CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Final Exam

January 3, 2011

Question 1. (*60 pts.*) Answer briefly each of the following questions:

a. What is Kerckhoffs' principle? Why is that principle important?

b. What is the "cube root problem" in RSA encryption? How does the PKCS address it?

c. Establishing a secure channel between two previously unacquainted parties over an insecure network requires support from a trusted third party, either a KDC or a CA. What are the relative advantages of each approach? For what type of networks is each suitable for?

d. What is key revocation? Is ID-based or traditional certificate-based key management more suitable with regard to key revocation? Why?

e. What is the salt in a password-based authentication system? How does it help in defending against offline dictionary attacks?

f. What is the main strength of the EKE protocol in comparison to Lamport's hash scheme?

g. What is the "single sign-on" (SSO) feature? How does Kerberos provide it?

h. What is the advantage of a puzzle scheme for DoS protection over a cookie scheme?

i. What is a virtual private network (VPN)? How can IPsec help establishing a VPN? Which mode of IPsec operation would be used for this kind of application?

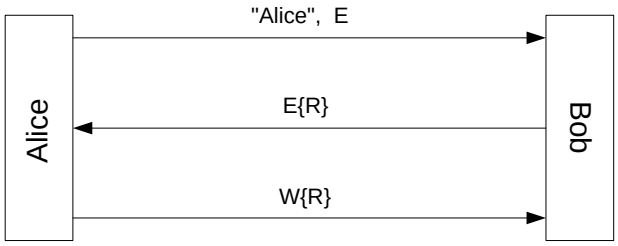
j. Does the SSL session establishment protocol (i.e., the main handshake protocol of SSL) have the feature of "perfect forward secrecy"? Why/why not?

k. Describe how 3D-Secure is related to and differs from its predecessor SET.

l. What is a rootkit? Why is it difficult to detect and remove kernel rootkits?

Turn the page

Question 2. (*20 pts.*) Consider the following protocol where W denotes a weak symmetric encryption key derived from a password, E is a strong public key generated by the client's terminal, and R is a random challenge.



a. Assume that the public key encryption scheme used is deterministic. How can the password be broken by an eavesdropper?

b. Let the public key encryption scheme be randomized. Describe how the password can be broken by an active attack.

c. Consider sending $W\{E\}$ in the first message instead of E. Does this preclude the attack in part (b)? Explain.

d. Consider the variant discussed in part (c). Suppose the terminal uses a fixed public key E instead of generating a fresh one for each session. What would a weakness of the protocol be?

Question 3. (*20 pts.*) On Bellovin's ESP attacks:

a. Summarize how each of the following attacks works:

- Reading encrypted data cut-and-paste attack
- Connection hijacking cut-and-paste attack
- IV attack on TCP destination port number

b. Is the TCP (or UDP) checksum a problem for these attacks? Why? If so, how can it be dealt with? Explain for each attack.

c. Is the TCP sequence number a problem for these attacks? Discuss for each attack.

Good luck