T-110.4206 Information security technology
Examination 2010-10-28
Lecturer: Tuomas Aura

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 terms (max 20 words each):

a. MAC (in relation to access control)
b. capability
c. ACL Access Control List
d. IAM
e. four-corner model
f. identity proofing

2. User authentication

The password policy at a university is changed so that, in the future, all passwords must have 8 characters, include at least two capitals (A...Z), at least two digits (0...9) and at least two special characters (*+[\$ etc.). <u>How</u> and <u>how much</u> does this affect the security of the passwords for

a. Alice who is used to composing her passwords by taking the first letter of each word in an approximately 8-word sentence (e.g. "My aunt Eve is sometimes an evil eavesdropper." = "MaEisaee")? ↑
b. Bob who is used to generating random 8-character passwords with a program he wrote?

Assume roughly 128 characters? ↓ $\Rightarrow (2^7)^8 = 2^{56}$

3. Unix security

Explain the purpose of the following Unix commands:

a.	% chmod 740 file.txt
b.	% umask 037 The default access rights
c.	% mkdir docs % chmod go+rw docs % chmod +t docs

for user, group and other: 740

(Hint: t=sticky)

4. **Secure storage**

Trusted Module Platform

Alice uses a TMP-based disk encryption solution to protect her 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.
   b. Alice's notebook computer is stolen from here suitcase.
   c. Security official at an airport asks Alice to boot up her notebook to show that it is a real computer. He then takes the computer to the back room to be scanned for explosives.

5. **Payment systems**

EMV payments have three different levels of security: Static data authentication (SDA), Dynamic data authentication (DDA), and Combined DDA and application cryptogram (CDA).

   a. What are the differences between these, and when and why would each one be used?
   b. How does the security of these methods compare with the old magnetic stripe cards?

6. **PKI and cryptography**

Explain reasons for the following:

   a. SSL uses public-key cryptography, which is known to be slow and computationally expensive. Nevertheless, SSL works quite fast on low-end client computers and mobile clients.
   b. Most Internet users do not have digital certificates. Nevertheless, they are able to connect to servers on the Internet with SSL, which uses certificates for authentication. Only server is authenticated
   c. Most root CAs do not issue certificates directly to web servers. Instead, they certify a sub-CA, which issues the end-entity certificates.