Ti5313500 Tietoturvan perusteet
LTY / TITE
Olli Hämäläinen

Tentti 14.12.2005

1. Selitä lyhyesti (max 3 riviä) (6p)

a) troijalainen
b) bruteforce hyökkäys
c) reverse engineering
d) kryptoanalyysi
e) DoS (Denial of Service)
f) IDS

2. Tiedon salaaminen (9p)
Esittele symmetrisen ja asymmetrisen salauksen toiminta. Mitkä ovat niiden vahvuudet ja heikkoudet?

3. Autentikointi (9p)
Henkilön autentikointi voi perustua siihen mitä hän on, johonkin mitä hän tietää tai mitä hän omistaa. Kerro esimerkkien avulla mitä hyviä ja huonoja puolia eri malleissa on ja missä tilanteissa niitä voidaan käyttää.

4. Ihmiset ja tietoturva (6p)
a) mitä on social engineering ja kuinka siltä voidaan suojautua?
b) miten henkilöstöturvallisuudella voidaan pienentää tietoturvariskejä?

Bonustehtävä (max 3p)
kerro
a) kuinka RFID tekniikkaa voidaan käyttää tunnistautumiseen?
b) minkälaisen juridisen ongelman MD5-algoritmin heikkous muodosti esimerkkitapauksessa?
c) miten EMV standardin mukaiset pankkikortit lisäävät turvallisuutta?

EI LASKINTA
EI MATERIAALIA