

# Harjoitustehtäväkierros 2: Tietoturva ja kuljetuskerros

T-110.2100 kurssihenkilökunta

deadline Tiistai 30.3.2010 18:00

## Johdanto

Tällä tehtäväkierroksella pääset pohtimaan tietoturvan perusasioita, lukemaan ihka oikean tieteellisen artikkelin ja vertailemaan kuljetuskerroksen protokollia.

Ensimmäisessä tehtävässä pohditaan SSL/TLS-salausta, koska sen merkitys tuntuu kasvavan nykyinternetissä huomattavasti.

Toisessa tehtävässä pääset pohtimaan sirukortilla maksamista ja sen kustannus- ja turvadynamiikkaa, koska asia on mielestämme mielenkiintoinen.

Kolmannessa pääset syventämään ymmärrystäsi kuljetuskerroksesta. Kuljetuskerrokseen palataan seuraavalla tehtäväkierroksella enemmän.

Tehtävä palautetaan Rubyc-järjestelmään kurssin Noppa-sivuilta löytyvien ohjeiden mukaisesti. *Kiinnitä huomiota palautuksen formatointiohjeisiin. Väärästä tiedostoformaatista tai merkistöstä sakotetaan pisteitä!*

## 1 SSL (7p)

Tarkastele upouuden Aalto-yliopiston yhtenäisen Oodin sertifikaatti.

- A Mistä mihin se on voimassa? Voitko päätellä koska sertifikaatti on luotu? (1p)
- B Kuka sertifikaatin on allekirjoittanut? (1p)
- C Mistä Firefoxista (tai muusta selaimesta) löydät listan allekirjoittajista, joiden allekirjoittamiin sertifikaatteihin selain automaattisesti luottaa?<sup>1</sup> (1p)

---

<sup>1</sup>Safari käyttää ainakin OS X:ssä käyttöjärjestelmän listaa, joten siitä itsestään ei kannata etsiä listaa.

- D Mistä selaimesi käyttämä salainen ja julkinen avain ovat peräisin? Tunnistaako Oodi sinut sinuksi kahdella peräkkäisellä käynnillä? (Oletus: suljet selaimen ja odotat päivän välissä). (2p)
- E Voisivatko ne olla jollain toisella tavalla luotuja? (vinkki: kannattaa selvittää mikä on X.509). Tunnistaisiko Oodi sinut silloin peräkkäisillä kerroilla? Tarvittaisiinko erillistä salasanakirjautumista? (2p)

## 2 Sisälukutaito (7p)

Lue Chip + PIN is broken

<http://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf>

sekä Luottokunnan ohjeita sirukortin käytöstä kuluttajille

[http://www.luottokunta.fi/fi/ohjeita\\_kortinhaltijoille/sirukortin\\_kaytto/](http://www.luottokunta.fi/fi/ohjeita_kortinhaltijoille/sirukortin_kaytto/)

- A Onko Murdochin ja kumppaneiden löydös sinulle kuluttajana hyvä vai huono asia? (1p)
- B Lukemasi artikkelin perusteella, onko todennäköistä että esitetty hyökkäysmekanismi saadaan estettyä. Mitä perusteluita löydät artikkelista mielipiteellesi? (4p)
- C Kauppiassetäsi kysyy sinulta (kun kerran olet koulujakäyvä tulevaisuudenlupaus ja oikeat konsultit ovat kalliita) pitäisikö hänen kaupassaan huolestua tai huomioida Murdochin ja kumppaneiden osoittamasta haavoittuvuudesta. Vastaa perustellen pitäisikö. (2p)

## 3 Kuljetuskerros (6p)

- TCP-yhteys tunnistetaan lähde- ja kohdekoneen osoitteiden ja sovelukset identifioivien porttien avulla. Voitaasiinko jokin näistä poistaa? Miksi? (2p)
- Haluat toteuttaa kellojen synkronointiprotokollan. Toteutatko protokollan TCP:llä vai UDP:lla? Miksi? (3p) <sup>2</sup>
- TCP-yhteys on mahdollista katkaista vain puoliksi. Arvioi miksi tällainen mahdollisuus on protokollassa? (1p)

---

<sup>2</sup>Vinkki: kannattaa vilkaista NTP:n toteutusta

## Materiaalia

- <https://noppa.tkk.fi/noppa/kurssi/t-210.1100/etusivu> Kurssin kotisivut
- <http://www.cse.tkk.fi/Tietoliikenne/Opinnot/Ohjeet/> T-110 -kurssien yleisiä ohjeita
- <http://opetuki2.tkk.fi/p/top/> Teekkarin ohjauspakki
- Internetin hakupalvelut (jos et löydä, googlaa)