T-110.4200 Tietoturvallisuustekniikka
Tentti 29.10.2009

1 **Selitä** lyhyesti seuraavat tietoturvallisuuteen liittyvät käsitteet. (6 p)
   a) Intrusion Detection System
   b) Malware (haittaohjelma)
   c) Whitelist filter
   d) Authorization
   e) Eheys
   f) Reference monitor

2 **Perustele** lyhyesti mitkä seuraavista väitteistä pitävät paikkansa ja mitkä eivät. (6 p)
   a) Lomakkeeseen liitetty syötteen tarkistava Javascript-funktio on hyvä keino siirtää tietoturvaan liittyvää laskentaa pois palvelimelta.
   b) Yrityksen kannattaa tallettaa itselleen kopiot tärkeistä salausavaimista.
   c) Replay-hyökkäys estetään salaamalla kunkin viestin sisältö
   d) Palomuurin asennus alkaa lukemalla organisaation tietoturvapolitiikka
   e) Kun on aihetta epäillä tietomurtoa, tärkeintä on irrottaa yrityksen verkko Internetistä.
   f) TLS:ää tai IPseciä ei tarvita käytettäessä Internetiä matkaviestimellä, koska mobiili tietoliikenne on jo salattua.

3 a) Palomuurit voivat toimia TCP/IP-mallin tasolla 3-4 (pakettisuodattimet) tai tasolla 5 (eli 7, sovellussuodattavat). Mainitse kaksi **esimerkkiä** siitä, mihin verkkoon sijoitettu sovellussuodattava palomuuri pystyy, mutta pakettisuodattava ei. (1,5 p)
   b) Palomuuri voi myös olla sovellus työasemassa, **perustele** miksi työasemaan kannattaa asentaa palomuuriohjelmisto, jos organisaatiolla on jo verkkopalomuuri. (1,5 p)
   c) Olet vastuussa ohjelmistoprojektista, jossa kokeneet **intranet**-ohjelmoijat toteuttavat ensimmäistä kertaa **Internet**-sovellusta. Pelkäät ohjelmoijien jättävän ohjelmistoon haavoittuvuuksia, kuvaile lyhyesti kaksi ohjelmistotuotannon käytäntöä ja yksi aiheeseen liittyvä standardi joilla yrität estää haavoittuvuuksien syntymistä. (3 p)

4 Tiedon salaus ja suojaus (6 p)
   a) Mitä salausavaimia tarvitaan salatun ja allekirjoitetun sähköpostiviestin lähettämiseen, kun oletetaan käytännön tilanne ja viesti on kooltaan suuri? Kuvaile kunkin salausavaimen käyttö ja mistä ko. avain saadaan. (3 p)
   b) TLS-kättelyn aluksi asiakas lähettää salausalgoritminsa ja noncen; palvelin vastaa omillaalgoritmeillaan, noncellaan ja varmenteellaan ja niin edelleen. Miksi kättely tarvitaan ja mikä on kättelyn tulos? (3 p)

5 Kurssilla on esitelty erilaisia tietoturvan teoreettisempia malleja, kuten yksinkertainen Bell-LaPadula, Bell-LaPadulan hilaversio, staattinen Biba, subject low watermark Biba, object low watermark Biba, Chinese Wall ja Clark-Wilson. **Kerro ja perustele** mikä malli sopisi parhaiten kuhunkin seuraavista tapauksista. Kerro myös oletukset, joille perustat perustelusi. (6 p)
   a) Cern on suuria ja kalliita tutkimuksia tekevä kansainvälinen tutkimusinstituutti, joka tuottaa suuria määriä alkuperäistä **mittausdataa**, jota ei siirretä Cernistä, vaan tutkijat pääsevät ajamaan omia ohjelmiaan Cernin tietokoneissa.
   b) Pankkitilisi saldo on oikeasti **numero tietokannassa**. Kun maksat maksun pankin kautta, sinä tai pankin työntekijä muutatte järjestelmän kautta sinun tilisi ja jonkin toisen tilin tietokentän arvoa.
   c) Poliisilla on oikeus poimia salakuunteluraportti tietojärjestelmästä, jos hän on riittävän korkea-arvoinen ja hän on mukana kyseisen rikoksen tutkinnassa.
   d) Nuori **motoristi** saattaa liittyä mihin tahansa moottoripyöräjengiin, mutta liityttyään hän ei voi vaihtaa jäsenyyttään toiseen jengiin, mm. koska hän tietää jengin salaisen tervehdyksen.

T-110.4206 Information Security Technology
Exam 29.10.2009

1 **Explain** briefly the following concepts and acronyms related to data security. (6 p)
- a) Intrusion Detection System
- b) Malware
- c) Whitelist filter
- d) Authorization
- e) Integrity
- f) Reference monitor

2 **Justify** briefly the following statements as either correct or false. (6 p)
- a) Including a Javascript function in a form to verify the input is a good way to move security related computation off the server.
- b) A company should store copies of important encryption keys.
- c) A replay attack can be prevented by encrypting the contents of each message.
- d) Installing a firewall starts by reading the organization's security policy.
- e) When an intrusion is suspected, the most important thing is to disconnect the company network from the Internet.
- f) TLS or IPsec are not needed when using the Internet from a mobile telephone, as mobile communications are already encrypted.

3 a) Firewalls can operate on the layers 3-4 of the TCP/IP model (packet filtering firewalls) or on layer 5 (or 7, application filter). Give two **examples** of what an application layer firewall can do that a packet filter can not do. (1.5 p)
- b) A firewall can also be an application in a workstation. Give two **justifications** for why a workstation should have a software firewall if there already is a network firewall. (1.5 p)
- c) You have been put in charge of a software project, where experienced **intranet** programmers are implementing an **Internet** application for the first time. You are afraid that the programmers will leave vulnerabilities to the code. Briefly describe two software production practices and one relevant standard that you will use to prevent the vulnerabilities. (3 p)

4 Protecting information (6 p)
- a) What encryption keys are needed to send an encrypted and signed e-mail message, in a practical situation and with largish message content? Describe how each key is used and where the key is obtained from. (3 p)
- b) A TLS handshake starts by the client presenting its cipher algorithms and a nonce; the server replies by its algorithms, nonce and certificate; and so on. Why is a handshake needed and what is the result of the handshake? (3 p)

5 Several theoretical data security models have been presented during the course, like simple Bell-LaPadula, Bell-LaPadula with lattice, static Biba, subject low watermark Biba, object low watermark Biba, Chinese Wall and Clark-Wilson. **Describe and justify** which model would be best suited to apply in each following case. Include the assumptions on which you base your justification. (6 p)
- a) Cern is an international research institution doing big and expensive experiments, resulting in huge amounts of original measurement **data** that not transferred from Cern, but scientist can run their software at the Cern computers.
- b) The balance of your bank account is just a number in a database. When you pay a bill through the bank, you or a bank employee use the system to change the value of a field belonging to your and recipient's account.
- c) A police officer may read a telephone eavesdropping report from the database if she is senior enough and if she is participating in the investigation of that particular crime.
- d) A young **motorist** may join any motorbike gang, however after joining up, he may not change his membership to another gang, as he knows the secret handshake.

Ohje tarkastajalle, guide for graders, not complete answers

1

a) tunnistaa hyökkäyksen (verkosta, koneista)
b) virukset yms. pahaa tekevät
c) suodatuslista sallituista asioista/merkeistä/paketeista tms.
d) valtuutus, mitä subjekti saa tehdä objektille
e) tieto ei muutu matkalla/talletettaessa, myös tietovarastoon ei tule väärää tietoa
f) pääsynhallintaoikeuksista päättävä osa

2

a) no, user might change/remove the function; moving security checks to software that we are not executing is not the smartest thing
b) right, e.g. for recovering encrypted backups if the original data and key is lost
c) the point of replay is that the recipient will decrypt and act on the message
d) right, a firewall is the technical implementation of the policy (at least in theory)
e) either way, disconnect: stop harm spreading, prevent destruction of stuff, no disconnect: keep intruder unaware, observe and monitor and get more info
f) false, mobile crypto is only handset to base station

3

a) in the net: virus and other content filtering, detecting protocols masquerading as others, protection from some attacks... Note, the English translation did not specify fw being in the net, adjust for students thinking about a firewall application
b) Depth of defense, internal threats, possible configuration mistakes in the main fw.
c) Design principles from the slides, testing (automated), code walkthroughs, layered, compartmentalized design etc. for standards, those that apply, SSE-CMM, ITSEC, Common Crit. design principles 8. luennon kalvoissa software sec ja standardit viimeisessä

4

a) own private key, (created by self); recipient's (trusted) public key, safe delivery for recipient key or signed key (certificate); session key, created in process, random, 1p each
b) why: agree on algorithms (and other parameters), create session key, receive credentials (certificate); result: shared secret, client trusts server; require 2 on why and 1 on result for 3 p

5 this was hard, as not all are perfect matches, as long as some understanding is shown, OK

a) biba (integrity)
b) Clark-Wilson (specific procedures, if not integrity checking)
c) Bell-LaPadula w/ lattice, jos vain toinen ½ p
d) chinese wall