TTY / TIE / J. Harju

TIE-03100 Tietoverkot ja tietoturva

Tentti 18.1.2016

Tentissä ei saa käyttää laskinta. Tätä tehtäväpaperia ei tarvitse palauttaa.

Sekä rastilomake että konseptiarkki pitää palauttaa. Huom. palautus ERI nippuihin: älä sijoita rastilomaketta konseptiarkin sisään!

Kirjoita vastauksesi esseetehtäviin (1-3) konseptiarkille ja rastitehtäviin (4-39) lomakkeelle. Kirjoita kummallekin nimesi ja opiskelijanumerosi. Lomakkeelle opiskelijanumero pitää merkitä myös rastimalla ao. numeromerkit. Tee rastitehtävien luonnokset ja korjaukset mieluummin tälle paperille kuin lomakkeelle! Tentin jälkeen voit silloin myös helpommin verrata vastauksiasi kurssin Moodlesta löytyvään oikeaan riviin sekä aikanaan tuloslistassa julkaistaviin vastauksiin, jotka on luettu lomakkeeltasi.

Kussakin rastitehtävässä 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.

TEHTÄVÄT 1-3 OVAT ESSEETEHTÄVIÄ, MAX 8p/teht. VASTAA KONSEPTIARKILLE!

---

1. Tarkastellaan julkisen avaimen ja symmetrisen avaimen salausjärjestelmiä.

   a) Kerro periaatteet kummastakin järjestelmästä, eli mitä tarkoitetaan julkisen avaimen järjestelmällä ja mitä symmetrisen avaimen järjestelmällä? (4p)
   b) Miksi molempia tarvitaan? Esitä konkreettisia esimerkkejä, millaisiin tilanteisiin ne soveltuvat ja miksi. (4p)

2. Reititys ja IP-protokolla ovat Internetin toiminnan keskeisimpiä asioita:

   a) Mitä tarkoitetaan aliverkolla, miten se määritellään IP-osoitteiden avulla ja mikä on sen merkitys reitityksen kannalta? (4p)
   b) Mikä on reititysprotokollien tehtävä ja mitä erityyppisiä reititysprotokollia Internetissä käytetään? (4p)

3. Tarkastellaan protokollien kerrosmallin kahta kerrosta, *kuljetuskerrosta* ja *siirtokerrosta* eli *linkkikerrosta*.

   a) Miten nämä kerrokset sijoittuvat kerrosmalliin? (2p)
   b) Mitkä ovat näiden kerrosten tärkeimmät tehtävät? (2p)
   c) Mitä yhteistä, mitä erilaista toiminnallisuutta näissä kerroksissa on? (2p)
   d) Mainitse nimeltä vähintään yksi protokolla kummastakin kerroksesta. (2p)

MONIVALINTAOSUUS ALKAA TÄSTÄ: TEHTÄVÄT 4 - 39 OVAT MONIVALINTATEHTÄVIÄ. VASTAA ERILLISELLE LOMAKKEELLE! Kirjaa vastauksesi myös tälle kysymyslomakkeelle, jonka voit ottaa mukaasi. Sen avulla voit helposti tarkastaa monivalintaosuuden tuloksesi, kun oikea rivi julkistetaan Moodlessa tentin jälkeisenä päivänä.

4. **Minkä seuraavista laitteista pitäisi lähinnä kyetä palomuurin tapaiseen pakettien suodatukseen?**
   a. ( ) työaseman verkkokortti
   b. ( ) verkkokytkin
   c. ( ) www-selain
   d. (x) reititin
5. **Mikä seuraavista ei päde reitityksessä:**
   a. ( ) reititystaulunsa perusteella reititin päättelee, mikä on seuraava etappi IP-paketin matkatessa kohti kohdettaan.
   b. ( ) runkoverkon reitittimen reititystaulu voi sisältää yli 300.000 kohdealiverkkoa.
   c. ( ) reititin voi hylätä paketin, jos sille ei löydy reittiä eteenpäin.
   d. (x) reititystaulunsa perusteella reititin muodostaa vastaavuuden paketin lähettäjän ja kohdelaitteen MAC-osoitteiden välille.
6. **Mikä seuraavista asioista liittyy mobiiliverkkoihin, mutta ei yrityksen tai organisaation WLAN-verkkoihin?**
   a. (x) Tiedonsiirron käytöstä on pystyttävä keräämään laskutustietoa.
   b. ( ) Turvallisuussyistä liikenne päätelaitteen ja tukiaseman välillä on syytä salata.
   c. ( ) Yhteyksien täytyy toimia siirryttäessä yhden tukiaseman alueelta toisen tukiaseman peittoalueelle.
   d. ( ) Verkon käyttäjät on pystyttävä tunnistamaan luotettavasti.
7. **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. (x) (i)
   b. ( ) (iii)
   c. ( ) (ii)
   d. ( ) (iv)
8. **Mihin seuraavista protokollista liittyy yhteydenmuodostusvaihe?**
   a. (x) TCP
   b. ( ) UDP
   c. ( ) ARP
   d. ( ) Ethernet
9. **ICMP-protokollan avulla laite voi lähettää ns. pingin eli Echo Request -viestin. Kun kohdelaite vastaanottaa pingin, niin se**
   a. ( ) jää odottamaan seuraavaa pingiä, mitaten siitä vasteajan.
   b. ( ) lähettää välittömästi pingin kaikille saman IP-aliverkon laitteille.
   c. ( ) lähettää Echo Reply -viestin reitittimelle.
   d. (x) lähettää Echo Reply -viestin takaisin lähettäjälle.

10. **Reititysvirheen sattuessa IP-paketti voi jäädä kiertämään kehää verkossa (ns. reitityssilmukka). Tilanteen pelastaa**
    a. (X) time-to-live-laskuri, jonka meneminen nollaksi aiheuttaa paketin tuhoamisen.
    b. ( ) alemman kerroksen protokolla, joka huomaa tilanteen ja tuhoaa paketin.
    c. ( ) kuljetuskerroksen protokolla, joka raportoi asiasta lähettäjälle.
    d. ( ) ICMP-protokolla, joka huomaa silmukan ja palauttaa paketin lähettäjälle.
11. **Miksei tyypillinen symmetrinen salaus- ja purkualgoritmi kelpaa allekirjoituskäyttöön?**
    a. ( ) Sellaisella ei voi muodostaa digitaalista kirjekuorta.
    b. (X) Kenelläkään ei olisi todentamiseen tarvittavaa avainta.
    c. ( ) Sellaisen avaimet ovat liian lyhyitä pitkäaikaiseen käyttöön.
    d. ( ) Allekirjoittaja voisi väittää, ettei hän vaan todentaja on laatinut allekirjoituksen.
12. **Ethernet-kytkin on laite, joka**
    a. (X) voi toimia verkon tähtitopologiassa keskussolmuna.
    b. ( ) toimii fyysisen kerroksen tasolla.
    c. ( ) tekee muunnoksen pakettikytkennästä piirikytkentään.
    d. ( ) reitittää lähiverkon paketteja IP-aliverkkojen välillä.
13. **Tietosuojan keskeinen merkitys on**
    a. ( ) yksityisten ihmisten salaisten tietojen suojaamisessa.
    b. ( ) yritysten erilaisille tiedonkerääjille kertomien tietojen suojaamisessa.
    c. ( ) yritysten salaisten tietojen suojaamisessa.
    d. (X) yksityisten ihmisten erilaisille tiedonkerääjille kertomien tietojen suojaamisessa.
14. **IPsecin voi asentaa myös reitittimien välille. Mitä seuraavista voi sen avulla tällaisessa yhteydessä toteuttaa: (i) tunkeutumisen havainnointi, (ii) sovellustason palomuuri, (iii) VPN? Vain**
    a. ( ) (i) ja (iii)
    b. (X) (iii)
    c. ( ) (i)
    d. ( ) (i) ja (ii)
15. **Mikä seuraavista ei kuulu käsitteen kryptoalgoritmi piiriin?**
    a. ( ) satunnaislukugeneraattori
    b. ( ) hash-funktio
    c. ( ) avaimellinen tiivistefunktio
    d. (X) haaste-vaste -menetelmä
16. **Internetissä tarvitaan luotettavaa yhteydellistä kuljetusprotokollaa, koska**
    a. ( ) fyysisellä kerroksella tapahtuneet bittivirheet voi korjata vain kuljetuskerroksella.
    b. ( ) reaaliaikavaatimukset (eli vaatimukset pienestä viiveestä ja viiveenvaihtelusta) edellyttävät luotettavaa kuljetusprotokollaa.
    c. (X) verkkokerroksen protokolla IP on yhteydetön ja siksi epäluotettava.
    d. ( ) yhteyksille olisi muuten mahdotonta taata riittävää tietoturvatasoa.
17. **Mikä seuraavista on mahdollinen merkintä niin sanotun C-luokan aliverkon 198.230.4.0 verkkomaskille? (i) /24, (ii) 11111111 11111111 11111111 00000000, (iii) 255.255.255.0.**
    a. ( ) vain (ii) ja (iii)
    b. (X) (i), (ii) ja (iii)
    c. ( ) vain (i)
    d. (X) vain (i) ja (iii)
18. **Jos pakettikytkentäisen verkon operaattori ns. ylibuukkaa verkkonsa eli myy verkon kapasitettia liian suurelle määrälle asiakkaita, niin**
    a. (X) asiakkaan kokema palvelunlaatu huononee sitä enemmän mitä enemmän käyttäjämäärä ylittää ylibuukkauskynnyksen.
    b. ( ) asiakas ei voi huomata asiaa ilman erityisiä protokollatyökaluja.
    c. ( ) asiakkaan verkkoyhteys katkeaa silloin, kun käyttäjämäärä ylittää ylibuukkauskynnyksen.
    d. ( ) se vaikuttaa välittömästi asiakkaan kokemaan palvelunlaatuun riippumatta ajankohdasta ja palvelua käyttävien asiakkaiden määrästä.
19. **Jos palomuuri hylkää jonkin paketin,**
    a. (X) se kirjoitetaan lokitiedostoon.
    b. ( ) sen kryptografinen tiiviste kirjoitetaan lokitiedostoon.
    c. ( ) se lähetetään takaisin sinne, mistä se tulikin.
    d. ( ) voidaan jättää lokimerkintä myös tekemättä.
20. **Selaaja pyrkii johonkin luottamusta edellyttävään www-osoitteeseen ja selain saa www-palvelimelta TLS-kättelyssä *ennalta näkemättömän* julkisen avaimen K, jonka pitäisi olla kyseisen palvelimen oma. Mitä sitten?**
    a. ( ) Käyttäjä pääsee haluamalleen www-sivulle suoraan, jos selaimessa on luottamus avaimeen, jolla K on varmennettu.
    b. ( ) Selain varoittaa asiasta ja käyttäjän pitäisi laskea kyseisen avaimen sormenjälki ja verrata sitä uudelleen ladatun sivun tuottamaan sormenjälkeen.
    c. ( ) Käyttäjä voi näennäisesti edetä haluamalleen www-sivulle vastattuaan "ok" selaimen kysymykseen, mutta palvelin on todennäköisesti jokin muu kuin hän luulee.
    d. (X) Selain pyytää K:lle varmenteen jostain varmennepalvelusta ja jos varmenne saadaan, selain antaa käyttäjälle mahdollisuuden asentaa K selaimeen.
21. **Päätelaitteen pitää lähettää IP-paketti kohdelaitteelle, joka IP-osoitteen mukaan sijaitsee samassa aliverkossa, jossa lähettäjäkin on. Suoran toimitustavan periaatteen mukaisesti päätelaitteen tulee selvittää kohteen MAC-osoite. Tähän se käyttää apunaan protokollaa nimeltä**
    a. ( ) DHCP.
    b. ( ) DNS.
    c. ( ) ICMP.
    d. (X) ARP.
22. **Tietoturvallisuuden osa-alueena mainitaan joissain yhteyksissä tietosodankäynti, mutta yrityksen näkökulmasta sen voi sisällyttää yleisemmän turvallisuusjaottelun osa-alueeseen**
    a. (X) turvallisuusjohtaminen.
    b. ( ) valmiussuunnittelu.
    c. ( ) force majeure -uhkien torjunta.
    d. ( ) ulkomaantoimintojen turvallisuus.
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. ( ) Et tarvitse salasanaa miltään muulta koneelta.
    b. (X) Salasanan takana ei ole mitään arvokasta.
    c. ( ) Salasana on niin entrooppinen, ettet pystyisi sitä muistamaan.
    d. ( ) Selaimesi salasanat ovat suojattuja muilta.

24. **Jos verkkopalvelussa pitää salasanan unohtamisen varalle keksiä kysymys ja vastaus, mikä seuraavista on autenttisuuden kannalta tärkeintä?**
    a. ( ) kysymyksen entrooppisuus
    b. ( ) kysymyksen ja vastauksen yhteensopivuus
    c. (X) vastauksen muistettavuus
    d. ( ) vastauksen entrooppisuus
25. **Käsite tietoverkon tietoturva kattaa tietyn osan tietoverkkoon liittyvästä tietoturvasta. Mikä seuraavista kuuluu sen piiriin, selvemmin kuin muut?**
    a. ( ) Arkaluonteisen Word- tai OpenOffice-dokumentin suojaksi asetetun salasanan murtuminen brute-force -hyökkäyksellä.
    b. (X) Www-palvelimen toiminnan lakkaaminen, kun siihen kohdistetaan DoS-hyökkäys useista eri osoitteista.
    c. ( ) Viranomaisten mahdollisuus luoda peiteoperaatioitaan varten anonyymia Bitcoin-verkkorahaa.
    d. ( ) Verkon päätelaitteen käyttöjärjestelmässä oleva haavoittuvuus.
26. **Materiaalissa sanotaan: "Avaintenvaihto on yksi tärkeimmistä kryptografisista protokollista." Mitä avaintenvaihto, eli 'key exchange' tässä tarkoittaa?**
    a. (X) Osapuolet kertovat toisilleen autentikoidusti julkiset avaimensa.
    b. ( ) Vanha julkinen avain peruutetaan ja uusi varmennetaan.
    c. ( ) Vanha symmetrinen avain päivitetään.
    d. ( ) Symmetrisestä avaimesta sovitaan.
27. **Autonomisten järjestelmien (AS) välisessä reitityksessä**
    a. (X) käytetään reititysprotokollana OSPF-protokollaa.
    b. ( ) käytetään reititysprotokollana BGP:tä.
    c. ( ) käytetään MAC-osoitteita ja APR-protokollaa.
    d. ( ) käytetään staattista reititystä.
28. **Hyökkääjän pääsy tietoverkon kautta aiheuttamaan harmia toteutuu neljän vaiheen kautta, jotka ovat tiivistettyinä aakkosjärjestyksessä haavoittuvuus, prosessi, tieto ja valtuuttamaton toimi. Mikä on oikea yleispätevä järjestys?**
    a. ( ) Haavoittuvuus käynnistää prosessin, jonka hyökkääjä saa haltuunsa ja voi siten vahingoittaa/saada selville tietoa.
    b. (X) Haavoittuvuus antaa mahdollisuuden valtuuttamattomaan toimeen, jossa hyökkääjä saa käyntiin prosessin, joka kohdistuu tietoon.
    c. ( ) Hyökkääjän käynnistämä prosessi käyttää haavoittuvuutta valtuuttamattomaan toimeen tietoa kohtaan.
    d. ( ) Tieto haavoittuvuudesta antaa hyökkääjälle mahdollisuuden käynnistää valtuuttamattomasti prosessi.
29. **Yksi mahdollinen toiminta IPsecillä on, että se**
    a. ( ) lähettää paketin mukana purkuavaimen digitaalisessa kirjekuoressa.
    b. ( ) kompressoi datapaketin.
    c. (X) salaa myös alkuperäisen vastaanottajan IP-osoitteen.
    d. ( ) purkaa datasta ylemmän protokollakerroksen tekemän salauksen.
30. **Millä seuraavista on vähiten tekemistä perinteisten 2G- tai 3G-matkapuhelujen kanssa?**
    a. ( ) autentikointi
    b. ( ) tietoturvapolitiikka
    c. ( ) avainten hallinta
    d. (X) virustorjunta
31. **Oletetaan (tavalliseen tapaan), että julkisen avaimen infrastruktuurissa esiintyy varmentajia, jotka menevät takuuseen siitä, että asiakkaan julkinen avain liittyy juuri kyseisen asiakkaan identiteettiin. Tämä avaimen ja identiteetin sidonta toteutetaan**
    a. ( ) allekirjoituksella, jonka varmentaja laskee identiteetistä ja julkisesta avaimesta käyttäen *omaa* yksityistä avaintaan.
    b. ( ) merkitsemällä sekä identiteetti että julkinen avain julkiseen mutta *turvattuun* tietokantaan.
    c. (X) tallentamalla identiteetti julkisesti ja vastaava *yksityinen* avain salaisesti turvattuun tietokantaan, josta varmentaja julkisen avaimen pätevyyttä kysyttäessä osoittaa sen allekirjoituksella ko. yksityistä avainta käyttäen.
    d. ( ) tallettamalla sekä identiteetti että julkinen avain toimikortille, josta ne voi *vain lukea* mutta ei muuttaa – ainakaan särkemättä korttia ja sille talletetun yksityisen avaimen käyttökelpoisuutta.
32. **Tutki väitettä: Kryptoalgoritmit ovat joko symmetrisiä salausalgoritmeja tai epäsymmetrisiä salaus- tai allekirjoitusalgoritmeja. Se on**
    a. ( ) tosi, koska salauksen purkamista tai allekirjoituksen todentamista ei ole järkevää luokitella erikseen.
    b. ( ) epätosi, mutta steganografian eli piilokirjoituksen mukaanottaminen tekisi väitteestä toden.
    c. ( ) epätosi, koska luettelosta puuttuu sellaisia algoritmeja, joissa ei käytetä avainta.
    d. (X) tosi, koska perinteisen salauksen rinnalle tullut digitaalinen allekirjoitus tapahtuu salauksen tapaisella algoritmilla, mutta se ei ole symmetrinen.
33. **Oletetaan, että päätelaitteen A ja palvelimen B välinen tietoliikenneyhteys koostuu Ethernet-pohjaisesta kytkin- ja reititinverkosta. B:n suojana on tilallinen palomuuri. Mitkä seuraavista laitteista käsittelevät A:n ja B:n välisellä TCP-yhteydellä kulkevan paketin TCP-headeria päätelaitteen ja palvelimen lisäksi? (i) palomuuri, (ii) Ethernet-verkon kytkimet, (iii) verkon reitittimet.**
    a. ( ) vain (iii)
    b. (X) vain (i)
    c. ( ) vain (ii)
    d. ( ) (i), (ii) ja (iii)
34. **Mikä on aliverkon 130.230.4.64/26 viimeinen osoite eli broadcast-osoite?**
    a. ( ) 130.230.7.255
    b. ( ) 130.230.4.255
    c. (X) 130.230.4.127
    d. ( ) 130.230.4.95
35. **Mikä on välttämätöntä, jotta kahden suuren alkuluvun p ja q tuloa voi käyttää julkisen avaimen kryptografiassa julkisena avaimena?**
    a. ( ) Pitää tarkistaa onko kyseisiä alkulukuja vastaavaa yksityistä avainta olemassa.
    b. ( ) Täytyy julkaista myös p*p modulo q, tai q*q modulo p.
    c. (X) Pitää tarkistaa, ovatko myös p-1 ja q-1 alkulukuja.
    d. ( ) Kyseiset alkuluvut eivät saa olla muiden kuin omistajansa tiedossa.
36. **Paketinnuuskijan ('packet sniffer') tarkoituksena on**
    a. ( ) poistaa verkkoliikenteestä asiaankuulumattomia paketteja.
    b. ( ) skannata verkon segmenttejä kaapelointivaurioiden varalta.
    c. ( ) jäljittää verkkoyhteyksiä ulkoisiin kohteisiin.
    d. ( ) kaapata (kopioida) verkkoliikennettä myöhempää analyysia varten.

37. **Minkä seuraavista voi verkkoon kytketty laite hankkia itselleen DHCP:n avulla? (i) vapaan porttinumeron, (ii) oletusreitittimen IP-osoitteen, (iii) uuden MAC-osoitteen.**
    a. ( ) kaikki kolme
    b. (X) vain (ii):n
    c. ( ) vain (i):n
    d. ( ) vain (iii):n
38. **Verkosta ladattavan ohjelman joistakin ominaisuuksista voidaan vakuuttua sellaisten allekirjoitusten perusteella, joita esimerkiksi Verisign tarjoaa, mutta nämä takaavat vain koodin**
    a. (X) alkuperää ja eheyttä.
    b. ( ) valmistajan ottavan vastuun mahdollisista turvaongelmista.
    c. ( ) läpäisseen virustarkistuksen, joskin useilla eri menetelmillä.
    d. ( ) vastaavan määrityksiään.
39. **IP-aliverkon oletusreititin**
    a. ( ) on reititin, jolle IP-aliverkon laite voi lähettää paketit, jotka ovat menossa ulos ko. IP-aliverkosta.
    b. (X) on reititin, jonka IP-osoite on 0.0.0.0.
    c. ( ) on reititin, jolle muualta Internetistä lähetetään paketit, joiden kohde on ko. IP-aliverkossa.
    d. ( ) on reititin, jonka avulla tapahtuu pakettien jakelu IP-aliverkon sisällä.