CS-C3130 Information security
Examination 2016-10-27
Lecturer: Tuomas Aura

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

Advice: Because of the large number of students, the exam questions this year may appear short and simple. Relatively short solutions are ok, but that means you should think extra carefully about them.

1. Payment systems

In addition to the card number, credit and debit cards have a short security code printed on the card. It is 3-4 digits long and often printed on the back of the card next to the cardholder signature panel. The code has many names, for example CVC2 in MasterCard and CVV2 in Visa. These codes have been added to credit and debit cards after the year 1997. Explain in detail the purpose and working principles of this this feature.

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. Data encryption

Every morning after arriving at the factory, Alice logs into her Windows workstation with her username and password. She then works on her secret product-plan documents, which are encrypted with the *Encrypting File System* (EFS). In the evening, she logs off and goes home. Bob, the industrial spy, has infiltrated Alice's company as a sanitation consultant. What different ways does Bob have for getting access to Alice's secret documents?

Please turn the paper for the remaining problems.

4. User authentication

Acme Inc. has created a cloud-based online service where the users can register and set up a username and password. So far, they have one million registers users. The passwords are machine-generated random 12-character strings with the following character set:

0123 4567 89bc dfgh jklm npqr stvw xz+#

The passwords are stored as hash values that are truncated to 128 bits:

hash = truncate(SHA-256(password), 128)

Sadly, the password database has leaked to the deep web where Wile E., a notorious hacker, has found them, and he now plans to do some brute-force cracking.

a) How much does it cost for the attacker to crack the password of the user *rrunner*?

b) How much does it cost for the attacker to crack all the passwords?

c) How can the security of the passwords storage be improved for the future without incurring significant costs? How would your solution change the answers to parts (a) and (b)?

Since no pocket calculator is available, approximate calculations are sufficient, but please show the intermediate steps of your calculations. Useful data: A high-performance GPU can compute 1000 million SHA-256 hash values per second. One GPU day costs about $1 considering that the price of the GPU is spread over a three-year lifetime. One day is 86400 seconds.

5. Online fraud

Explain what is the most likely purpose behind the following emails if they appear in your inbox:

a) From: Chase Bank Online
Subject: Important message about your account

b) From: U.N. Relief Commission
Subject: Awarded donation funds

c) From: Roger Baker
Subject: Work from home earn $500 a week as financial transaction processor

d) From: Tuomas Aura
Subject: FW: FW: Laughed my ass off when I opened this file

e) From: Virtanen Pekka
Subject: Security bulletin 27.10.2016 - ransomware malware!

f) From: Anna
Subject: Looking for romance, eagerly waiting your answer