TLT-3201 Tietoturvallisuuden jatkokurssi

Välikoe, I yrityskerta 25.10.2012

---

1. **CBC-salauksen purussa voi tulla kaksi samanlaista selkotekstilohkoa peräkkäin.**
   a. (X) Tosi b. ( ) Epätosi

2. **ElGamalin julkisen avaimen kryptosysteemin turvallisuus perustuu siihen, että kahden suuren alkuluvun tuloa on vaikea jakaa tekijöihin.**
   a. ( ) Tosi b. (X) Epätosi

3. **Luotettu tietojenkäsittelyjärjestelmä, TCB, on sellainen laitteiston ja ohjelmiston kokoelma, että sen ulkopuoliset osat voisi periaatteessa antaa vaikka hyökkääjän rakennettaviksi, eikä tietoturvapolitiikasta silti tarvitsisi tinkiä.**
   a. (X) Tosi b. ( ) Epätosi

4. **PGP kertoo käyttäjälleen laskennallista tietoa julkisen avaimen luotettavuudesta.**
   a. (X) Tosi b. ( ) Epätosi

5. **Oletetaan, että jokin luonnonilmiö tuottaa muuten ennustamattomia bittejä, mutta siinä on jokin vinoutuma. Mikä seuraavista on sellainen vinoutuma, jonka vuoksi tuotettuja bittijonoja ei voi korjata kryptografisiin tarkoituksiin kelpaaviksi?**
   a. (X) Kun ilmiö pannaan uudestaan käyntiin samasta alkutilasta, se tuottaa saman bittijonon kuin ennenkin.
   b. ( ) Osajonona ei koskaan esiinny 101010.
   c. ( ) Nollia tulee keskimäärin 40% biteistä.
   d. ( ) Aina kun on tullut viiden ykkösen juoksu, ilmiö jää jumiin ja tuottaa viisi peräkkäistä ykköstä ennen kuin jatkaa normaalisti.

6. **Miksei tavanomainen vastesuunnitelma riitä, jos tarvitaan suunnitelma yrityksen liiketoiminnan turvaamiseksi tietoturvapoikkeamien sattuessa?**
   a. (X) Koska se liittyy vain siihen, mitä tehdään hyökkäyksille tai hyökkääjille.
   b. ( ) Koska se muodostetaan jättämällä pois yritykseen soveltumattomat kohdat VAHTI-ohjeiden tai vastaavien yleisten suositusten tarkistulistoista.
   c. ( ) Koska siinä esitettyjen toimien kesto on liian lyhyt.
   d. ( ) Koska se ei sisällä passiivisiin uhkiin reagointia.

7. **Diffie-Hellmanin avaintenvaihtoprotokollassa:**
   a. ( ) Jos diskreettien logaritmien laskeminen modulo suuri alkuluku tosiaan on vaikea probleema (kuten yleisesti uskotaan), DH-protokolla varmistaa DH-neuvotteluun osallistuneille saman avaimen, jota kukaan muu ei tiedä.
   b. ( ) Toinen osapuoli keksii alkuluvun p ja toinen alkuluvun q. Näiden suurten lukujen tulo n on julkinen avain, joka toimii avaintenvaihdon moduulina.
   c. (X) Kumpikin osapuoli korottaa kantaluvun g johonkin potenssiin modulo p, ja kertoo tuloksen toiselle, mutta kumpikaan ei tule tietämään, mikä toisen osapuolen käyttämä eksponentti oli.
   d. ( ) Välimieshyökkäys A:n ja B:n välillä käytävää DH-protokollaa vastaan johtaa tulokseen, jossa viestejä releöineellä välimiehellä on sama avain sekä A:n että B:n kanssa.

8. **Yhtenä AES:n kierrosten neljästä operaatiosta on kunkin tavun korvaaminen jollain toisella, joka määräytyy**
   a. ( ) satunnaisesti muodostetun vakiona pysyvän korvaustaulun perusteella.
   b. ( ) avaimesta riippumattoman matemaattisen kaavan mukaan.
   c. ( ) avaimen perusteella samalla tavalla kullakin kierroksella.
   d. ( ) kierrosavaimen perusteella eri tavalla kullakin kierroksella.

9. **Mikä seuraavista ei ole jonkin kryptosysteemin standardoinnissa mahdollista?**
   a. ( ) Standardin on julkaissut vain jokin yritys eikä kansainvälinen organisaatio.
   b. ( ) Samasta algoritmista samalla nimellä on julkaistu epäyhteensopivia standardeja.
   c. ( ) Useampi kuin yksi standardointiorganisaatio julkaisee samanlaisen standardin.
   d. ( ) Samanaikaisesti on standardoituna eri versiota samasta kryptosysteemistä.

10. **Mikä seuraavista on vähiten välttämätön julkisen avaimen K varmenteessa X.509:n mukaan? Tieto**
    a. (X) varmennepolitiikasta
    b. ( ) K:n haltijasta
    c. ( ) algoritmista, jolla K:ta käytetään
    d. ( ) voimassaolon alkuajasta

11. **Bell-LaPadula -mallin vuorovesimerkki tarkoittaa**
    a. ( ) ylintä tasoa, jonka mukaista tietoa prosessi on lukenut. Merkki on siis prosessilla.
    b. (X) alinta tasoa, jonka mukaista tietoa prosessi on lukenut. Merkki on siis prosessilla.
    c. ( ) ylintä tasoa, jonka mukainen prosessi on käsittelyt tietoa. Merkki on siis tiedolla.
    d. ( ) alinta tasoa, jonka mukainen prosessi on käsittelyt tietoa. Merkki on siis tiedolla.

12. **Miten prosessit, säikeet ja keskeytykset lähinnä suhtautuvat toisiinsa?**
    a. ( ) Säikeet ovat prosesseja, jotka eivät voi keskeytyä.
    b. ( ) Useista prosesseista voi muodostua säie, keskeytys käynnistää aina prosessin.
    c. ( ) Kellon lisäksi prosessien keskeytykset aiheutuvat säikeistä.
    d. (X) Prosessi voi jakautua säikeisiin, jotka voivat keskeytyä.

13. **Niissä RAID-systeemeissä, jotka edistävät tietoturvaa,**
    a. ( ) esiintyy levyrikosta toipumisen tapauksessa ylimääräinen uhka luottamuksellisuudelle.
    b. (X) voi olla mukana myös nopeuden edistäminen.
    c. ( ) on luontevaa toteuttaa eritasoisia tietoturvatarpeita eri tiedostoille.
    d. ( ) korvautuu varmuuskopioinnin tarve laitteistovikojen uhkan osalta.

14. **Microsoftin salaavassa tiedostojärjestelmässä EFS:ssä generoidaan eri salausavain**
    a. ( ) jokaiselle hakemistolle, jossa on salattavia tiedostoja.
    b. ( ) jokaiselle levytallennuksen lohkolle, jota salaus koskee.
    c. ( ) jokaiselle käyttäjälle.
    d. ( ) jokaiselle salattavalle tiedostolle.

15. **Mihin lähinnä liittyy sivutetun keskusmuistin sivutaulussa oleva läsnäolobitti?**
    a. ( ) heittovaihtoon (swapping)
    b. ( ) semanttiseen segmentointiin
    c. ( ) muistin suojauksiin
    d. ( ) osoite- ja muistiavaruuden eroon

16. **Kun toisen osapuolen pitää löytää juuri se kohde, jota kohteen nimennyt osapuoli tarkoittaa, voi nimen toimivuudessa ilmetä ongelmia. Mikä seuraavista on kattavin luokitus näille?**
    a. ( ) kohde kateissa -- useita kohteita -- väärä kohde -- nimi kateissa
    b. ( ) nimeä ei tunneta -- nimellä useita kohteita -- väärä tulkinta -- väärä nimi
    c. ( ) konteksti väärä -- käännös väärä -- aika väärä -- nimi puuttuu
    d. ( ) kohde vaihtunut toiseksi -- kohde kadonnut -- nimeä käytetty uudestaan -- nimi virheellinen

17. **Mitä tekee TPM, Trusted Platform Module?**
    a. (X) Tekee julkisen avaimen krypto-operaatioita, joissa tarvitaan sen sisältämää yksityistä avainta.
    b. ( ) Tarkistaa käynnistyksen yhteydessä BIOS:n ja käynnistyssektorin haittaohjelmien varalta.
    c. ( ) Tarkistaa käyttäjän autentikoitumisdatan.
    d. ( ) Tallentaa palomuurisääntöjen ja haittaohjelmatietokannan tarkistussummat.

18. **Materiaalissa esiteltiin konkreettisia ohjelmoinnin turvaohjeita. Yksi listoista sisälsi 18 kohtaa, joista muutama liittyi muuttujien arvojen kelpoisuuden tarkastamiseen. Mitä seuraavista suositeltiin?**
    a. ( ) Käyttöjärjestelmän tarjoamien rajan tarkistusrutiinien soveltaminen.
    b. ( ) Muuttujille sallittujen vaihteluvälien ajoittainen säätäminen.
    c. ( ) Joidenkin muuttujien arvojen visualisointi käyttäjälle ohjelman suorituksen kuluessa.
    d. (X) Aliohjelmalle tai funktiolle menevän syötteen tarkistus.

19. **Kolme tunnettua tietoturvamallia ovat Bell-LaPadula (BLP), Biba ja Clark-Wilson (CW). Missä seuraavista on jaoteltu oikein näiden ominaisuudet?**
    a. ( ) hierarkkinen: BLP, Biba; luottamuksellisuus: BLP, CW; eheys: Biba
    b. ( ) hierarkkinen: BLP; luottamuksellisuus: BLP, CW; eheys: Biba, CW
    c. ( ) hierarkkinen: BLP, Biba; luottamuksellisuus: BLP; eheys: Biba, CW
    d. ( ) hierarkkinen: Biba, CW; luottamuksellisuus: BLP; eheys: Biba, CW

20. **Symmetrisen salauksen avaimen pituuden kaksinkertaistamisen seurauksena raa'an voiman hyökkäyksen vaatima aika muuttuu aiempaan verrattuna**
    a. ( ) enintään kaksinkertaiseksi
    b. ( ) vähintään kaksinkertaiseksi, mutta ei nelinkertaiseksi
    c. ( ) nelinkertaiseksi
    d. (X) toiseen potenssiin

21. **Materiaalissa esitettiin luettelo yli kymmenestä seikasta, jotka voivat vaikuttaa valintaan sen jälkeen kun vertailtavina on enää varsinaisen turvallisuustavoitteen toteuttavia mekanismeja. Mikä seuraavista kysymyksistä oli mukana listassa?**
    a. ( ) Ovatko ne valmiita palikoita?
    b. ( ) Onko niitä käytössä muilla yrityksillä?
    c. ( ) Ovatko ne eettisesti hyväksyttäviä?
    d. ( ) Edistävätkö ne luottamusta yritykseen?

22. **Mikä seuraavista ei kuulu symmetrisen kryptosysteemin avaimenhallintaan?**
    a. (X) avaimen pakkoluovutus (key escrow)
    b. ( ) avaimen asettaminen sulkulistalle
    c. ( ) avainmateriaalin luonti
    d. ( ) avainten jakelu

23. **Mikä seuraavista on muita turvallisempi tiivistealgoritmi?**
    a. (X) SHA-256
    b. ( ) MD-256
    c. ( ) MAC-3
    d. ( ) SHA1

24. **Oletetaan, että salasanatiedosto ei voi päästä asiattomien käsiin ja salasanat on tallennettu sinne salaamattomina. Mitä tällaisesta seuraisi?**
    a. ( ) Salasanoja ei tarvitsisi salata siirron aikana.
    b. ( ) Tavalliset käyttäjät eivät pystyisi vaihtamaan salasanaansa.
    c. (X) Kaikkien salasanat jouduttaisiin silti vaihtamaan ylikäyttäjän vaihtuessa.
    d. ( ) Salasanojen ei tarvitsisi olla yhtä pitkiä kuin yleensä.

25. **Kuinka monta eri turvaluokkaa syntyy, jos on tasot julkinen, sisäinen ja salainen sekä toimialueet A ja B?**
    a. ( ) 6
    b. ( ) 7
    c. (X) 12
    d. ( ) 5

26. **Unix/Linux-järjestelmissä tiedostojen ACL- eli pääsynvalvontalista**
    a. ( ) täytyy toteuttaa rooliperustaisen pääsynvalvonnan avulla, jos tiedoston moodi-bitit toimijoille user, group ja others eivät riitä.
    b. ( ) on uusimmissa versioissa korvannut tiedoston moodi-bitit.
    c. ( ) ei ole mahdollinen.
    d. (X) ei kuulu perinteiseen Unixiin mutta on joissakin järjestelmissä mahdollinen.

27. **Vesileimaus**
    a. ( ) särkyy, jos kuvaa vähääkään muunnellaan.
    b. ( ) toimii vain kuvatiedostoissa.
    c. ( ) on mekanismi tekijänoikeuden siirtämiseen.
    d. (X) voidaan tehdä niin, ettei sitä erota paljaalla silmällä edes suurennoksesta, jossa pikselit näkyvät erikseen.

28. **Mitä tarkoittaa DMA, direct memory access?**
    a. ( ) Sovellusohjelmaa käynnistäessään käyttöjärjestelmä tarkistaa ohjelman muistiviittaukset eikä tarkistuksia enää tarvita ajon aikana.
    b. (X) Laiteohjain pääsee käsiksi muistiin ilman, että tietoa täytyy siirtää CPU:n kautta.
    c. ( ) Virtuaalimuisti toteutetaan nopean väylän avulla ohi levyajurin.
    d. ( ) Kääntäjä ja linkittäjä tekevät ohjelman muistiviittauksista sillä tavoin absoluuttiset, ettei käyttöjärjestelmän tarvitse muuntaa niitä.

29. **Mitä tekemistä ohjelmalaskurilla (program counter) on käyttöjärjestelmän (KJ) kanssa?**
    a. ( ) Sen avulla KJ hallinnoi kyseisen ohjelman resurssien kulutusta.
    b. ( ) Se on KJ:n sovellusohjelmalle tarjoama ympäristömuuttuja.
    c. (X) Jos se osoittaa väärään kohtaan, KJ voi estää ohjelman suorituksen.
    d. ( ) Sen avulla KJ hallinnoi kaikkien samanaikaisesti ajossa olevien ohjelmien resurssien kulutusta.

30. **Mikä seuraavista vastaa parhaiten teoreettista määritelmää äärellistilaiseksi automaatiksi ajatellun tietojenkäsittelyjärjestelmän turvallisuudesta? Järjestelmä on turvallinen, jos**
    a. (X) kaikki mahdolliset tilasiirtymät politiikan mukaan turvallisista tiloista johtavat toisiin turvallisiin tiloihin.
    b. ( ) kaikki siirtymät turvallisten ja turvattomien tilojen välillä pystytään tunnistamaan.
    c. ( ) kaikki mahdolliset tilat ovat politiikan mukaan turvallisia.
    d. ( ) kaikki mahdolliset tilasiirtymät ovat politiikan mukaan turvallisia.

31. **Salaaminen NTRU-algoritmilla**
    a. ( ) on merkittävästi nopeampaa kuin salauksen purku.
    b. ( ) on nopeudeltaan RSA:n tapainen mutta tarvitsee merkittävästi vähemmän tilaa.
    c. ( ) on sama operaatio kuin NTRU-allekirjoituksen todentaminen.
    d. ( ) on satunnaistettu eli voi tuottaa samasta selkotekstistä eri kerroilla eri tuloksen.

32. **Luvuilla modulo 5 on kaksi generaattoria eli primitiivialkiota. Ne ovat**
    a. (X) 2 ja 3
    b. ( ) 2 ja 4
    c. ( ) 1 ja 4
    d. ( ) 3 ja 4

33. **Mikä seuraavista ei vaikuta DES-salauksessa tapahtuvaan lumivyöryilmiöön?**
    a. ( ) Ennen ja jälkeen varsinaisen Feistel-verkon DES toteuttaa permutaation.
    b. ( ) Joka kierroksella lohkon puolikkaat vaihtavat paikkaansa.
    c. ( ) Sen jälkeen kun S-laatikosto on korvannut 48 bittiä 32 bitillä, tehdään permutaatio ennenkuin kierrosfunktion tulos XOR-summataan lohkon toiseen puoliskoon.
    d. ( ) Kierrosfunktiossa f tapahtuu ensin bittimäärän kasvatus ja sitten kutistus.

34. **Hanoin torni -systeemi varmuuskopionnissa**
    a. ( ) edellyttää levyjen käyttöä tallennusvälineenä.
    b. ( ) on oleellisesti sama kuin grandfather-father-son -systeemi.
    c. (X) kuluttaa rotaatioon osallistuvia tallennusvälineitä epätasaisesti.
    d. ( ) on alunperin tarkoitettu välineille, joita ei voi kirjoittaa uudestaan.

35. **Mikä ero IPsecin ESP:n ja AH:n toiminnassa on?**
    a. ( ) AH:ssa MAC-algoritmin tulosta ei katkaista 96 bittiin kuten ESP:ssä.
    b. ( ) AH:ta ei voi käyttää tunnelimoodissa.
    c. (X) AH:ssa ei ole lainkaan salausta.
    d. ( ) ESP:ssä turvaparametri-indeksi (SPI) on kryptattu mutta AH:ssa ei.

36. **Missä salausmoodissa selkoteksti ei vaikuta lainkaan siihen, mitä lohkoalgoritmi saa syötteekseen?**
    a. (X) CTR
    b. ( ) OCB
    c. ( ) ECB
    d. ( ) CBC

37. **Java-kielen yleisiä turvallisuutta edistäviä piirteitä on**
    a. (X) osoittimien puuttuminen.
    b. ( ) automaattinen tyypinmuunnos.
    c. ( ) oliotyyppinen ohjelmointi.
    d. ( ) liukulukuvertailujen puuttuminen.

38. **Asiakas autentikoituu palvelimelle kertakäyttöisellä salasanalla, jotka on toteutettu iteratiivisella yksisuuntaisella funktiolla h. Tällöin tapahtuu oleellisesti seuraavaa:**
    a. ( ) palvelin laskee edellisen kerran vasteesta h:n ja lähettää haasteena autentikoitujalle.
    b. (X) asiakas lähettää arvon, palvelin laskee siitä h:n ja jos tulos on viimekertainen arvo, autentikointi on onnistunut.
    c. ( ) asiakas laskee muistamastaan edellisen kerran arvosta h:n ja lähettää tuloksen palvelimelle.
    d. ( ) palvelin lähettää haasteena jonkin edellisen kerran arvon ja asiakas laskee siitä h:n ja lähettää palvelimelle.

39. **Yrityksen tai organisaation tietoturvallisuus riippuu paljolti siitä, miten hyvin sen jäsenet noudattavat politiikkaa. Tähän on tutkimuksen mukaan kolme väylää. Mikä seuraavista ei ole yksi niistä?**
    a. ( ) perinteinen palkkioiden ja rangaistusten menetelmä.
    b. ( ) tietoisuuden kasvattaminen koulutuksen tai harjoittelun kautta
    c. (X) automaattisten valvontaohjelmistojen ja -välineiden käyttäminen
    d. ( ) tietoisuuden kasvattaminen turvakampanjoilla

40. **Vain yksi seuraavista tiedoista voi olla tarpeen neuvotella, kun sovitaan symmetrisestä salauksesta. Mikä?**
    a. ( ) algoritmin versio
    b. ( ) avainta modifioiva suola-arvo
    c. ( ) alustusvektori
    d. ( ) täytteen pituus