CS-C3130 Information security
Examination 2017-03-04
Lecturer: Tuomas Aura

No electronic equipment or reference material is allowed in the examination.

1. Identity and privacy

Define or explain the following concepts (max three sentences each):
(a) Privacy
(b) Identity provider
(c) Identity proofing

(In Finnish: *yksityisyys, identiteetin tarjoaja, ensitunnistus*)

2. Access control

Carol is the system administrator on the office Linux server, which has four users: the bosses Alice and Bob, and the development team A members Carol and David. Here is the output of the `ls -l` command on a folder on the computer:

```
-rw-------   1 david    teama     18378002 27 Oct 03:11 code.zip
-rw-r-----   1 alice    teama      8943593 27 Oct 03:02 spec.doc
-r--r-----   1 bob      bosses      288431 10 Jul  2015 synergy.pptx
-rw----r--   1 alice    bosses    20322136 21 Jun 05:06 yacht.jpg
```

Problem: Show the protection state for the above objects in the form of an access control matrix. If your solution matrix does not give a complete picture, add an explanation.

3. Authentication

A mechanical combination lock has 3 to 6 wheels, each with digits 0–9. In order to open the lock, one needs to align the right numbers on one line.

a) What is the entropy of the secret key information for 3-wheel and **4**-wheel locks? Give an approximate numerical answer including the unit.
b) The mechanical combination locks are replaced with a new electronic lock, which has a PIN pad and a connection to a backend server. You are asked to help designing the new lock system. How can the security of the electronic lock be improved compared to the mechanical one?


Note for part (b): You do *not* need to consider mechanical or software flaws in your answer.

Please turn the paper for the remaining parts of the examination.

4. Encrypted storage

Consider disk encryption solutions for server computers that do not require user interaction or input during a reboot, for example, after a security update or power outage. Compare solutions based on (a) encryption built into the disk drive hardware or firmware, (b) solution where the master key is sealed by a TPM, and (c) purely software-based solution. In your answer, explain briefly the threats and attack scenarios that are significant for the comparison. (You can either base your answer on the different usage modes of BitLocker or take a more general point of view.)

5. Threat analysis

A concert venue decides to start using NFC (contactless) wristband tickets. The tickets are sold to attendees online before the concert and delivered by post. They are read with an NFC reader at an automated entrance gate. The tickets are pretty cheap and will be thrown away after a single use. What security threats and potential vulnerabilities are there in this system? Which of the threats are the most serious ones from the point of view of the concert organizers?