**T-110.4206 Information security technology**
**Examination 2013-12-17**
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 concepts**

   Explain the relation between the concepts (1) confidentiality, (2) privacy, and (3) access control.

2. **Access control**

   Give an application example of each of the following:

   a) Chinese wall policy
   b) low-water-mark policy
   c) parameterized role

3. **Passwords**

   An online service authenticates its users with 8-character passwords, which the service provider selects randomly for the user. The character set for the passwords is the following:

   abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890–+

   The service stores the passwords in a database as hash values. The hash function is SHA-256, which is computed on the password and a constant string:

   *hash = SHA-256 ("Bob's service" | password)*

   The service has about 100000 users.

   (a) How many bits of entropy does one password have?

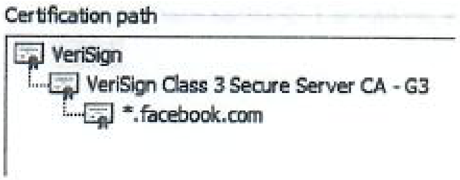
   (b) The attacker has a fancy graphics card that can compute 500 million SHA-256 hashes in a second. If the attacker manages to read the hash values from the database, e.g. with SQL injection, how long does it take to crack at least 100 passwords with brute-force trial? (A rough estimate is ok. Do not use an electronic calculator.)

   (c) The service operator wants advice on improving the security of this system further. What advice would you give?

Please turn the paper for problems 4-6.

## 4. PKI

Explain in detail how the user and web browser verify the authenticity of the web page https://www.facebook.com/, which has the following certificate chain:


Certification path

- VeriSign
  - VeriSign Class 3 Secure Server CA - G3
    - *.facebook.com

Note: It is not necessary to list or explain the SSL protocol messages.

## 5. Payment systems

In addition to the credit card number, card holder name and expiration date, the magnetic stripe or integrated circuit on the card contains the *Card Verification Value (CVV)*. The CVV is typically 5 bytes of binary data. Another value called *Card Verification Value 2 (CVV2)* is printed on the back of the card. CVV2 is typically 3 decimal digits.

How are CVV and CVV2 used for security and what are the limitations or security weaknesses of these two security mechanisms in the following use cases:

(a) parking fee payment in an offline terminal without a PIN pad
(b) web shopping

Note: The terminology varies between systems. Other names for the same concepts include card verification code (CVC) and card security code (CSC). CVV may also be called iCVV when the value is stored in the chip (integrated circuit).

## 6. Threat analysis

An amusement park uses wrist band tickets. The ticket is valid for unlimited rides on any park equipment during one day within a year from the purchase. Tickets are read with a bar code scanner at a gate before each ride. What security threats and potential vulnerabilities are there in this system? Prioritize the threats (approximately) from the point of view of the amusement park business.