Exercises, set 3

Computer Security

- You do not have to hand this in. You can completely ignore these exercises if you wish.
- These exercises are given for you to check your knowledge during the course.
- These exercises are based on material in Chapters 11-15 (except 14 and 15.5). Some exercises may require you to look for information outside the textbook as well.
- Exam questions can be based on some or none of the exercises.
- The teachers are happy to help you out if you run into problems.

Exercise 3.1
a) Describe the information flow in the Bell-LaPadula security model.
b) Assume that process A has a higher security level than process B. Moreover, process A is not considered trusted and the security level of an object cannot be changed. How is it possible for process A to send information to process B without violating the access rules of the model?

Exercise 3.2
a) What is a replay attack?
b) How can a replay attack be prevented?
c) Explain how Kerberos prevents replay attacks.

Exercise 3.3 Following the unexpected failure of the xor-based three-way protocol from exercise 1.6 the same person has now invented a new protocol. The new protocol is based on the Encrypted Key Exchange (EKE) protocol designed to resist offline dictionary attacks. In the original protocol Alice uses her password to encrypt a public key and the result is sent to Bob. Bob then encrypts the session key using Alice's public key. The result is then again encrypted using the shared password. The observation leading to the modification is that symmetric algorithms are much faster than asymmetric ones, so why waste any time? Instead of encrypting a public key with the password Alice now encrypt a 128 bit AES key using the password. Subsequently Bob decrypts the AES key using the shared password, encrypts the session key using AES, and encrypts the result using the password. Analyze this protocol with respect to offline dictionary attacks. Is it still as resistant as the original protocol? NOTE: As with the original protocol we have to assume that anyone can intercept data encrypted with the session key and that this data has some redundancy.

Exercise 3.4
a) What parameters are assumed to be known to the man-in-the-middle attacker in the Diffie-Hellman protocol?
b) Show how the attack works using a numerical example. Explain clearly who chooses and has access to the different parameters.

Exercise 3.5 Give at least 3 important differences between TCSEC and Common Criteria.

Exercise 3.6 According to the *-property of the chinese wall security model, a person once having read sensitive information at Ericsson will never be allowed to write any information to any other company, e.g., Swedbank. Explain why such a restrictive rule is needed in theory.

Exercise 3.7 In the Bell-LaPadula security model, two different security levels are used for subject. The maximum level $f_S(s)$ is used to control read access and the current level $f_C(s)$ is used to control append access. Since we always have that $f_C(s) \leq f_S(s)$ it would be possible to read an object o while at the same time appending to an object o', with $f_O(o') \leq f_O(o)$. The downward information flow made possible here is solved by adding an extra restriction to the *-property.
a) Describe this extra restriction to the *-property.
b) What if we instead modify the ss-property, and instead of using $f_S(s)$, we use $f_C(s)$ to control read access? Then it would not be possible to have read access to an object with higher security level than objects we have append access to. Analyse this alternative approach.

Exercise 3.8 Operating system A has been evaluated according to the Orange Book and has received the classification C2. Operating system B has been evaluated using Common Criteria and has received level EAL4. What can you say about the functionality and assurance for OS A and OS B?

Exercise 3.9 In the last message of the Needham-Schroeder protocol the message $eK_{ab}(n_b - 1)$ is sent, while in Kerberos $eK_{ab}(T'_a)$ is sent.
a) Why do we have to send $eK_{ab}(n_b - 1)$ in Needham-Schroeder? Why can't we send $eK_{ab}(n_b)$?
b) Why do we *not* have to send $eK_{ab}(T'_a - 1)$ as the last message in Kerberos. Or do we?

Exercise 3.10 In the Windows implementation of Kerberos the first message sent from the client to the KAS includes a timestamp encrypted with a key derived from the user's password. This is not included in the Kerberos description given in Gollman's book. It is optional in the protocol and referred to as preauthentication.
a) Explain to which extent this is more secure against attacks on the password.
b) If preauthentication is used the server can decrypt the timestamp using the password of the client and check that the timestamp is valid. This would authenticate the client. How is the client authenticated if preauthentication is not used?