T-110.4206 Information security technology

Examination 2013-01-11

Lecturer: Tuomas Aura

No electronic equipment or reference material allowed in the examination.

*Answer **only 5** of the 6 problems. If you answer them all, only problems 1–5 will be marked.*

1. **Security terminology**

   Explain the meaning of the following terminology:
   a) trusted path
   b) privacy
   c) pseudo-SSO

2. **Access control**

   (a) The output below shows the permissions on three files in a Unix system. The system has four user accounts: root, alice, bob and carol. Only alice and carol belong to the gamers group. Present this access control state in the form of an *access control matrix*. Include in the matrix also information about *who is allowed to change the access rights* on each file.

```
$ ls -l
-rwxr-x---  1 alice   gamers  0 28 Dec 11:15 maxviolence
-rw-r--r--  1 alice   users   0 28 Dec 11:15 proof.tex
-rw-r--r--  1 bob     users   0 28 Dec 11:15 story.doc
```

   (b) Explain the purpose of the "no read up", "no read down", "no write down", and "no write up" rules in multi-level security: (1) what security property does each one of the rules protect and (2) against whom. (max four sentences in total)

3. **Cryptography and user authentication**

   What properties and features are needed in a function that is used for computing hash values of user passwords for password storage? Explain also why.

4. **PKI**

   Explain in detail how a certificate chain is verified and how it is used to check the authenticity of a secure web page.

Please turn the paper for problems 5-6.

5. **Secure storage**

Alice and her company use a TPM-based disk encryption solution to protect data. How does the *cold boot attack* against disk encryption affect the security of Alice's data in the following situations?

a) Alice locks her screen when she leaves her workstation unattended in the office.

b) Alice forgets her computer at the airport security check and, when she comes back to look for the computer, it is not there.

c) Thieves break into the company's server room and steal the expensive new file server.

6. **Threat analysis**

What security threats are there related to *wireless home routers*? Most homes now have one of these devices. The computers at home are connected to the router over Wireless LAN or Ethernet, and the router connects them to the Internet. Remember to consider broadly the potential attackers and their motivations.

[Photo: Wikipedia]

559-este

558 - mod este !

557-este

555 -este

531 -este

560-?