Practice Homework for the Final
Introduction to Information Security (266-642) [Spring 2007]
Due Date: None

In the homework, "the Stallings book" refers to [Sta06] and "the Handbook" refers to [MOV97] (I have linked the Handbook to the class homepage. You can download it for free.) Unless otherwise stated each part of a question has equal weight.

Question 1:
Part A: How do SYN-cookies protect a server from flooding attacks?
Part B: In a distributed-reflected denial-of-service attack, whose address is sent as the Source-IP of the SYN? Whose address is sent as the Source-IP of the SYN/ACK? Explain your answer. Use the following terminology:
M (Malicious Flood Generator)
R (Reflection Server (Innocent Bystander))
V (Victim of the Attack)

Question 2 (Authentication Protocols):
Part A Problem 13.4 from the Stallings book.
Part B: Problem 13.5 from the Stallings book.

Question 3 (DSA):
Part A: Assume that Alice uses the same random number k to sign two messages M and M'. Demonstrate that if Oscar knows the two signatures, he can derive the private key x.
Part B: Show that knowing the random number x is *equivalent* to knowing the random number k, i.e., if Oscar knows x, he can find k and vice-versa.
Part C: Problem 13.14 from the Stallings book.

Question 4 (Kerberos): For this question you have to read the explanation of Kerberos version 5 and appendix 14A from the Stallings book.
Part A: Problem 14.1 from the Stallings book.
Part B: Problem 14.2 from the Stallings book.
Part C: Suppose there is a "trust relationship" between realms in the CS and Biology department. Bob, who is a user in the CS realm, wants to access a server V in the Biology realm. Show the various steps required for Bob to authenticate himself to V.

Question 5 (X.509:)
Part A: Problem 14.3 from the Stallings book.
Part B: Consider the CAs arranged in a hierarchy as shown in Figure 1. Show the various certificates used to "navigate" the hierarchy. Demonstrate the chain that "validates" the public key of `Alice` to `Bob` and vice-versa.

Question 6 (SSL):
Part A: Problem 17.1 from the Stallings book.
Part B: Problem 17.2 from the Stallings book.

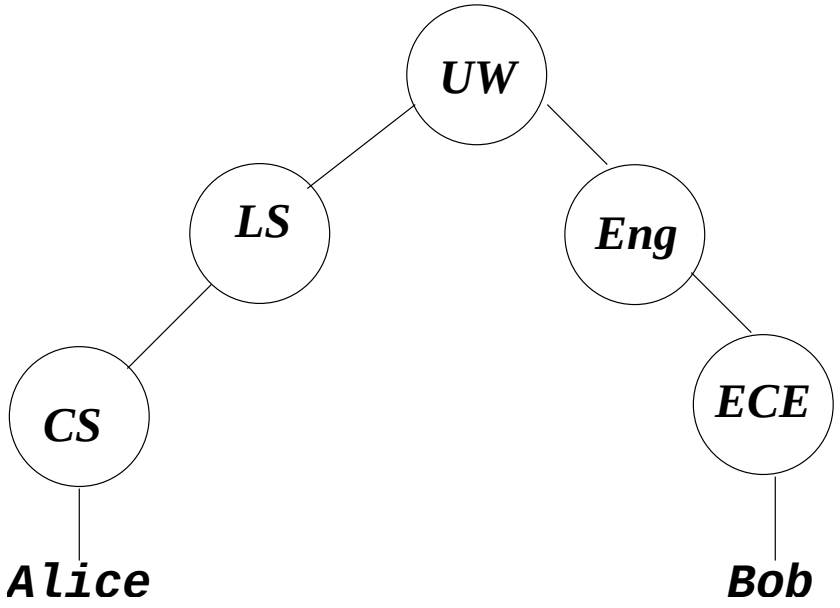

Figure 1: Hierarchy of certificate authorities.

References

[MOV97] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1997.

[Sta06] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2006.