

TLT-3201 Tietoturvallisuuden jatkokurssi**Tentti II 19. 1. 2009**

Merkitse vastauspaperiin nimesi viereen sitova valinta, oletko tekemässä A- vai AB-tenttiä. Sen mukaan määräytyy, kumpi versio tehtävästä 1 vaaditaan. Muissa tehtävissä on [B]:llä merkittyjä kohtia, jotka edellytetään vain AB:n tenttijöiltä. Niissä on mainittu myös maksimipistemäärä. Se vähentää AB-tentissä saman tehtävän muiden kohtien osuutta 6 pisteestä, joka on kaikissa tehtävissä maksimipistemäärä. Kyseisten muiden kohtien vaativuus pysyy silti samana kuin se on pelkässä A-tentissä.

~~1.~~ [A] Millaisissa tapauksissa tarvitaan politiikka, jonka antaa joillekin kyselijöille joihinkin tietokantakyselyihin vastauksen mutta samoille kyselijöille joihinkin toisiin näennäisesti samaakin asiaa koskeviin kysymyksiin ei? Millä mekanismeilla tällaista politiikkaa voidaan toteuttaa?

1. [B] Millaisissa tapauksissa tarvitaan politiikka, jonka antaa joillekin kyselijöille joihinkin tietokantakyselyihin vastauksen mutta toisille kyselijöille samoihin kysymyksiin ei? Millä mekanismeilla tällaista politiikkaa voidaan toteuttaa? Kysymys näyttää melko samalta kuin 1[A], mutta tässä tehtävässä pitää tarkastella sellaista tietokantaa, jossa on eri tasoille **turvaluokiteltuja** tietoja.

~~2.~~ Kun poliisille jätetään passihakemus, pitää mukana olla passikuva, jolle on asetettu lukuisia laatuvaatimuksia. Osa niistä liittyy tunnistettavuuteen ja osa tekniikkaan, jolla kuva siirretään passiin visuaaliseksi ja digitaalseksi kopioksi. Joskus asiakkaan kuva ei kelpaa, vaan hän joutuu hankkimaan uuden. Paperikuva skannataan hakemuksen käsittelyn alkuvaiheessa ja asiakkaan läsnä olleessa voidaan tehdä minimaalisia korjailuja kuten siirtoa tai skaalausta. Digikuvien aikakaudella tuntuu oudolta, että alun perin digitaalinen erittäin tarkka kuva ensin tulostetaan pieneksi paperinpalaksi (36x47 mm) ja sitten uudelleen digitoidaan (A4-skannerilla). Tämän vaiheen ohittaminen on periaatteessa helppoa, mutta siinä on monenlaisia haasteita. **Tarkastele digitaalisen passikuvan suoran toimittamisen tietoturva-asteita ja esitä niille ratkaisuja.** Käsittele mahdollisuutta, että asiakas toimittaa kuvaamosta saamansa tai itse tuottamansa kuvan poliisin tietojärjestelmään sähköpostitse, web-lomakkeen tms. kautta tai muistivälillä paikallaan päällä sekä sitä, että kuvaamo toimittaa kuvan verkkoitse. Jossain vaiheessa asiakkaan täytyy käydä tunnistautumas- ja olemassa kuvansa näköinen. Nykykäytännössä tämä tapahtuu hakemuksen jättövaiheessa, jolloin myös maksu suoritetaan. Ratkaisuisasi voit ottaa muita vaihtoehtoja huomioon.

3. (i) Selvitä digitaalisen allekirjoituksen **turvaominaisuuksia ja käyttökelpoisuutta** suhteessa pankkitunnusten käyttöön. Huomaa, että digitaalista allekirjoitusta voidaan käyttää myös tunnistamiseen (toisin kuin tavanomaista) ja pankkitunnuksia käytetään sähköisessä asioinnissa sellaisiin tarkoituksiin, joissa perinteisesti on käytetty allekirjoitusta.

(ii) [B, 2p] Selitä digitaalisen allekirjoituksen käyttö luottamuksen hallinnan yhteydessä ja ota huomioon myös muunlaiset kuin henkilöihin liittyvät allekirjoitukset.

~~4.~~ (i) Esittele vähintään neljä sellaista fyysistä turvamekanismia, joita kannattaa käyttää korkeaa turvallisuutta vaativien laitteiden suojaamiseen, mutta jotka eivät yleensä ole perusteltuja esim. TLT-laitoksen konehuoneen kaltaisissa tiloissa.

(iii) [B, 2p] Mikä on PUF, Physical Unclonable Function?

5. Tässä ovat tutkielmakysymykset. Tarkoitus on, että jokainen saa valita seitsemästä muuta kuin omaa työtä koskevasta kysymyksestä **kuusi**, joihin vastaa. Tätä varten muistuta ensin lukijaa, mikä olikaan tutkielmasi aihe. Jos sitä koskeva kysymys ei ole kysymysten (1) – (7) joukossa, valitse niistä kuusi ja vastaa niihin. Muussa tapauksessa valitse kysymyksistä (1) – (8) kuusi muuta kuin omasi ja vastaa niihin.

~~1.~~ Kerro FairPlayn toiminnan pääpiirteet.

~~2.~~ Selitä lyhyesti, minkälaisia käytännön toimenpiteitä yrityksissä voidaan kriisitilanteissa jatkuvuussuunnitelman mukaan tehdä.

~~3.~~ Kerro kaksi tapaa poistaa tietoa kiintolevyiltä tai flash-muistilta. *yläkini demaqrtaanti*

(4) Mihin kaikkeen erilaisia kryptoalgoritmeja tarvitaan salasanantallennusjärjestelmässä?

~~5.~~ Määrittele lyhyesti termi "vakoiluohjelma".

~~6.~~ Miten voidaan parantaa "RESTful"-web-palvelun saatavuutta käyttämällä kryptografista pääsynhallintaa haaste-vaste -autentikoinnin sijaan?

~~7.~~ Mihin luokkiin visuaaliset salasanat voidaan jakaa? *tunnistaa muistinvon maistra vastaviih*

~~8.~~ Kotikäyttäjän tietoturvatiedon tarpeet: Mitä tietoa kotikäyttäjä tarvitsee?