarkoitettu torjumaan erilaisten numeroiden tai merkkijonojen syötössä tapahtuvia näppäilyvirheitä? Se**
   a. ( ) sijoitetaan aina numerosarjojen alkuun tai loppuun.
   b. ( ) sijoitetaan hajautettuna useamman merkin alueelle.
   c. (X) lasketaan kaikista muista merkeistä.
   d. ( ) lasketaan yhteenlaskulla muista merkeistä.

8. **Sähköisen kaupankäynnin aapisen maksutapojen esittelyssä ei oteta huomioon,**
   a. ( ) onko luottoriski myyjällä, ostajalla vai jollakulla muulla.
   b. (?) että kertamaksu voi olla niin pieni, ettei sitä kannattaisi maksaa erikseen.
   c. ( ) että web-maksut edellyttävät tietoturvallisuutta.
   d. (X) onko kaupankäynti laillista.

9. **Opiskelija jättää tenttisalissa valvojalle lomakkeen, jossa on tekstattu nimi, opiskelijanumero ja vastauksina rasteja ruuduissa. Jos hän poistuu pystymättä osoittamaan henkilöllisyyttään eikä valvoja tunne häntä, niin myöhemmin ei ole mitään käytännöllistä keinoa varmistua siitä, kuka vastaukset antoi. Miten tilanne voitaisiin korjata varmimmin? Oletetaan että suluissa mainitut oletukset toteutuvat.**
   a. ( ) Pyydetään häntä kopioimaan lomakkeen taakse muutama valvojan kirjoittama lause ja käymään tentin tarkastajan luona kirjoittamassa samat, henkilötodistus mukanaan. (Tarkastajalla on tähän mahdollisuus.)
   b. ( ) Pyydetään opiskelijaa soittamaan valvojalle. Valvoja kysyy nimitiedustelusta, kenelle soitosta poimittu numero kuuluu. (Molemmilla on puhelin mukanaan.)
   c. (X) Pyydetään häntä kirjautumaan TTY:n intranettiin ja katsotaan sieltä, mikä hänen nimensä ja numeronsa on. (Valvojalla on tietokone mukanaan.)
   d. ( ) Kysytään joltakulta muulta tenttijältä, onko hän se joka väittää olevansa. (Tämä ei häiritse liikaa muita.)

10. **Mitä seuraavista lähinnä tarkoittaa julkisen avaimen kryptosysteemin salaluukku?**
    a. ( ) algoritmia diskreetin logaritmin laskemiseksi modulo n, kun n on kahden suuren alkuluvun tulo
    b. (X) jotain julkisessa avaimessa olevaa salaista rakennetta, kuten kahta suurta alkutekijää
    c. ( ) julkisen avaimen salauksen purkuavainta tai allekirjoituksen laadinta-avainta
    d. ( ) keinoa suorittaa julkisen avaimen salausoperaatioita ilman että tuntee avaimia

11. **Tarkastellaan tietojenkäsittelyrauhan rikkomuksia, joita tietojenkäsittelylaitteeseen fyysisesti käsiksi pääsevä voi aiheuttaa. Mikä seuraavista ei ole *laitteistonäkökulmasta* tietoturvaongelma?**
    a. ( ) laitteen fyysisten suojausten poistaminen
    b. (X) esiintyminen tietoverkossa laitteen käyttäjän nimissä
    c. ( ) laitteen siirtäminen toiseen paikkaan
    d. ( ) laitteen identiteetin muuttaminen

12. **Viitemonitorin tehtävänä luotetussa tietojenkäsittelyssä on**
    a. ( ) autentikoida käyttäjät.
    b. ( ) hallinnoida epäsuorien muistiviittausten osoitetauluja.
    c. (X) asettaa pääsynvalvonnan tauluihin käyttäjien oikeudet resursseihin.
    d. ( ) välittää kaikki vuorovaikutus käyttäjien ja resurssien välillä.

13. **Kun tietoaineistoturvallisuuden yhdeksi keinoksi mainitaan tietoaineistojen luokitus, tarkoitetaan**
    a. ( ) tiedon luokitusta, jonka avulla määräytyy mm. millaista pääsynvalvontaa tietoon pitää soveltaa.
    b. (X) aineiston jaottelua salaisiin, tosiaikaisiin ja käytettävyydeltään kriittisiin tietoihin.
    c. ( ) käsittelysääntöjen jakoa käytettävyyden, eheyden ja luottamuksellisuuden mukaisesti.
    d. ( ) jaottelua tietovälineiden asianmukaiseen hallintaan, käsittelyyn, säilytykseen ja hävittämiseen.

14. **Kun yksityisellä avaimella tehtyä allekirjoitusta todennetaan vastaavalla julkisella avaimella, matemaattinen kytkentä varmistaa lähinnä sen, että**
    a. ( ) allekirjoittajan henkilöllisyys on sama kuin se, joka on kytketty kyseiseen julkiseen avaimeen varmenteen avulla.
    b. (x) allekirjoittaja, kuka hän onkin, on tulkinnut oikein bittijonon, jonka hän on syöttänyt allekirjoitusalgoritmille.
    c. ( ) allekirjoittaja omistaa tai on omistanut kyseisen julkisen avaimen.
    d. (x) allekirjoittajalla on ollut hallussaan julkista avainta vastaava yksityinen avain.

15. **Kun TLS:ää käytetään www-kauppatapahtuman yhteydessä tehtävässä tilisiirrossa, tarvitaan tyypillisesti**
    a. ( ) selainkoneen sertifikaatti, jonka TLS välittää ainakin yhdelle palvelimelle.
    b. ( ) yhteys vain yhteen palvelimeen: kauppaan, josta otetaan yhteys muihin palvelimiin.
    c. (x) selainkoneen luottamus useamman kuin yhden palvelimen sertifikaattiin.
    d. ( ) yhteys kolmeen palvelimeen: kauppaan, pankkiin ja luottokuntaan.

16. **Mikä laki lähinnä vaikuttaa teknisin menetelmin toteutettuun valvontaan työpaikoilla?**
    a. ( ) Laki valvonnan ja tietoverkon käytön järjestämisestä työelämässä
    b. (x) Sähköisen viestinnän tietosuojalaki
    c. ( ) Henkilötietolaki
    d. ( ) Laki yksityisyyden suojasta työelämässä

17. **Haittaohjelma voi käynnistyä oikean ohjelman sijasta tai silloin kun mitään ohjelmaa ei ollut tarkoitus käynnistää. Millä seuraavista on tämän kanssa vähiten tekemistä?**
    a. ( ) dokumenttitiedoston avaaminen
    b. (x) virtuaalimuisti
    c. ( ) tiedostonimet
    d. ( ) käyttöjärjestelmän monipuolisuus

18. **Henkilötietolaki antaa henkilörekisteriin merkitylle tiettyjä oikeuksia kieltää omien tietojensa käsittely. Olettaen että rekisteri sinänsä on lainmukainen, hän ei voi ko. lain perusteella kieltää käsittelyä**
    a. ( ) suoramainontaa varten.
    b. ( ) henkilömatrikkelia varten.
    c. ( ) sukututkimusta varten.
    d. (x) viranomaistarkistusta varten.

19. **Mitä seuraavista materiaalissa käsitelty CERT:n laatima tarkistuslista ei kehota ylläpitäjää etsimään/tarkastamaan hyökkäysten havaitsemiseksi?**
    a. (x) varusohjelmistot
    b. ( ) allekirjoitetut tiedostot
    c. ( ) suid- ja sgid-tiedostot
    d. (x) ajastettuina ajettavat ohjelmatiedostot

20. **Verkkoympäristössä tapahtuvaa viestintää koskevat uhkat tiivistetään yleensä viiteen keskeiseen tapaukseen, joista yksi on etäresurssin luvaton käyttö verkon yli. Muut neljä käsittelevät viestien "kohtaloa". Piirrä niitä kuvaavat nuolikaaviot, jotka muuntelevat jotenkin sitä, että lähettäjästä A on viestin kulkua osoittava nuoli vastaanottajaan B. Kuinka monessa neljästä kaaviosta nuoli liittyy vain toiseen osapuolista A ja B?**
    a. ( ) 3
    b. ( ) 2
    c. ( ) 1
    d. ( ) 0

21. **Kotihakemiston ei pitäisi olla hakupolussa. Syynä on se, että muuten**
    a. ( ) tiedoston haku joutuu aina käymään läpi kaikki alihakemistot ja saatavuus heikkenee.
    b. (x) varusohjelman sijasta käyttäjä voi tulla käynnistäneeksi hyökkääjän kirjoittaman ohjelman.
    c. ( ) lokitietoja tallettuu myös päähakemistoon ja käytettävyys heikkenee.
    d. ( ) salakuunteleva hyökkääjä pääsee paremmin jäljittämään käyttäjän toimia.

22. **Työsuhteen päättymiseen liittyvät tietoturvariskit luottamuksellisuuden osalta rajoittuvat siihen tietoon, jonka eroava työntekijä on hankkinut ennen kuin hänen tietovälineensä on palautettu yritykselle ja pääsyoikeutensa on peruutettu. Väite on melko lähellä totuutta, mutta riskinä voi olla myös *muiden* tietojen vuotaminen työntekijän**
    a. ( ) oman muistin kautta, vaikka tiedot voivatkin olla epätarkkoja tai vanhentuneita.
    b. (x) talletettua aineistoja yrityksen ulkopuolelle esim. johonkin seittipalveluun.
    c. ( ) tehdessä ulkopuolelta hyökkäyksen jonkin aiemmin asentamansa takaportin kautta.
    d. ( ) Ei mikään muista kohdista, vaan alkuperäinen väite on tosi.

23. **Java-hiekkalaatikko ei voi estää koodilta**
    a. ( ) uuden ohjelmakirjaston lataamista.
    b. (x) nollalla jakamisen yrittämistä.
    c. ( ) paikalliselta levyltä lukemista.
    d. ( ) uuden prosessin käynnistämistä.

24. **Salasanasta on sanottu, että sitä pitäisi kohdella kuin omaa hammasharjaa. Kuinka monta seuraavista salasanaan liittyvistä ominaisuuksista tämä sanonta edustaa? Salasanan (i) entropia, (ii) käytettävyys, (iii) pitäminen vain omassa käytössä, (iv) vaihtaminen riittävän usein.**
    a. ( ) yhtä
    b. (x) kahta
    c. ( ) kaikkia
    d. ( ) ei yhtään

25. **Www-sivuja julkaisevien palveluntuottajien tietoturvahuolten neljä luokkaa materiaalissa ovat (i) palvelun saatavuus, (ii) palvelun eheys, (iii) maksun saaminen ja (iv) vastuut. Missä luokassa palvelun yksittäinen käyttäjä voi helpoimmin aiheuttaa huolta pelkällä tuottamallaan staattisella sisällöllä?**
    a. ( ) (i)
    b. ( ) (ii)
    c. ( ) (iii)
    d. (x) (iv)

26. **Minkä seuraavista pitäisi lähinnä kyetä palomuurin tapaiseen pakettien suodatukseen?**
    a. ( ) www-selain
    b. (x) reititin
    c. ( ) verkkokytkin
    d. ( ) työaseman verkkokortti

27. **Mikä seuraavista pätee mille tahansa kryptoalgoritmille, kun sitä käytetään haaste-vaste -menetelmässä?**
    a. ( ) Todennettava syöttää siihen jotain, jonka hän voisi ilman riskiä näyttää hyökkääjällekin.
    b. ( ) Kumpikin osapuoli tekee sillä saman operaation.
    c. (x) Todentavan osapuolen ei tarvitse tuntea sitä.
    d. ( ) Sillä tehtävä operaatio saa olla mahdollinen vain todennettavalle osapuolelle.

28. **Mitä eroa on tiedon luvattomalla käytöllä ja väärinkäytöllä?**
    a. ( ) Toinen on toisen erikoistapaus, eli käsitteenä suppeampi.
    b. (x) Toista ei voi tiedon omistaja tehdä, mikäli hän on tietoa koskevien oikeuksien ainoa haltija.
    c. ( ) Jos samalle tiedolle tapahtuu molemmat eri aikaan, niin ensin tapahtuu väärinkäyttö.
    d. ( ) Toinen on lainvastaista, toinen ei.

29. **Mitä tarkoitetaan uhkapuilla?**
    a. ( ) Tiettyä biologista vertauskuvaa uhka-arvioinnin "mitä-jos" -tyyppiselle skenaariotyöskentelylle.
    b. ( ) Tiettyjä fyysisiä uhkia tietoturvallisuudelle tai yleiselle turvallisuudelle.
    c. ( ) Tiettyä käyttäjäpalautteen kautta etenevää ja haarautuvaa uhkien ja haavoittuvuuksien luokittelumenetelmää.
    d. ( ) Tiettyä hierarkkista, kattavuuteen tähtäävää tapaa jäsentää uhkia.

30. **Mikä yleinen sääntö sopii parhaiten sille, miten tietojärjestelmän tärkeiden tehtävien (i) varahenkilöt, (ii) varalaitteet ja (iii) varatilat suhtautuvat toisiinsa?**
   a. (X) Jos (iii) on olemassa, pitäisi olla sekä (i) että (ii).
   b. ( ) Jos (ii) on olemassa, pitäisi olla (i), mutta ei välttämättä (iii).
   c. ( ) Mikä tahansa voi olla järkevä myös ilman muita.
   d. ( ) Jos (i) on olemassa, pitäisi olla (ii), mutta ei välttämättä (iii).

31. **Kun *tietoturvallisuuden olemusta* kartoitetaan kysymyksillä, niin eniten vastauksia -- ainakin kurssimateriaaliin -- tuottaa kysymys,**
   a. (X) mitä tietojenkäsittelyssä pitäisi tapahtua.
   b. ( ) mikä tietojärjestelmässä on arvokasta muille kuin omistajalle.
   c. ( ) kuinka arvokkaita tietojärjestelmän sisällöt ovat omistajalle.
   d. ( ) mitä tietojenkäsittelyssä ei saisi tapahtua.

32. **Luotettava biometrinen autentikointi edellyttää, että sopivan fyysisen piirteen lisäksi vaaditaan**
   a. ( ) useampaa kuin yhtä mittausta autentikointitilanteessa.
   b. ( ) jonkin esineen hallussapitoa.
   c. ( ) jonkin asian tietämistä.
   d. (X) läsnäoloa autentikointitilanteessa.

33. **Tulipaloon pitää varautua ja siinä yhteydessä on tarpeen määrätä vastuuhenkilöitä. Mille seuraavista kannattaa muita ennemmin tehdä näin?**
   a. ( ) Raivaustoimet, joihin pitää ryhtyä heti pelastuslaitoksen väen annettua luvan.
   b. ( ) Vakuutusyhtiölle tehtävien korvaushakemusten laatiminen.
   c. ( ) Toimet, joilla tietokonelaitteita ja tietovälineitä ajetaan alas tai siirretään turvaan.
   d. (X) Erilaiset tiedotustehtävät asiakkaiden ja viranomaisten suuntaan.

34. **Ylivoimaisena uhkana tietoturvalle voidaan pitää myös tietynlaisen internet-palvelun keskeytymistä. Tämä on mainittu Saksan tietoturvaviraston käsikirjassa kohtana "Ausfall eines Weitverkehrsnetzes / Failure of a wide area network". Mihin palveluun tämä uhka liittyy?**
   a. (X) yhteyspalvelu
   b. ( ) haku- tai hakemistopalvelu
   c. ( ) sähköpostipalvelu
   d. ( ) nimipalvelu (DNS)

35. **Mikä seuraavista on sellainen yleisen *yritysturvallisuuden osa-alue*, jolla on muita *vähemmän* tekemistä sen kanssa, mitä tietoturvallisuudessa tavoitellaan?**
   a. ( ) Työturvallisuus
   b. (X) Liikenneturvallisuus
   c. ( ) Valmiussuunnittelu
   d. ( ) Kiinteistö- ja toimitilaturvallisuus

36. **Mikä on oikea järjestys tietoturvaa rakennettaessa?**
   a. ( ) turvapolitiikka – uhkakartoitus – riskianalyysi – turvamekanismit
   b. ( ) turvapolitiikka – turvamekanismit – uhkakartoitus – riskianalyysi
   c. ( ) turvamekanismit – uhkakartoitus – turvapolitiikka – riskianalyysi
   d. (X) uhkakartoitus – riskianalyysi – turvapolitiikka – turvamekanismit

37. **Selaimesi näyttää jotain sivua ja siirryt uudelle sivulle ilman, että käytät alkuperäisellä sivulla olevaa linkkiä (siis kirjoitat osoitteen tai käytät kirjanmerkkiä). Tällöin eri palvelin, jolla uusi sivu on, ei saa tietää, miltä sivulta tulit. Mitä muuta palvelin ei saa tässä tapauksessa tietää?**
   a. ( ) Koneesi IP-osoitetta.
   b. ( ) Aiemman käyntisi yhteydessä lähettämäänsä cookie-tiedostoa/tietuetta.
   c. (X) Sähköpostiosoitettasi.
   d. ( ) Sitä pystyykö selaimesi näyttämään JPEG-kuvia.

38. **Spam-viestinnän alajakoa voi tehdä sen mukaan, (i) meneekö viesti suoraan uhrille, (ii) meneekö uhri itse viestin luo, vai (iii) onko mukana hakukoneen kaltainen välittäjä. Missä seuraavista luetteloista on kaikkia kolmea tyyppiä olevia spam-viestinnän keinoja?**
   a. ( ) sblog, wiki, spim
   b. ( ) smishing, vishing, pharming
   c. ( ) spamdexing, sblog, spit
   d. (X) sosiaalinen media, sms-spam, pharming

39. **"Erot langattoman ja langallisen tietojenkäsittelyn tietoturvassa johtuvat tietoliikennekanavan erilaisista ominaisuuksista." Väite on**
   a. (X) yleensä epätotta; jos kanava on autentikoitu ja salattu, muut erot ovat merkittävämpiä.
   b. ( ) yleensä totta; on muitakin eroja, jotka eivät ole lainkaan niin merkittäviä kuin kanavan aiheuttamat.
   c. ( ) epätotta lähes aina; muiden erojen rinnalla kanavan erilaisuus ei paljon merkitse.
   d. ( ) totta lähes aina, poikkeukset ovat vähäisiä.

40. **Jos käytössäsi ei ole päällekirjoitusohjelmaa tiedostojen turvalliseen hävittämiseen, mikä seuraavista olisi muita turvallisempi korvike? Oletetaan, että tuhottavana on muutaman sadan kilotavun kokoinen tekstidokumentti ja näiden toimien jälkeen deletoit tiedoston tavalliseen tapaan niin, että se ei jää roskakoriin tai vastaavaan.**
   a. ( ) Korvaat jokaisen rivinvaihdon sivunvaihdolla ja tallennat.
   b. ( ) Pyyhit teksturissa kaiken tekstin ja tallennat.
   c. ( ) Vaihdat tiedostonimen ja annat tiedostotyypiksi jpg.
   d. (X) Korvaat teksturissa välilyönnit ja yleiset kirjaimet i, t, n, e, s ja l yleisimmällä eli a:lla ja tallennat.

41. **Kertakirjautuminen**
   a. ( ) on tarpeeton mekanismi, koska kertaalleen suoritettavan autentikoinnin voi hoitaa jo oikeuksien myöntövaiheessa.
   b. ( ) on turvaton mekanismi, koska siinä pääsyoikeuksien myöntäminen sekoitetaan autentikointivaiheeseen.
   c. ( ) tuottaa pääsyn mihin tahansa yhteen resurssiin yhdeksi käyttökerraksi.
   d. (X) voi tuottaa pääsyn useaan resurssiin, mutta on voimassa vain jonkin rajoitetun aikamäärän tai istunnon ajan.

42. **Vaikuttaako Työelämän tietosuojalaki siihen, mitä tietoja työnantaja saa selvittää työntekijän taustasta, kun tarkistuksen kohde on työnhakija yrityksen (i) sisältä, (ii) ulkopuolelta?**
   a. ( ) Vaikuttaa (i):een mutta ei (ii):een.
   b. (X) Vaikuttaa molempiin.
   c. ( ) Ei vaikuta kumpaankaan.
   d. ( ) Vaikuttaa (ii):een mutta ei (i):een.

43. **Mikä standardi sisältää arviointiluokat D, C1, C2, B1, B2, B3 ja A1?**
   a. ( ) Common Criteria for Information Technology Security Evaluation (kansainvälinen)
   b. ( ) European Criteria for Information Technology Security
   c. ( ) ISO 27000-standardiperhe
   d. (X) Trusted Computer System Evaluation Criteria (USA)

44. **Jos jossain tietoturvaloukkausten luokittelussa kaikkien hyökkäysten yhtenä vaiheena esiintyy tietoon kohdistuva prosessi, niin kyseinen luokittelu pystyy kattamaan**
   a. ( ) vain tahattomia ihmisen suoraan aiheuttamia loukkauksia.
   b. ( ) vain tahattomia loukkauksia, joita ihminen ei ole suoraan aiheuttanut.
   c. ( ) sekä tahallisia että tahattomia loukkauksia.
   d. ( ) vain tahallisia loukkauksia.

45. **Tietoturvamekanismeja laajasti mutta abstraktisti esittelevässä käsitekartassa mainitaan**
   a. ( ) roskapostin suodatus.
   b. ( ) varmuuskopiointi.
   c. ( ) virustorjunta.
   d. ( ) tunkeutumisen havainnointi.

46. **Mitä lähinnä saavutetaan, kun yrityksessä dokumentoidaan jonkin kriittisen työn tehtäväkuvaus?**
    a. ( ) Ei tarvita kahta tai useampaa vakituista henkilöä hoitamassa samaa tehtävää.
    b. (X) Kyseisen työn tekijän estyessä kuluu todennäköisesti vähemmän aikaa työn jatkumiseen kuin ilman dokumenttia.
    c. ( ) Ei tarvitse valita eikä valmentaa varahenkilöitä, jotka voisivat siirtyä omista töistään kyseiseen työhön.
    d. ( ) Yritys saa pätevämpiä työnhakijoita kyseiseen tehtävään kuin ilman dokumentaatiota.

47. **Verkosta ladattavan ohjelman joistakin ominaisuuksista voidaan vakuuttua sellaisten allekirjoitusten perusteella, joita esimerkiksi Verisign tarjoaa, mutta nämä takaavat vain koodin**
    a. ( ) vastaavan määrityksiään.
    b. ( ) läpäisseen virustarkistuksen, joskin useilla eri menetelmillä.
    c. (X) alkuperää ja eheyttä.
    d. ( ) valmistajan ottavan vastuun mahdollisista turvaongelmista.

48. **Miten toimikorttien prosessorit suhtautuvat julkisen avaimen kryptosysteemin (i) operaatioihin ja (ii) avainten luomiseen?**
    a. ( ) Ne kykenevät molempiin.
    b. ( ) Ne eivät kykene kumpaankaan.
    c. ( ) Ne kykenevät (i):een mutta eivät (ii):een.
    d. ( ) Ne kykenevät (ii):een mutta eivät (i):een.

49. **Mikä laki sanoo tähän tapaan: palvelun tarjoaja ei ole vastuussa tallennettujen tietojen sisällöstä tai välittämisestä, kunhan hän viipymättä havaitsee ja poistaa saatavilta aineiston, joka sisältää ... ?**
    a. ( ) Laki tietoyhteiskunnan palvelujen tarjoamisesta
    b. ( ) Sähköisen viestinnän tietosuojalaki
    c. ( ) Ei mikään laki
    d. ( ) Julkisuuslaki

50. **Tunnelimoodissa tehty IPsec-salaus merkitsee sitä, että**
    a. ( ) viestinnän osapuolet tarvitsevat lisäavaimet tunnelin purkamiseen.
    b. ( ) AH-protokollaa ei ole voitu soveltaa samaan pakettiin.
    c. ( ) paketti on pitempi kuin se olisi transport-moodissa.
    d. ( ) koko eteenpäin lähtevä paketti on salattu.

51. **Materiaalissa luetellaan luontoon liittyviä, ihmisestä jossain määrin riippumattomia uhkia tietoturvalle. Niitä ei kannata käsitellä materiaalissa ainakaan peruskurssilla kovin laajalti, koska**
    a. ( ) kyseisenlaisten uhkien merkitys tietoturvalle on varsin vähäinen.
    b. ( ) kyseisenlaisten uhkien tai niiden vaikutusten torjunta on yleensä tarpeen muistakin kuin tietoturvasyistä.
    c. ( ) tietoturvauhkat, joihin voidaan vaikuttaa, ovat ihmisten aiheuttamia.
    d. ( ) tarvittavat torjuntamekanismit ovat huomattavan mutkikkaita.

52. **Mikä seuraavista edustaa sellaista fyysistä tiedon tallennetta, jonka väärentäminen vaikuttaa toimijan oikeuksiin mutta ei autenttisuuteen?**
    a. (X) kirjaston lainauskortti
    b. ( ) huvipuiston ranneke
    c. ( ) matkakortti, jolla on arvolippu
    d. ( ) musiikki-CD

53. **Mikä seuraavista on lähinnä sellainen tehtävä, jonka hoitamiseen voidaan käyttää kryptografista protokollaa?**
    a. ( ) salausavaimesta sopiminen
    b. ( ) sähköpostiviestin muuttaminen salatekstiksi
    c. ( ) salausavaimen turvallinen säilytys
    d. ( ) salausavaimen generointi hyvien satunnaislukujen perusteella

54. **Käyttöjärjestelmän tehtävänä EI ole torjua tietokantaa uhkaavaa eheysongelmaa, joka seuraa**
    a. ( ) tietokantakoneeseen murtautuneen käyttäjän prosessin yrittäessä kirjoittaa kannanhallintaohjelman muistialueelle.
    b. (X) siitä, että samanaikaisesti kantaa käyttävät henkilöt saavat käyntiin kannan hallintaohjelman kahtena tai useampana erillisenä prosessina.
    c. ( ) kahden tietokantaa päivittävän käyttäjän lukiessa kannasta samoja tietoja samaan aikaan.
    d. ( ) tietokantakoneen keskusmuistin ja oheismuistin välillä tapahtuvan tiedonvaihdon epätahtisuudesta.

55. **Seittiselauksen evästeen tarkoituksena on välittää www-palvelimelle**
    a. (X) samaa tietoa kuin palvelin on itse joskus välittänyt selaimelle.
    b. ( ) tietoa selaimen turva-asetuksista.
    c. ( ) selaimen käyttäjältä keräämiä tietoja.
    d. ( ) selaimen muilta palvelimilta keräämiä tietoja.

56. **Mitä omistajan kannattaa ensisijaisesti tehdä löytääkseen oman tietojärjestelmänsä haavoittuvuuksia?**
    a. (X) käyttää tunkeutumisen havainnoinnin tekniikoita.
    b. ( ) tarjota järjestelmän rinnakkainen versio hakkereiden tutkittavaksi.
    c. ( ) soveltaa automaattisia hyökkäystyökaluja.
    d. ( ) asentaa jokin root-kit.

57. **Jos laitteistojen turvallisuutta tarkastellaan peukaloinnin näkökulmasta, niin keskeistä on, ettei mikään luvaton toimenpide pääse kohdistumaan niihin ja että käyttäjä voi myös vakuuttua tästä. Tällaisessa tarkastelussa jää huomiotta jotain tärkeää, mitä laitteistojen valmistuksessa pitäisi ottaa huomioon. Mitä?**
    a. (X) Laitteen fyysinen kestävyys, toimivuus ja muu tietoturvan saatavuusnäkökulma.
    b. ( ) Mahdollisuus sijoittaa laite siten, että se ei aiheuta eikä siihen kohdistu palovaaraa eikä säteilyvaikutusta.
    c. ( ) Se, että laitteen pitää ennemmin tuhota siihen valmistuksessa asennettu kryptoavain kuin päästää sitä paljastumaan.
    d. ( ) Valmistuksen vaiheistus siten, ettei kukaan saa liikaa tietoa rakenteesta tai pääse asentamaan siihen takaportteja.

58. **Mikä seuraavista kuvaa parhaiten puskurin ylivuotoa?**
    a. ( ) Ohjelmalaskuri eli seuraavaksi suoritettavan käskyn osoite siirtyy yhdellä eteenpäin, vaikka ollaan jo aliohjelman viimeisessä käskyssä.
    b. ( ) Se on aina tietoturvauhka, sillä hyökkääjä voi sen avulla saada aikaan pahojaan -- vähintään ohjelman kaatumisen.
    c. (X) Ohjelman tekemä muistiviittaus osoittaa jonkin toisen prosessin muistialueelle.
    d. ( ) Taulukon indeksointiin käytetään lukua, joka on suurempi kuin taulukon koko, eikä käyttöjärjestelmä estä tätä viittausta.

59. **Mikä laki sanoo tämän: Automatisoitujen soittojärjestelmien sekä telekopiolaitteiden, sähköposti-, teksti-, puhe-, ääni- tai kuvaviestien avulla toteutettua suoramarkkinointia saa kohdistaa vain sellaisiin luonnollisiin henkilöihin, jotka ovat antaneet siihen ennalta suostumuksensa ?**
    a. ( ) Sähköisen viestinnän tietosuojalaki
    b. ( ) Julkisuuslaki
    c. (X) Henkilötietolaki
    d. ( ) Laki tietoyhteiskunnan palvelujen tarjoamisesta

60. **Turvallisuuden pahin vihollinen taitaa kyllä olla ihminen, mutta mikä on toiseksi pahin -- jota usein myös pahimmaksi sanotaan?**
    a. (X) ketjun heikoin lenkki
    b. ( ) monikerroksisuus
    c. ( ) yksitasoisuus
    d. ( ) ei mikään näistä