Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March 14, 2013, 14–19

- You may answer in either Swedish or English.
- If any data is lacking, make (and state) reasonable assumptions.
- Use legible hand writing. If your answers cannot be read, you will receive zero points on that problem.
- Only pencil and eraser is allowed.
- Grading is done as follows.
  Grade 3 = 20–29 points,
  Grade 4 = 30–39 points,
  Grade 5 = 40–50 points.

Problem 1. The course has given (at least) three examples of situations where introducing publicly known randomness has resulted in more secure solutions. These are initialization vector (IV), salt, and nonce. For each of these, explain how this publically known value adds security. (3 points)

Problem 2. A server often wants to authenticate a client. The SSL/TLS handshake protocol includes the possibility to authenticate the client, but this possibility is typically not used on the Internet when requesting SSL/TLS protected webpages. Why? (3 points)

Problem 3. Give two differences between the LM and the NTLM hash that are important for security. (3 points)

Problem 4. In the Bell-LaPadula security model, a secure state is a state that satisfies the ss-property, the *-property and the ds-property. Define these properties. (3 points)

Problem 5.

a) Explain how a canary value can be used to detect a buffer overflow attack.

b) Give an example of how a buffer overflow attack can be prevented.

(2+1 points)

Problem 6. IPsec can be used in either transport mode or tunnel mode and using either the AH or the ESP protocol.

a) A new IP header is constructed when tunnel mode is used. Explain the advantages of this (i.e., the advantages of tunnel mode compared to transport mode).

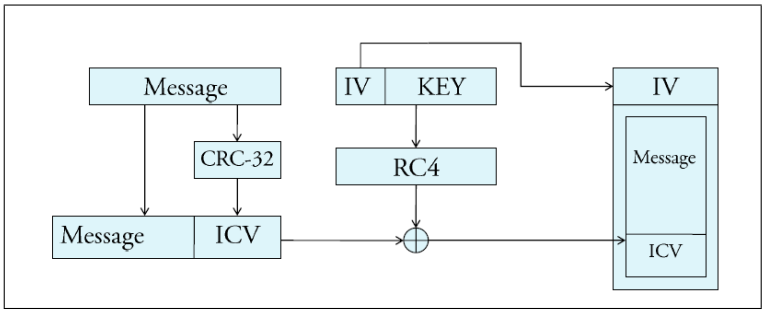
b) How does IPsec protect against replay attacks?

(2+1 points)

Problem 7. What are the differences between the two IDS techniques *anomaly detection* and *misuse detection*? (3 points)

Problem 8. How are the Orange book, ITSEC and Common Criteria related? How do they differ in their treatment of functionality and assurance? (3 points)

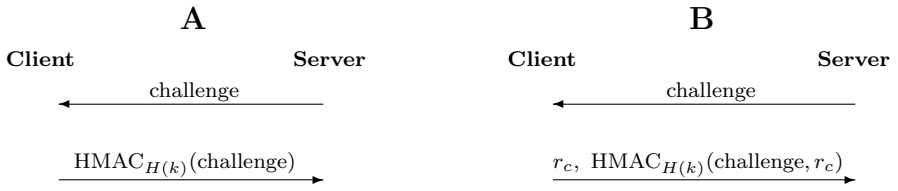
Problem 9. In order to have integrity protection of the messages in WEP, CRC-32 is used. The linear function CRC-32 is used to compute an integrity check value (ICV) of the message. The ICV is appended to the message and the resulting bitstring is encrypted using RC4 (see figure). To verify that the message has not been changed during transmission, the recipient decrypts the bitstring, computes the ICV of the message using CRC-32 and compares it to the value in the decrypted bitstring.



Adding ICV to message in WEP.

Assume that you can intercept these encrypted bitstrings, change them, and forward them to the intended recipient. Explain how you could flip the first and the last bit of the message without the recipient being able to detect this when checking the integrity of the message. (3 points)

Problem 10. Consider the two authentication protocols given below. $\text{HMAC}_{H(k)}(x)$ is an HMAC computed on the input x using key $H(k)$, where $H(k)$ is the hash computed on a password k.



a) You want to perform a TMTO attack to recover the password. Explain how a MITM attack can make a client use a challenge chosen by the attacker in protocol A.

b) A *known* (i.e., eavesdropped) challenge would be enough in a brute force or dictionary attack. Why is a known challenge not sufficient in a TMTO attack?

c) In protocol B, the client adds a random number r_c to the response. How will the security in the protocol change?

(1+1+1 points)

Problem 11. Consider protocol A from Problem 10.

a) Explain how you would *build* the TMTO tables (or rainbow table, choose which you like best). Make sure you mention *startpoint*, *endpoint* and *reduction function*.

b) Assume that our online attack time should take time $T = 2^{24}$ and require memory $M = 2^{24}$. Approximately how complex can the recovered password be? Give the length of the largest passwords that can be broken assuming the passwords are alphanumerical.

c) How would a function like `PBKDF2()` improve the security of the protocol?

(2+2+1 points)

Problem 12. Consider a hash function with n-bit output.

a) Explain what is meant by *preimage resistance, second preimage resistance*, and *collision resistance*.

b) How many different inputs are needed (approximately) before a collision is found.

c) How many different inputs are needed (approximately) before a second preimage is found?

(3+1+1 points)

Problem 13. An example listing of directory content in Linux is given below, together with an excerpt from the file `/etc/group`.

Directory listing:

```
drwxrwsrwt   root   students  .
-rwsrwxrwx   alice  root      prog
```

/etc/group file:

```
students:x:1001:alice,bob,charlie
```

a) What will be the *ruid* of a process that executes prog?

b) What will be the *euid* of a process that executes prog?

c) Who can delete the file prog? Answer by giving an element in the powerset of {alice, bob, charlie, root}

d) Assume umask is 027, give the corresponding line in a directory listing when Alice creates a new non-executable file.

e) The file `/etc/passwd` often also has an 'x' in the corresponding position as can be seen in the `/etc/group` file above. What does this 'x' mean in the `/etc/passwd` file?

(1+1+1+1+1 points)

Problem 14. Explain shortly the following five terms:

a) Reference monitor

b) Clark-Wilson

c) CBC mode

d) Security descriptor

e) inode

(1+1+1+1+1 points)
