CSE-C3400 Information security
Examination 2014-10-23
Lecturer: Tuomas Aura

No electronic equipment or reference material allowed in the examination.

1. Security terminology

Explain the following concepts (max three sentences each):
(a) Privacy
(b) Handshake and session protocol
(c) EMV dynamic data authentication

2. Access control

The family Macintosh computer has three users: the parents Alice and Bob, and their children Carol and David. Carol is the system administrator. She has set up user groups for the parents and children.

Here is the output of the `ls -l` command on some folder on the computer:

```
-rw-r-----   1 bob    parents    1224238 10 Jul 20:52 Photo.jpg
-rw-r-----   1 alice  children      5408 26 Mar  2013 Story.txt
-rw----rw-   1 bob    parents    8322136 21 Jun 05:06 Data.db
-rw-------   1 carol  children  23943593 14 Aug 10:11 Movie.mpeg
```

Problem: Show the protection state for the above objects in the form of an access control matrix.

3. PKI

Aalto University buys web certificates from commercial certification authorities like TeliaSonera. The university could save this money by becoming its own CA. What other advantages and disadvantages would there be in addition to not having to pay for the certificates? Also, would you recommend university take such a step, and why?

4. Data encryption

Design a client-based file encryption system for files stored in Dropbox, OneDrive or a similar cloud storage service. In your design, specify what keys and cryptographic algorithms are used, and what is encrypted or signed. The security goal is to protect confidentiality of the file contents in the cloud storage. It should be possible to share files between users and to revoke access to the shared files. Each user trusts his or her own client computer and the software on it, but the storage server should not be able to learn the file contents.

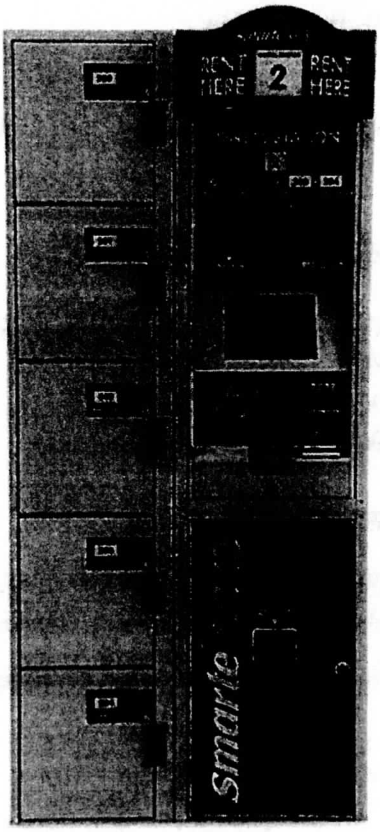
Please turn the paper for problem 5.

5. Threat analysis

An electronic locker facility (luggage storage) at a railway station works as follows: User pays the storage fee for one day at the terminal. The payment is made with a debit or credit card. The printer outputs a 6-digit PIN code. At the same time, a locker door opens electronically. The user puts the luggage into the locker and closes the door. Later, the user returns and enters the PIN code into the terminal. If more than 24 hours have elapsed, the user is required to make another payment. The locker door then opens electronically and the user takes the luggage.

The lockers have been analyzed by a professional locksmith, who found them to withstand physical attacks. Also, the card payment system is certified for EMV payments. Now, you have been asked, as a computer security expert, to analyze the system security. You are told to ignore the physical attacks and the EMV payment security in your analysis.

Problem: Analyze the security threats against the lockers. Additionally, prioritize the 3-4 most important threats.



[Image source: smartecarte.com]