University of Oslo
INF3510 Information Security
Spring 2012
Workshop Questions

Lecture 6: Key Management and PKI

Question 1

a. Why is the management of cryptographic keys such an important issue?
b. Three main key categories are: i) symmetric secret keys, ii) asymmetric public keys and iii) asymmetric private keys. Explain which type of security service/protection is required for each key category.
c. Describe security mechanisms/methods that can be used to implement the required security service/protection for keys.
d. Briefly list the main issues a key management system must deal with.

Question 2

a. Draw the diagram showing the key states and transitions between them as described by NIST SP800-57. Explain the diagram.
b. When a key is active, it may be designated to protect only, process only, or both. Referring to the 19 key types described in NIST SP800-57, give two examples of key types that are designed to protect only, two examples of key types that are designed to process only, and two examples of key types that are designed to both protect and process.
c. Explain why key types 17, 18 and 19 are misnomers. Suggest better names for those key types.

Question 3

Describe reasons why online services can benefit from public-key cryptography? Why is symmetric key cryptography alone not suitable for online services?

Question 4

a. Explain what is meant by the spoofing problem with respect to public-key cryptography.
b. Clearly explain how digital certificates can provide a solution to the spoofing problem.
c. How much trust should be placed in a digital certificate? Justify your answer.
d. Is a digital signature the same as a digital certificate? Justify your answer.

Question 5

a. Briefly describe the primary purpose of a public key infrastructure.
b. Describe and contrast the function of each of the following basic components in a PKI system:
   - Certification authorities (CA)
   - Registration authorities (RA)

Question 6

a. Describe the Browser PKI trust model.
b. List the advantages and disadvantages of this model.

Question 7

Access to the stored root and intermediate certificates in your browser is via the browser menus. For example

- MS Internet Explorer, select: Tools → Internet Options → Content → Certificates → Root certificates, then you will be able to examine certificates installed in your browser.
- Firefox, select: Tools → Options → Advanced → Encryption → View Certificates

Look through certificates installed in your browser to determine the expiration dates.

a. Which certificates have short lifetimes?
b. Can you find certificates with expiration dates in excess of ten years from now?
c. Can you find certificates that have already expired? What happens when viewing them?

Question 8

a. Why is it important to have a limited cryptoperiod for keys? Give at least four reasons.
b. What is the difference between protection and processing when using keys?
c. Compare the recommended cryptoperiod for private and public signature keys according to NIST SP800-57? Would you say that the validity period of root certificates in web browsers follow the recommendations of NIST SP800-57?