

TLT-3101 Tietoturvallisuuden perusteet

Tentti (III) 9. 11. 2009

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.

Tosi-epätosi -tehtävissä väittämät ovat joko tosia tai epätosia eli oikea vastaus on joko (a) tai (d). Jos rastit näistä laittimmaisista ruuduista väärän, menetät yhden pisteen. Jos rastit jommankumman vaihtoehdoista (b) ja (c), saat tai menetät puoli pistettä sen mukaan, mikä on oikea vastaus. Näiden keskivaihtoehtojen tarkoitus on mahdollistaa osittaisen tietämyksesi hyvittäminen. Ne eivät siis ole oikeita vastauksia eivätkä edusta mitään osatotuuksia.

Normaaleissa neljän vaihtoehdon tehtävissä (21-60) väärä vastaus vähentää pistetilä 1/3 pisteellä.

- Allekirjoitusavaimen omistajan voi olla lain mukaan mahdollonta kiistää sähköistä allekirjoitusta, vaikka sen olisi tehnyt joku muu.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Jos salausalgoritmissa tehtäisiin niin, että selkotekstin bittien järjestystä vain muutettaisiin, mutta se tehtäisiin satunnaisella, avaimesta riippumattomalla tavalla, tuloksena olevasta salatekstistä ei voisi enää purkaa selkotekstiä takaisin.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Jos salasanan unohtamisen varalle saa esim. seittipalvelussa muotoilla muistutuskysymyksen ja siihen vastauksen, vastaus on oleellisesti toinen salasana.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Ohjelmiston uudesta versiosta voi olla sekä hyötyä että haittaa tietoturvallisuuden kannalta.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Jos ohjelma toteuttaa täsmällisesti määrityksensä, se on myös tietoturvallinen.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Lyhimmässäkin AES-avaimessa on yli sata bittiä.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Julkisella paikalla olevan (kiinteän) tietokoneen lukitseminen salasanalla suojatulla joutonäytöllä riittää varoimenpiteeksi eheyttä varten, jos pitää välillä käydä keventymässä.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi

- Jos jätetään huomiotta tietoturvamekanismien kuten SSL:n tarvitsemat tiedot, käyttäjä voi estää selaintaan lähettämästä palvelimelle kaiken muun paitsi selain- ja palvelinkoneen IP-osoitteet.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Alkuperäisen tekijän tekijänoikeus koskee myös teosta, jota on muunneltu.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Samankaltaisia automaattisia hyökkäysokaluja, joita tunkeutajat soveltavat, voi myös käyttää tunkeutumisten havainnointiin.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Jos henkilöstön pääsyoikeuksia tietojenkäsittelyresurssihin (mukaanlukien tiedot) onnistuttaisiin säätämään täydellisesti sen mukaan, mitä he todella tarvitsevat työssään, tietojen eheys voisi tunareiden takia kylläkin särkyä, mutta ei arkojen tietojen luottamuksellisuus.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Turvallisten oletusarvojen periaate kieltää pääsyn, ellei lupaa erikseen ole myönnetty.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Jos hyökkääjä pystyy kaappaamaan käyttäjän biometriset tiedot esim. tietokannasta tai matkan varrelta, biometrinen järjestelmä ei voi enää jatkossa autentikoida käyttäjää luotettavasti saman piirteiden perusteella.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Jos pääset lukemaan lokitietoja, jotka Unix kerää yhteydenotoista (wtmp), voit saada tietoja, joilla pääset vastaisuudessa kirjautumaan koneeseen jonain muuna kuin itsenäsi.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- SSL ei pysty suojaamaan sellaista kokonaisuutta, jonka muodostaa tuotteen valinta verkkokaupasta ja luottokorttitietojen lähettäminen kyseiselle kauppiaille.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- PGP-ohjelmalle on ominaista, että se määrittelee avainrenkaassa olevien julkisten avainten luotettavuutta hakemistoista tai muualta tietoverkosta hakemiensa varmenneketjujen avulla.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Langattomilla päätelaitteilla on yleensä langallista suurempi riski joutua väärin käsiin, mutta muuten edellisten tietoturvariskit ovat keskimäärin samankaltaiset kuin langallisilla päätelaitteilla.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Vaikka tietojärjestelmän tärkeisiin tehtäviin olisi olemassa varahenkilöt, niin tehtäviä varten ei välttämättä tarvitse olla varailaitteistoineen.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi
- Jos haaste-vaste -menetelmä perustuu kryptografisen tiivistefunktion käyttöön, käyttäjän salasanan riittää olla todentajalla tallessa tiivistetyssä muodossa.
a. Tosi b. Luulen todeksi c. Luulen epätodeksi d. Epätosi

20. Digitaalinen allekirjoitus RSA-tekniikassa on pitkä, (esim.) 1024 tai 2048 bittiä, minkä vuoksi siitä lasketaan tiiviste.
a. () Tosi b. () Luulen todeksi c. () Luulen epätodeksi d. (X) Epätosi
21. Tiedon luottamuksellisuuden turvaamiseksi kannattaa joskus käyttää
a. () pelkän tiivistearvon tallentamista tiedon sijasta.
b. (X) silppuria.
c. () aineiston "piilottamista" julkisuuteen lukemattomien muiden vastaavanlaisten tietojen joukkoon.
d. () salattua tallentamista vain yhteen paikkaan, eli jättää varmuuskopio tekemättä.
22. Rabin-allekirjoitus muodostetaan korottamalla viesti tiettyyn potenssiin ja laskemalla jakojännös julkisen moduulin suhteen. Mikä seuraavista on mahdollinen eksponentti?
a. (X) 3
b. () 1000-bittinen satunnaisluku
c. () 2
d. () 1/2 (eli lasketaan viestistä neliöjuuri)
23. Jos selaimesi tarjoaa sinulle mahdollisuuden tallentaa juuri syöttämäsi salasana vastaista käyttöä varten, minkä ehdon seuraavista olisi tärkeintä täyttyä, jotta sinun kannattaa tehdä talletus?
a. () Salasana on niin entrooppinen, ettei pystyisi sitä muistamaan.
b. () Salasanan takana ei ole mitään arvokasta.
c. (X) Kukaan muu ei pääse käsiksi selaimeesi.
d. () Et tarvitse salasanaa milteään muulta koneelta.
24. 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) nimipalvelu (DNS)
b. () haku- tai hakemistopalvelu
c. () sähköpostipalvelu
d. () yhteyspalvelu
25. Millä seuraavista on vähiten tekemistä perinteisten GSM-puhelujen kanssa?
a. () peukaloinnin torjunta
b. (X) sovellustason palomuri
c. () autentikointi
d. () riskianalyysi
26. Mikä seuraavista ei ole pahoista ohjelmista käytetty nimitys?
a. () kani
b. (X) hoax
c. () bot-agentti
d. () bakteeri
27. Java-hiekkalaatikko voi estää koodilta
a. () syötteen vastaanoton käyttäjältä.
b. () liukulukuoperaatiot.
c. (X) levyiltä lukemisen.
d. () näytölle kirjoittamisen.
28. Sähköisen kaupankäynnin aapisen maksutapojen esittelyssä ei oteta huomioon,
a. () onko luottoriski myyjällä, ostajalla vai jollakulla muulla.
b. () onko kaupankäynti laillista.
c. () että kertamaksu voi olla niin pieni, ettei sitä kannattaisi maksaa erikseen.
d. () että web-maksut edellyttävät tietoturvasuorituksia.
29. Yksi kolmesta yleisimmästä ohjelmistojen tietoturvaan liittyvästä virheestä on puutteellinen tiedonkulun hallinta (yhdeksi käsittelyrutiinilta toiselle; "incomplete mediation"). Tästä esimerkkinä on
a. () aliohjelman kutsuminen ilman parametreja.
b. () muistialueen rajojen yli kirjoittaminen.
c. (X) puutteellinen virheiden käsittely.
d. () tiedon muuttuminen sen lukemisen ja käytön välillä.
30. Oletetaan, että pääsynvalvontaa varten on jo luotu tietty ryhmärakenne toimijoille ja kohteille: kaikki oliot kuuluvat yhteen tai useampaan joukkoon. Mikä seuraavista malleista sallii eniten pääsyä? Toimijan pääsy kohteeseen sallitaan, jos
a. () toimijan ryhmitys on kohteen ryhmityksen osajoukko.
b. (X) toimija kuuluu ainakin yhteen kohteen ryhmistä.
c. () toimija kuuluu tarkalleen samoihin ryhmiin kuin kohde.
d. () kohteen ryhmitys on toimijan ryhmityksen osajoukko.
31. Miten toimikorttien prosessorit suhtautuvat julkisen avaimen kryptosysteemissä (i) avainten luomiseen, (ii) salaukseen, (iii) allekirjoitukseen? Ne kykenevät
a. (X) kaikkiin.
b. () (i):een mutta eivät muihin.
c. () (ii):een mutta eivät muihin.
d. () (ii):een ja (iii):een mutta eivät (i):een.
32. Kertakirjautumisen mekanismeja ovat
a. () SSL, Passport, Liberal Allowance
b. () Kerberos, Passphrase, Liberal Allowance
c. () Kerberos, Passport, Liberty Alliance
d. () SSH, Passphrase, Liberty Alliance
33. Suojamekanismeja valittaessa on otettava huomioon eri vaiheita, joihin ne voivat soveltua. Mitkä kolme?
a. (X) ehkäisy, havaitseminen ja reagointi.
b. () suunnittelu, toteutus ja valvonta.
c. () politiikan muodostaminen, uhkien torjunta ja vahinkojen korjaaminen.
d. () välttäminen, estäminen ja havaitseminen.
34. Tarkastellaan tietojenkäsittelyrauhan rikkomuksia, joita tietojenkäsittelylaitteeseen fyysisesti käsiksi pääsevä voi aiheuttaa. Mikä seuraavista ei ole laitteistonäkökulmasta tietoturvaongelma?
a. () laitteen siirtäminen toiseen paikkaan
b. () laitteen identiteetin muuttaminen
c. (X) esiintyminen tietoverkossa laitteen käyttäjän nimissä
d. () laitteessa olevien resurssien käyttö

35. Tietoturvaluisuus on yksi kohta yleisessä turvallisuusjaottelussa, jonka monilla muillakin kohdilla on yhtymäkohtia tietoturvaluuteen. Millä seuraavista yleisen turvallisuuden osa-alueista on *eniten* tekemistä sen kanssa, miten tietoturvaluisuutta varten toimitaan päivittäin?

- a. Ympäristönsuojelu
- b. Kiinteistö- ja toimitilaturvaluisuus
- c. Työturvaluisuus
- d. Valmiussuunnittelu

36. Etäkäytössä täytyy autentikoida kohdekone, jotta se ei voisi

- a. lähettää käyttäjän koneelle haittaohjelmia.
- b. antaa käyttäjän autentikointitietoja hyökkääjälle.
- c. joutua palvelunestohyökkäyksen kohteeksi.
- d. kohdistaa DoS-hyökkäystä käyttäjään.

37. Tietosuojavaltuutettu on

- a. Maija Kleemola
- b. Petri Jääskeläinen
- c. Riitta-Leena Paunio
- d. Reijo Aarnio

38. Mikä seuraavista ei päde, kun tietokannassa on arkaluonteisia tietoja? Voi olla, että

- a. niistä saa suojauksista huolimatta tietoa päättelyillä sallittujen kyselyiden avulla.
- b. niistä laaditut yhteenvetotiedot eivät ole arkaluonteisia.
- c. suojaukseksi riittää, etteivät sivulliset osaa muodostaa oikeanlaisia kyselyehtoja.
- d. tiedon olemassaoloakaan ei saa paljastaa.

39. Mikä seuraavien joukosta on tärkeintä, kun vanhemmat haluavat estää lastaan pääsemästä hänen kannaltaan arveluttaville seittisivuille?

- a. suodatuksen tekeminen sekä selaimessa, palomuurissa että palveluntarjoajalla.
- b. selaimessa olevan suodattimen perustaminen useisiin erityyppisiin kriteereihin.
- c. sisällön suodattimen asetusten suojaaminen muuntelulta.
- d. suodatussääntöjen muuttaminen lapsen iän mukana.

40. TTY:n (tai yhtä hyvin TaY:n) yleisen tason tietoturvaluoliikassa

- a. määrätään politiikan perustaksi jokin tietoturvaluustandardi.
- b. on alaluku joka erittelee toimintaohjeet poikkeusoloja varten.
- c. todetaan, että sen ja standardien perusteella laaditaan yliopiston tietoturvaluustitelma.
- d. määritellään joitakin tietoturvaluisuuden peruskäsitteitä.

41. Mikä seuraavista on muita tärkeämpää VPN:ssä, jonka pitää täyttää etäkäytön verkkoyhteyden tietoturvaluustarpeet?

- a. tunnelointi ja päätepisteiden kätcentä
- b. virtuaalisuus
- c. verkon toimivuus läpinäkyvästi
- d. autentikointi

42. VRK:n varmennepoliitikassa todetaan: "Kansalaisvarmenne koostuu varmenneparista, jolla on kaksi eri käyttötarkoitusta: todentamis- ja salausvarmenne ja allekirjoitusvarmenne". Mitä tämä toteamus sisältää?

- a. Toista varmennetta käytetään todentamiseen, toista puolestaan salaukseen ja allekirjoitukseen.
- b. Varmenne koostuu yksityista ja julkisesta osasta: toista (yksityistä) käytetään allekirjoitukseen ja toista (julkista) muihin tarkoituksiin.
- c. Yksi varmenne koskee allekirjoituksen todentamisavainta ja toinen sitä avainta, jolla muut salaavat viestejä varmenteen omistajalle tai autentikoivat hänet.
- d. Kummallakin varmenteella on kaksi eri käyttötarkoitusta.

43. Mikä seuraavista toteuttaa huonoimmin varsinaisen varmuuskopioinnin tavoitteita?

- a. sellainen päivittäinen kopiointi, jota ei yleensä tarkisteta
- b. kirjoitettavien CD-levyjen käyttö siten että niitä säilytetään samassa huoneessa
- c. Snapshot-tekniikkaa käyttävä tiedostojärjestelmä
- d. tiedostojärjestelmän sijainti verkkolevyllä, ja paikallisen koneen pitäminen käynnissä, jolloin muuttunut tieto on sen muistissa

44. Kotihakemiston ei pitäisi olla hakupolussa. Syyinä on se, että muuten

- a. varusohjelman sijasta käyttäjä voi tulla käynnistäneeksi hyökkääjän kirjoittaman ohjelman.
- b. tiedoston haku joutuu aina käymään läpi kaikki alihakemistot ja saatavuus heikkenee.
- c. salakuunteleva hyökkääjä pääsee paremmin jäljittämään käyttäjän toimia.
- d. lokitietoja tallettuu myös päähakemistoon ja käytettävyyys heikkenee.

45. Haittaohjelma voi käynnistyä oikean ohjelman sijasta tai silloin kun mitään ohjelmaa ei ollut tarkoitus käynnistää. Millä seuraavista on tämän kanssa vähiten tekemistä?

- a. tietoturva-aukko seittipalvelimen koodissa
- b. tiedostonimet
- c. dokumenttitiedoston avaaminen
- d. käyttöjärjestelmän vajaatoiminta

46. Tiedon ja datan yleistä olemusta jäsennetään materiaalin käsittekartassa viiteen pääsuuntaan. Seuraavissa luetteloissa on mainittu joitakin kartassa esiintyvistä tekijöistä. Missä luettelossa on vain sellaisia tekijöitä, jotka kartassa sisältyvät yhteen ja samaan suuntaan?

- a. siirto -- osoittamistapa -- levinneisyys
- b. toiminta (inhimillinen) -- prosessointi -- aktiivisuus
- c. roolit (ihmisen) -- elinkaari -- koodaustapa
- d. media -- alusta -- taso (piistä neuroneihin)

47. Kun tietokoneista rakennetaan suuria verkkoja, tiettyihin seikkoihin liittyy yhtäältä hyötyjä ja toisaalta tietoturvaluustarpeita. Tällaisia verkon piirteitä ovat kurssiaineiston mukaan mm.

- a. resurssien jakaminen, monimutkaisuus, asiakas-palvelin -rakenne.
- b. resurssien jakaminen, arvaamattomat polut, anonyymius.
- c. hyökkäyskohtien lukuisuus, anonyymius, protokollien kerroksellisuus.
- d. arvaamattomat polut, protokollien kerroksellisuus, epämääräiset rajat.

48. **Materiaalissa sanotaan: "Avaintenvaihto on yksi tärkeimmistä kryptografisista protokollista." Mitä avaintenvaihto, eli 'key exchange' tässä tarkoittaa?**
- Symmetrisestä avaimesta sovitaan.
 - Julkinen avain peruutetaan ja uusi varmennetaan.
 - Päivitetty julkinen avain rekisteröidään.
 - Vanha symmetrinen avain päivitetään.
49. **Yksi turvallisen ohjelmoinnin perussäännöistä on "Vähennä hyökkäyskohteita." Se tarkoittaa lähinnä, että**
- ohjelma vastaanottaa mahdollisimman vähän syötteitä käyttäjältä.
 - ohjelma pystyy toimimaan mahdollisimman vähin eritasoisin oikeuksin.
 - ohjelmaan on talletettu mahdollisimman vähän muiden ohjelmien, palveluiden tai seittiviestien nimiä ja osoitteita.
 - ohjelman vähän käytetyt piirteet ovat oletuksena epäaktiivisessa tilassa.
50. **Viitemonitorin tehtävänä luotetussa tietojenkäsittelyssä on**
- tehdä lokimerkintä tietoturvaliikkeen vastaisesta tietoliikenteestä.
 - asettaa käyttäjien oikeudet resurssisiin pääsynvalvonnan tauluihin.
 - välittää kaikki vuoro vaikutus käyttäjien ja resurssien välillä.
 - hallinnoida epäsuorien muistiviittausten osoitetauluja.
51. **Ihmisiä voidaan suojata tiedolta tai tietoa ihmisiltä. Mikä seuraavista on tavallisin esimerkki jälkimmäisestä?**
- Tietoon ei haluta antaa pääsyä ilmaiseksi.
 - Tieto ei ole luotettavaa.
 - Muualla vapaasti saatavilla olevaa tietoa ei haluta vastaanottaa jossain päin maailmaa.
 - Suojaamatta ja rajoituksetta leviävä tieto tukkisi tietoliikenneverkot.
52. **Mikä seuraavista edustaa sellaista fyysistä tiedon tallennetta, jonka väärentäminen vaikuttaa toimijan oikeuksiin mutta ei autenttisuuteen?**
- matkakortti, jolla on arvolippu
 - kirjaston lainauskortti
 - musiikki-CD
 - huvipuiston ranneke
53. **Millaisia torjuntamekanismeja voi jättää riskianalyyysissa käsittelemättä?**
- Sellaisia, jotka ratkaisevat saman ongelman kuin analyysissa jo käsitellyt mekanismit.
 - Mekanismeja, jotka eivät torju tarkasteltavaan järjestelmään kohdistuvia uhkia.
 - Sen tyyppisiä mekanismeja, joita kohdejärjestelmässä ei ole vielä olemassa.
 - Riskianalyyysiin ei kuulu torjuntamekanismien käsittely.
54. **Tavallinen salalukku julkisen avaimen kryptosysteemeissä on**
- kahden suuren alkuluvun tulon tekijöiden eli kyseisten eri alkulukujen tunteminen.
 - suuren alkulukupotenssin neliöjuuren tunteminen.
 - kyky laskea diskreetti logaritmi kahden alkuluvun tulon suhteen.
 - kyky laskea diskreetti logaritmi suuren alkuluvun suhteen.
55. **Tietoturvatavoite kiistämättömyys tarkoittaa, että**
- henkilöllä, johon tiedot liittyvät, ei ole perusteita väittää, ettei liittymää olisi.
 - joku sopimuksen osapuolista on yrittänyt sanoutua irti tiedoista, mutta hänen on voitu todistaa erehtyneen.
 - tietoihin niiden hyväksymisen jälkeen vahingossa tai tahallaan tehdyt muutokset pystytään korjaamaan.
 - tiedot (esim. sopimus), joihin se liittyy, on ymmärretty ja hyväksytty.
56. **Jos www-sivuja julkaisevien osapuolten tietoturvaluokkia jaotellaan neljään luokkaan, niin mitkä seuraavista kattavat ne parhaiten?**
- sivujen luottamuksellisuus, sivujen eheys, asianmukaisen korvauksen saaminen, vastuiden kantaminen.
 - sivujen saatavuus, sivujen eheys, asianmukaisen korvauksen saaminen, se että pystyy huolehtimaan vastuista.
 - sivujen saatavuus, sivujen autenttisuus, tekijänoikeuksien puolustaminen, vastuiden kantaminen.
 - sivujen autenttisuus, sivujen eheys, asiakkaan autenttisuus, vastuista vapautuminen.
57. **Kurssimateriaalissa mainituissa kolmessa tietoaineistojen luokitusmerkissä keskeisimmät luokat ovat lähes tosiaikainen, kriittinen ja salainen. Minkä näkökulman mukaan tehtävää luokitusta näissä ei ole mukana?**
- luottamuksellisuus
 - saatavuus
 - eheys
 - ajantasaisuus
58. **Mikä seuraavista on huonoin vastaus kysymykseen: "Tarvitaanko tietokannoissa tarkempaa pääsynvalvontaa kuin tietokannan sisältävän koneen käyttöjärjestelmä tarjoaa?"**
- Yleensä tarvitaan.
 - Kyllä tarvitaan, jos tiedosto-oikeuksien tasolla tehty käyttäjien erottelu ei riitä.
 - Ei tarvita, jos tietokannan käyttäjiä ei tarvitse erotella toisistaan.
 - Ei tarvita, jos kaikilla koneen käyttäjillä on samat oikeudet tietokantaan.
59. **Työelämän tietosuojalaki vaikuttaa siihen, mitä tietoja työnantaja saa selvittää työntekijän taustasta. Mikä on lain vaikutus, kun tarkistuksen kohde on työnhakija yrityksen (i) sisältä, (ii) ulkopuolelta?**
- Vaikuttaa (ii):een mutta ei (i):een.
 - Ei vaikuta kumpaankaan.
 - Vaikuttaa (i):een mutta ei (ii):een.
 - Vaikuttaa molempiin.
60. **Mitkä seuraavista ei ole käytetty www-termin 'cookie' suomennoksena?**
- keksi
 - pipari
 - kuitti
 - keite