

8306000 Tietoturvallisuuden perusteet

Syksyn 1999 kurssin neljä tenttiä.

Tenttejä oli normaalin kolmen sijasta neljä, koska ensimmäinen oli alkuperäiseen tenttijärjestykseen merkitty vasta joulukuulle. Ensimmäinen oli siis ylimääräinen. Näitä ei julkaistu verkossa ennen kuin viimeinenkin oli pidetty.

Asteriskilla * on (jälkikäteen) merkitty tehtävät, jotka on muokattu niistä, joita opiskelijat ehdottivat viimeisellä luentokerralla.

Tuloksista on yhteenveto.

Alkuohjeena tenttipapereissa oli:

*Tutustu ensin kaikkiin tehtäviin ja laadi jokaiseen vajaan kymmenen avainsanan mittainen luonnos (jota ei tarvitse palauttaa). Kirjoita sitten **kuuteen** valitsemaasi tehtävään tiivis, oleelliseen keskittyvä vastaus, jonka etukäteiseen jäsenyykseen käytät vielä ehkä viisikin minuuttia. Rönsyilyistä tai pelkästä tunnelman luomisesta ei heru pisteitä, päinvastoin: Yli puolen sivun mittaista vastausta ei kannata kirjoittaa näihin kysymyksiin, ellei todella tiedä asiaansa, ja siinä tapauksessa sen osaa ja se riittää sanoa lyhyemminkin.*

1. tentti 19.10.1999

1. Miksi avaimenvaihto on niin tärkeä juttu ja miksi se on niin hankalaa? Diffie-Hellmanin protokollassa kaikki tietävät luvun g , A keksii luvun x ja saa B:ltä luvun g^y , B keksii luvun y ja saa A:ltä luvun g^x . Kumpikin voi siis laskea avaimeksi luvun g^{xy} . Mikä matemaattinen "yksityiskohta", joka jäi tässä kertomatta, tekee suunnattoman vaikeaksi kenellekään muulle laskea lukua g^{xy} ?
2. Kenen pitää laatia tietoturvaläpöintiä ja miten se tapahtuu?
3. * Mitä toivottavia ominaisuuksia saavutetaan seuraavanlaisella elektronisella äänestysmenettelyllä ja mitä puutteita siitä on? Äänestäjät saavat kelpuuttajaviranomaiselta henkilökohtaisen kelpoisuusmerkin, joka sellaisenaan ei kuitenkaan yksilöi heitä. Kukin äänestäjä lähettää kerääjälle kelpoisuusmerkinsä selväkielisenä ja äänensä salattuna itse valitsemallaan symmetrisellä avaimella. Kerääjäviranomaisen julkaisee luettelon näistä salatuista äänistä. Määräajan mentyä umpeen äänestäjät lähettävät avaimensa, kerääjä purkaa salaukset ja julkaisee äännet ja tuloksen.
4. Mitä voidaan tavoitella digitaalisella vesileimauksella? Mitä ongelmia siihen liittyy?
5. * Mitä oikeastaan tapahtuu, kun nostat rahaa pankkikortilla? Kuvaile prosessi tietoturvan näkökulmasta. Tapahtuuko prosessissa jotain, jolla on merkitystä joltain muulta mutta ei tietoturvan kannalta?
6. Missä mielessä spam eli roskapostit on tietoturva-uhka? Esittele yksi keino, jolla sitä voi torjua.

7. Mihin tarvitaan CC:n (Common Criteria for Information Technology Security Evaluation) kaltaista standardia?

2. tentti 21.12.1999

1. * Millaiset voivat olla viruksen tekijän motiivit ja mitä keinoja hänellä on saada tekeleensä "tartumaan" ja toisaalta suojaan "vasta-aineilta"?
2. * Valitse ja kuvaile lyhyesti jokin tietojenkäsittelyjärjestelmä, muu kuin tehtävissä 4, 5 ja 7. Esittele viisi siinä ilmenevää todellista tietoturva-uhkaa ja kullekin jokin torjuntakeino.
3. Esittele julkisen avaimen kryptosysteemin yleistä ideaa sen verran, että voit kuvata, miten sitä käytetään muodostettaessa digitaalista kirjekuorta (jollainen on PGP:n, SET:n ja monien muiden järjestelmien käytössä). Laadi tällainen kuvaus, jonka pohjalta kurssia käymätön voi muodostaa kuoren, kunhan vain opettelee algoritmit.
4. * Miten luottokortin käyttö eroaa kaupassa ja internetissä tietoturvan näkökulmasta? Mikä on SET:n (Secure Electronic Transactions) keskeinen etu luottokorttimaksamisessa?
5. Millä tavoin yhdistelyt ja päätelyt voivat muodostaa uhan tietokantojen tapauksessa? Mainitse ainakin neljä keinoa, joilla niitä voidaan estää.
6. Miten voidaan havaita, jos jokin ison tietokoneen sadoista prosesseista onkin jollain tavalla luvaton?
7. Mikä rooli GSM-puhelimissa olevalla SIM-kortilla on tietoturvassa?

3. tentti 29.2.2000

1. Mihin ja miten käytetään yksisuuntaisia tiivistefunktioita?
2. * Suorita tietoturva-uhkien *kartoitus* (siis tasaisen kattava, alussa mainitun mittakaavan puitteissa) seuraavassa tilanteessa: tavallinen kauppaan kuuluva yksityinen lähikauppa, jossa päivittäinen toiminta sekä kirjanpito perustuvat myynnin ja varaston seurantaan tietokoneitse. Kanta-asiakkaat "tunnetaan" korttijärjestelmän avulla. Internet-yhteyskin on, mutta sitä käytetään vain sähköpostitse tehtäviin tilauksiin joiltakin toimittajilta.

Mainitse myös ainakin kaksi asiaa, jotka eivät ole uhkana tässä tapauksessa mutta ovat jossain muussa.
3. * Mikä on haaste-vaste-menetelmän idea? Onko "one-time-password" tällainen menetelmä? Miten nollatietoperiaate liittyy haaste-vaste-menetelmään?
4. Erilaisia sadan bitin mittaisia bittijonoja on runsaat 10^{30} ja melkein mikä tahansa niistä voi päätyä avaimeksi johonkin sopivaan kryptoalgoritmiin. Mainitse jokin yhteys, jossa näin tapahtuu ja kuvaile kolme erilaista elinkaarta, jonka avaimena käytettävät bitit voivat kokea tässä järjestelmässä.
5. Mainitse ainakin kolme tavallista ja konkreettista tilannetta, joissa yrityksen henkilöstö voi olla tietoturva-uhka yritykselle, tahattomasti tai tahallaan. Miten yritys voi torjua nämä uhat?

Ellei edellä vielä tullut esille, mainitse myös sellainen uhka, jonka torjuntakeino jollain tavoin heikentää työntekijän yksityisyyttä.
6. Vertaile SSH:ta ja PGP:tä viidestä näkökulmasta, joiden joukossa ovat seuraavat kolme: mihin

on tarkoitettu, millaisia alustuksia tarvitsee ennen kuin normaali käyttö voi alkaa, millä tavoin soveltaa julkisen avaimen kryptosysteemiä.

7. Minkä *tyyppisiä* seikkoja on otettava huomioon jonkin yritykselle hankittavan järjestelmän tai tuotteen tietoturvan arvioinnissa ja miten jokin Common Criterion kaltainen standardi voi auttaa arvioinnissa? (Ensimmäisen osan vastaus ei ole oikein, jos siitä muodostuu pitkä luettelo.)

4. tentti 3.4.2000

1. Biologiset virukset tulevat tietoisuuteen vasta sairauden puhjettua. Miten tarttuneen tai tarttumaisillaan olevan tietokoneviruksen voi löytää ja nitistää ennen kuin se tekee pahojaan?
2. Mitä tarkoitetaan sillä, ettei saa lukea ylhäältäpäin eikä kirjoittaa alaspäin ja missä yhteydessä tällaisiin sääntöihin pitää turvautua?
3. * Esittele sellaisia olion autentikoimismenetelmiä (ainakin kolmea erilaista), jotka perustuvat johonkin, mitä olion tietää. Määrittele ensin, mitä olion autentikointi tarkoittaa.
4. * Selitä käsitteet julkisen avaimen infrastruktuuri ja julkisen avaimen varmenne sekä niiden yhteys toisiinsa. Voiko jompikumpi olla olemassa ilman toista? Liittyykö käsite key escrow jotenkin näihin? (Kyllää tai eitä tärkeämpiä ovat perustelut.)
5. Mitä tietoja www:tä selaava henkilö "vuotaa" seittiin (palvelimelle tai matkan varrelle)? Mitä haittaa tästä voi olla hänelle ja mitä hyötyä jollekulle muulle?
6. Virusten ja muiden pahoissa aikeissa tehtyjen ohjelmien lisäksi tietojenkäsittelyn turvallisuuden uhkana ovat monenlaiset puutteet ja virheet ohjelmissa, käyttöjärjestelmästä alkaen. Mitä voidaan tehdä, jotta ohjelmat olisivat tässä suhteessa sellaisia kuin pitääkin? (Nyt ei siis pidä käsitellä viruksia yms.) Jäsennä vastauksesi ohjelman elinkaaren kannalta ainakin kolmeen osaan ja mainitse yhteensä ainakin kuusi tärkeää asiaa.
7. Minkälaista tietoturvaa IPsec:n AH- ja ESP-protokollat tuovat Internet-protokollan liikuttelemille paketeille? Mitä (IPsec:n puitteissa) pitää tapahtua ennen näiden protokollien käynnistymistä?

8306000 Tietoturvallisuuden perusteet

Arvosanojen jakaumat syksyn 1999 kurssin neljässä tentissä

	19.10.1999	21.12.1999	29.2.2000	3.4.2000
arvosana				
0	20	11	6	4
1	19	12	7	5
2	42	13	5	4
3	52	18	10	10
4	41	9	8	4
5	2	2	4	2

yht.	175	65	40	29
läpi	155	54	34	25
	89%	83%	85%	86%

Tentti 13.8.2001

Vastaa viiteen tehtävään, ja tehtävissä 2 ja 3 a-kohdan lisäksi vain joko b- tai c-kohtaan.

Kun olet saanut vastaukset valmiiksi, merkitse vastauspaperin alkuun tehtävien numerot siinä järjestyksessä kuin arvioit osanneesi niihin vastata, paras ensimmäiseksi, huonoin viimeiseksi. Jos arvostelu tuottaa saman järjestyksen, saat lisäpisteen.

1. Jos kaikki tietoturvatilat pitäisi luokitella, mitä muuta pitäisi ottaa huomioon kuin ne asiat, jotka esiintyvät Howardin taksonomiassa? Siinähan esitellään taulukkomuodossa toisensa poissulkevat luonnehdinnat hyökkääjälle, hänen käyttämälleen välineelle, keinolle päästä käsiksi tietoon, tulokselle jonka hän saa aikaan suhteessa tietoon sekä tavoitteelle, joka hänet motivoi.
2. Sovelletaan hash-funktiota h tuhat kertaa peräkkäin satunnaislukuun r ja kerrotaan tulos turvallisesti palvelimelle.
 - a) Miten tästä saadaan autentikointimenetelmä ja miksi se on turvallinen?
 - b) Miten menettelyä voi (alustuksen jälkeen) nopeuttaa, jos autentikointi tapahtuu myös sellaiselta asiakaslaitteelta, jossa h :ta ei voi laskea kovin nopeasti?
 - c) Missä suhteessa a-kohtaa heikompi on OPIE-menettely, jossa r kerrotaan palvelimelle?
3. Rabinin kryptosysteemissä on julkinen avain n ja yksityiset avaimet p ja q . (p ja q ovat suuria alkulukuja, joiden jakojäännös modulo 4 on 3; $n=pq$.)
 - a) Miten salataan viesti m , joka halutaan lähettää n :n omistajalle ja miten tämä saa sen auki? (Avaamisen tarkkoja kaavoja ei vaadita mutta sellainen tarkkuus kylläkin että syy redundanssin käyttötärpeelle selviää.)
 - b) Jos avain n eli moduuli on 500-bittinen ja viesti m on 100-bittinen, mitä m :lle pitää tehdä ennen salauksen soveltamista ja miksi?
 - c) Jos viesti onkin sitten 100 000-bittinen, se pitäisi käsitellä 200 lohkona. Miksei näin kuitenkin yleensä tehdä ja mikä on tavallisempi menettely (kuten RSA:ssakin)?
4. Etsi esimerkki tietokannasta, jossa yhtäältä joudutaan vastaamaan kyselijälle mutta toisaalta joudutaan pimentämään jotain samalta henkilöltä. Mainitse kolme mekanismia, joilla pimitystä voidaan toteuttaa.
5. Missä mielessä toimikortilla oleva prosessori on turvallinen? Millä valmistusvaiheen menettelyillä turvallisuus saavutetaan?
6. Esittele viisi menettelyä, joilla yritys voi torjua työntekijöidensä tahallisesti aiheuttamia tietoturvarikkomuksia.
7. Yhden pisteen kysymyksiä, eli vastaa/selitä juuri sen verran, että lukija vakuuttuu että tiedät mistä on kyse:
 - Makrovirus
 - Tietosuoja
 - Digitaalinen allekirjoitus
 - Common Criteria (CCITSE)

- Kertakirjautuminen
- Digitaalinen vesileima

Tentti 5.3.2001

Vastaa viiteen tehtävään.

Kun olet saanut vastaukset valmiiksi, merkitse vastauspaperin alkuun tehtävien numerot siinä järjestyksessä kuin arvioit osanneesi niihin vastata, paras ensimmäiseksi, huonoin viimeiseksi. Jos arvostelu tuottaa saman järjestyksen, saat lisäpisteen.

1. a) Mitä ovat seittiselauksen evästeet (eli cookiet eli piparit)? (1p)
b) Miksei niiden kautta voi tapahtua hyökkäystä koneesi eheyttä vastaan? (1p)
c) Millä tavoin ne voivat aiheuttaa ongelmia yksityisyytesi kannalta? (2p)
d) Millä tavoin seittiseläus yleisesti heikentää yksityisyyttäsi, evästeistä riippumatta? (2p)
 2. Ensimmäisellä luentokerralla esiteltiin lyhyesti seuraavat 22 informaatiollista tietoturvamekanismia:
 - salakirjoitus -- tarkistussumma (yleisemmin: tiivistefunktio) -- allekirjoitus -- nimettömyys (anonymiteetti) -- tunnistus (identification) -- olion autentikointi -- pääsynvalvonta -- erottelumekanismit -- auditointi -- oikeutus, auktorisointi -- omistusoikeus -- valtuutus, delegointi -- validointi, kelpuutus -- varmentaminen (certification) -- aikaleimaus -- todistaminen (witnessing) -- kuittaus -- konfirmointi -- kiistämättömyys -- peruutus (revocation) -- tietoliikennemekanismit -- toipumismekanismit
- Valitse näistä kolme sellaista, joilla ei ole mitään tekemistä virustorjunnassa. Selitä miksi ei ja mihin ne sitten liittyvät.
3. Oletetaan, että A ja B ovat sopineet symmetrisestä avaintensalausavaimesta K, jota he käyttävät päivittäin vaihdettavien datansalausavainten salaukseen seuraavien kahden vuoden ajan. Mitä avaintenhallintaan liittyviä tapahtumia voidaan niiden bittien elinkaarissa erotella, joista K muodostuu?
 4. Jos jätetään jälkikäteen ohjelmiin tartutetut virukset huomiotta, mitä toimia ohjelman oikean toiminnan takaamiseksi voivat suorittaa ohjelmien tekijät, hankkijat ja ajajat?
 5. Esittele kolme erilaista tapaa, joilla henkilö A voi vakuuttaa etäällä olevan henkilön B siitä, että K on A:n julkinen avain. Ainakin yhden tavan pitää toimia ilman kolmatta osapuolta ja ainakin yhdessä sellainen pitää olla.
 6. Yhden pisteen kysymyksiä, eli vastaa/selitä juuri sen verran, että lukija vakuuttuu että tiedät mistä on kyse:
 - Hash-funktio.
 - Riskianalyysi.
 - Päätely tietoturvaongelmana tietokannoissa.

- Tehtävässä 4 ei ole tarpeen esitellä Common Criteriaa eli CC:tä, mutta CC:n noudattamisesta voi silti olla hyötyä tehtävässä mainituille kolmelle toimijaryhmälle. Mikä niistä joutuu eniten CC:n kanssa tekemisiin? (Pelkkä arvaus ei riitä.)
- Tunnelointi.
- SSL, Secure Socket Layer.

TTKK / Tietoliikenne / J.Koskinen

8306000 Tietoturvallisuuden perusteet

Tentti 22.1.2001

Vastaa viiteen tehtävään.

1. Sovittele virustorjunnan eri vaiheita ja menetelmiä seuraaviin luokkiin. Enintään yksi luokka saa jäädä tyhjäksi.
 - Välttäminen (avoidance) *ei vaihtoa / Escrow*
 - Pelottaminen (deterrence) *mainitsee*
 - Estäminen (prevention) *firewall*
 - Havaitseminen (detection) *skannaus*
 - Toipuminen (recovery) *varmuuskopiat → palautus*
 - Korjaaminen (correction) *tyhjään varuustilaan*
2. Mikä erottaa tietoturvamallin (jollainen esim. Bell-LaPadula on) ja tietoturvapoliitikan? Mitä yhteistä niillä voi olla? Miten tietoturvasuunnitelma sitten liittyy näihin?
3. Mainitse kolme turvallisuusongelmaa, jotka liittyvät salasanapohjaiseen autentikointiin. Minkä ongelman ratkaisuyritys on seuraavanlainen? Autentikoituja lähettää todentajalle tiedot: id, r, t, h(id, r, t, pw), missä id=käyttäjätunnus, r=satunnaisluku, t=aika, h=hash-funktio, pw=salasana.
4. Oletetaan, että saat A:lta salatun PGP-viestin, jonka hän on myös allekirjoittanut. Mistä PGP-ohjelmasi saa avaimet salauksen purkuun ja allekirjoituksen todennukseen? Kumpaa se tarvitsee ensin (eli kumpi operaatio on ulompana)? Millä perusteilla sinä voit luottaa, että juuri A on allekirjoittanut viestin?
5. Millä tavoin palomuurilla edistetään tietoturvaa: toisin sanoen, mitä sillä konkreettisesti tehdään ja miten se vaikuttaa?
6. Yhden pisteen kysymyksiä, eli vastaa/selitä juuri sen verran, että lukija vakuuttuu että tiedät mistä on kyse:
 - Salakirjoituksen kerta-avain-systeemi (one-time pad)
 - Troijan hevonen (nykyaikainen)
 - SET, Secure Electronic Transactions
 - PICS, Platform for Internet Content Selection
 - Julkisen avaimen systeemeissä lasketaan kokonaisluvulla, mutta miksi tämä tehdään modulo jokin iso kokonaisluku, eli ottamalla aina jakojäännös tämän luvun suhteen?

- Lähätät kaverillesi jonkin dokumentin levykkeellä, mutta olet aiemmin käyttänyt levykettä myös yksityisiksi tarkoitamiesi tiedostojen käsittelyssä. Miksei näiden tiedostojen tuhoaminen, deletointi, riitä luottamuksellisuuden säilyttämiseen?

TTKK / Tietoliikenne / J.Koskinen

8306000 Tietoturvallisuuden perusteet

Tentti 4.12.2000

Vastaa viiteen tehtävään.

1. Mitä samanlaista ja mitä eroa on (symmetrisessä) lohkosalauksessa ja yksisuuntaisessa tiivistämisessä (eli kryptograafisessa hash-funktiossa)? Käsittele kysymystä (a) näiden operaatioiden tavoitteiden ja (b) algoritmien tyypillisen tekniikan kannalta.
2. Kahden osapuolen yhteistä salaisuutta voidaan käyttää molemmin- tai toispuoliseen autentikointiin monin eri tavoin. Mikä on heikoin tuntemasi tapa (joka on käytössä) ja mikä vahvin? Esittele myös jokin kolmas tapa näiden väliltä. (Voit rajoittaa toispuoliseen autentikointiin, mutta mainitse aina kumpi osapuoli autentikoidaan kummalle.)
3. Millä tavoin VRK:n laatima allekirjoitus saa aikaan sen, että muut osapuolet voivat luottaa sinun HST-korttisi prosessorin sinun puolestasi laskemaan allekirjoitukseen ikäänkuin sinä olisit sen omin käsin tehnyt?
4. Missä suhteessa tietokannan eheyttä voidaan ylläpitää samoilla mekanismeilla kuin yleensä tiedostojärjestelmän eheyttä? Missä suhteessa tietokanta vaatii erityisjärjestelyjä? Mainitse kaksi sellaista.
5. Britanniassa on lokakuussa astunut voimaan laki, jonka mukaan viranomaisilla on tietyissä tilanteissa oikeus vaatia tietojärjestelmästä vastuussa olevaa purkamaan kyseisessä järjestelmässä olevan tai sieltä tietoverkkoon lähetetyn tiedon salaus. Viranomainen on jo alunperin saanut ja tallettanut kopion lähetetyistä viesteistä.
 - a) Mitä eroa ja mitä yhtäläisyyttä tällä ja key escrow'lla on? Kyseiseen lakiin on tulossa myös lisäys, joka kieltää purkuvaatimuksen saanutta verkon tms. ylläpitäjää kertomasta asiasta kenellekään muulle kuin asianajajalleen. Erityisesti hän ei siis saa varoittaa salausta käyttävää asiakastaan siitä, että tämän mahdollisesti valonarat viestit tullaan avaamaan. Tämän kiertämiseksi on kehitelty seuraava keino: ylläpitäjä merkitsee viranomaisille paljastettavan avaimen käyttöänsä päättyneeksi ja kun asiakas tietenkin kysyy, miksei avain enää kelpaa, ylläpitäjä vastaa, ettei hänellä ole lupa kertoa.
 - b) Selitä, millä tavoin tuo "kiertotie" on esimerkki piilokanavasta (covert channel).
6. Yhden pisteen kysymyksiä, eli vastaa/selitä juuri sen verran, että lukija vakuuttuu että tiedät mistä on kyse:
 - a) Sama fyysinen viruskoodi voi tehdä tihutyötä useita kertoja. Jos tällaista virusta ei kertahaitan vähäisyyden ansiosta huomata moneen viikkoon, toipumisesta voi tulla erityisen hankalaa. Miksi?
 - b) Kryptograafisesti vahva satunnaisluku

- c) Kertakirjautuminen (single sign-on)
- d) Tietosuojat
- e) Tietoturvaluokitus
- f) VPN (virtual private network)

nämä uhkat torjutaan GSM-järjestelmässä? (Vähintään kolme uhka-torjunta -paria.)

5. Miten olion autentikointi voidaan kytkeä johonkin sellaiseen, mitä olio tietää mutta kukaan muu ei tiedä: Miten tuohon tiedettyyn kytketään olion henkilöllisyys ja miten todentaja voi vakuuttaa, että joku autentikoitumista yrittävä todella tietää sen, mitä pitääkin?

TTKK / Tietoliikenne / J.Koskinen

8306000 Tietoturvallisuuden perusteet

Tentti 30.10.2000

Pidä huoli, että tulet vastanneeksi kaikkiin kysymysten kohtiin ja osiin. Vain kahteen viimeiseen tehtävään kannattaa vastata pitemmin kuin lyhyesti. Viimeiseen ei kannata vastata ilman etukäteistä jäsentämistä.

1. RSA-kryptosysteemissä on julkiset avaimet n (moduuli) ja e (eksponentti) sekä niitä vastaava yksityinen avain d .
 - (a) Jos RSA-avain on 1024-bittinen, niin mikä näistä kolmesta silloin on sen mittainen?
 - (b) Näytä, miten n , e ja d toimivat salauksessa ja miten allekirjoituksessa (ja tietenkin myös mitä vastaanottaja tekee). Matemaattisia todistuksia ei tarvita.
 - (c) RSA-avain luodaan mm. HST-kortin prosessorin sisällä. Tupakan työ pikku prosessorilla on suurten alkulukujen löytämisessä. Se tapahtuu testaamalla, onko satunnaisesti keksitty luku alkuluku. Pitääkö jonkin luvuista n , e tai d olla suuri alkuluku, vai mihin alkulukuja tarvitaan?
2. Common Criteria-standardissa vakuuttavuuteen vaikuttavat tekijät on jaoteltu seitsemään luokkaan, kukin niistä useisiin ryhmiin ja ryhmät puolestaan komponenteiksi. Valituista komponenteista on pantu kokoon seitsemän erilaista evaluoinnin vakuuttavuustasoa EAL 1 - EAL 7 (evaluation assurance levels).
 - (a) Selitä ensin yleisesti, mitä vakuuttavuus tässä oikeastaan tarkoittaa?
 - (b) Millaisia ne vakuuttavuuteen vaikuttavat tekijät sitten ovat? Mainitsitpa sitten komponentteja, ryhmiä tai luokkia, ainakin kolmeen luokkaan kuuluvia asioita pitäisi tulla esille, pienen selityksen kera.
 - (c) Kuten a- ja b-kohdan vastauksistasi varmaan käy ilmi, vaativakaan EAL-paketti ei sellaisenaan riitä tietoturvan kriteeriksi. Mitä muita palasia standardi tarjoaa tietoturvan arvioimiseksi?
 - (d) Mitä tekemistä vakuuttavuudella tai yleensä arvioidulla tietoturvalla voisi olla vakuutettavuuden kanssa (siis sen kanssa mitä vakuutusyhtiöt tarjoavat)?
3. (a) Millaisilta vierailta, siis muualta tulevilta, biteiltä ihmisistä tai hänen tietojenkäsittelyjärjestelmäänsä pitää suojella? Mainitse ainakin kolme erityyppistä asiaa.
 - (b) Koska a-kohdan mukaisessa suojaamisessa perille pääsevien bittien määrää pitää vähentää, näyttäisi siltä, että saatavuus (availability) voi vain heikentyä suojauksen seurauksena. Miksei asia ole näin yksioikoinen?
 - (c) Miksei tietosuojalla ole mitään tekemistä a-kohdan kanssa, samankaltaisesta nimestään huolimatta?
4. Mitä uudenlaisia tietoturvaohjelmia matkapuhelimissa on lankapuhelimeen verrattuna? Miten