Practice Homework for the Final
Introduction to Information Security (266-642) [Spring 2008]
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 Problem 11.4 from the Stalling’s book.
Part B Problem 11.6 from the Stalling’s book.

Question 2:
Part A: Problem 12.2 from the Stallings book.
Part B: Problem 12.3 from the Stallings book.

Question 3:
Part A Problem 13.1 from the Stallings book.
Part B: Problem 13.2 from the Stallings book.

Question 4:
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 5: For this question you have to read the explanation of Kerberos version 5 and appendix 14A from the Stallings book. Moreover, please read my note on interrealm authentication in Kerberos version 5.
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 6 (X.509:
Part A: Problem 14.3 from the Stallings book.
Part B: Consider the CAs arranged in a hierarchy as shown in Figure 2. Show the various certificates used to “navigate” the hierarchy. Demonstrate the chain that “validates” the public key of `Alice` to `Bob` and vice-versa.

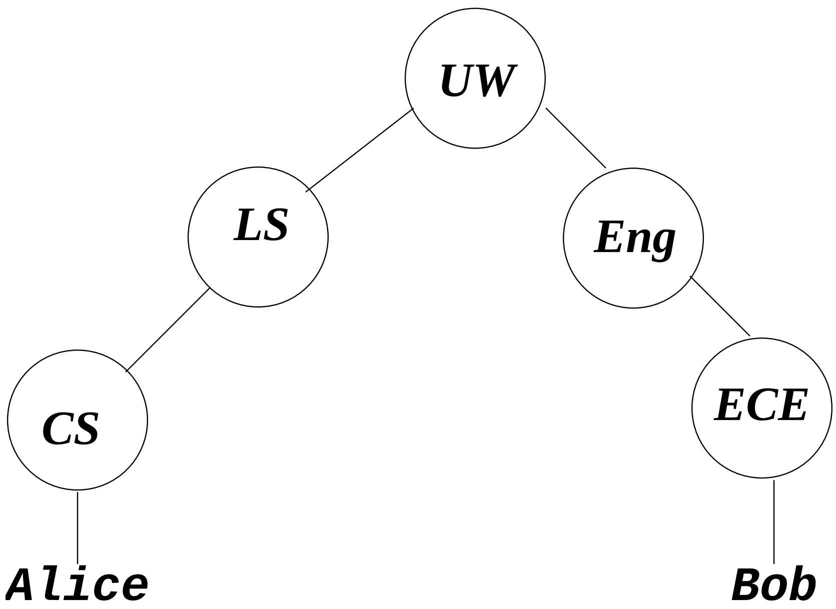

Figure 1: Hierarchy of certificate authorities.

1 Interrealm Authentication in Kerberos Version 5

Scenario: Assume that user U is in realm R_1 and wants to access the server V in realm R_k. There is a path $R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_k$ from realm R_1 to R_k. Conceptually, each edge $R_i \rightarrow R_{i+1}$ (for $1 \leq i < k$) represents a trust relationship between realm R_i and R_{i+1}, which usually means that there is a shared key between the two realms.
Initial request: U requests a *ticket-granting ticket* or *TGT* from the KDC in realm R_1 (which we denote by $KDC[R_1]$) for realm R_k with the `FORWARDABLE` flag set.[1] Since R_1 does not have a trust relationship with R_k, it issues a TGT $TGT[R_1 \rightarrow R_2]$ for realm R_2 with the `FORWARDABLE` flag set. We are assuming that there is a mechanism for realm R_1 to discover that there is a path to realm R_k that goes through R_2. *Note:* I am also assuming that the servers only issue these tickets if their policy allows it. For example, $KDC[R_1]$ only issues the TGT with the `FORWARDABLE` flag on to U, if its policy allows it. This will be implicit throughout the document.
Walking the path: Using the TGT $TGT[R_1 \rightarrow R_2]$, U requests a TGT for realm R_3 from the *ticket granting server* or *TGS* (denoted by $TGS[R_2]$) in realm R_2. The TGT issued by $TGS[R_2]$ (denoted by $TGT[R_2 \rightarrow R_3]$) for R_3 has the `FORWARDABLE` and `FORWARDED` flags on. The $TGT[R_2 \rightarrow R_3]$ can have a different address than U (presumably an agent is handling this on behalf of the user U). This process is repeated until U "reaches" the realm R_k, i.e., it has a TGT $TGT[R_{k-1} \rightarrow R_k]$ issued by $TGS[R_{k-1}]$ for the realm R_k.
Accessing V: The TGT $TGT[R_{k-1} \rightarrow R_k]$ is presented to the TGS $TGS[R_k]$ to obtain a *service-granting ticket* or *SGS* $SGT[R_k, V]$ for server V. This SGS can then be used to access the server V.

[1] In general, an entity will be indexed by the realm that it pertains to, e.g., a ticket-granting ticket or TGT issued by realm R_i for realm R_j will be denoted by $TGT[R_i \rightarrow R_j]$.

Question 7
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 8(Authentication Protocols):
Part A Problem 13.4 from the Stallings book.
Part B: Problem 13.5 from the Stallings book.

Question 9 (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 10 (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 11 (X.509:)
Part A: Problem 14.3 from the Stallings book.
Part B: Consider the CAs arranged in a hierarchy as shown in Figure 2. 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 12 (SSL):
Part A: Problem 17.1 from the Stallings book.
Part B: Problem 17.2 from the Stallings book.

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.

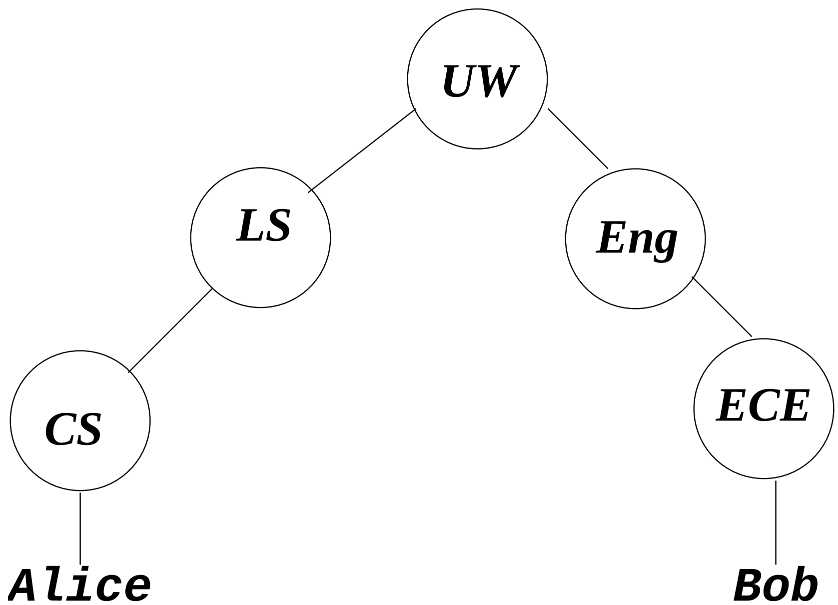

Figure 2: Hierarchy of certificate authorities.