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

Final Exam

December 23, 2005

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

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

b. For a hash function, does collision-resistance imply one-wayness? Explain briefly.

c. Describe how the RSA signature function $S(x) = x^d \bmod N$ can be shared among n parties, such that when they all come together they can compute the signature of a message without revealing their shares, but $n-1$ or fewer cannot sign a message or obtain any information on the private key.

d. 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?

e. What is the purpose of the salt in a password-based authentication systems? Describe how it is used when a user logs into the system from a terminal.

f. What is the "single sign-on" property? How does Kerberos provide it?

g. Consider using RSA-EKE in a mobile computing environment where the client is typically a restricted device such as a palmtop computer. What is the major change you would do on the protocol discussed in class? Explain your reasoning.

h. Describe the processing of an outgoing IP packet on a machine running IPsec.

i. What is the main complication for Bellovin's cut-and-paste attack to read encrypted ESP data that would be brought by the use of IPv6? How can that be circumvented?

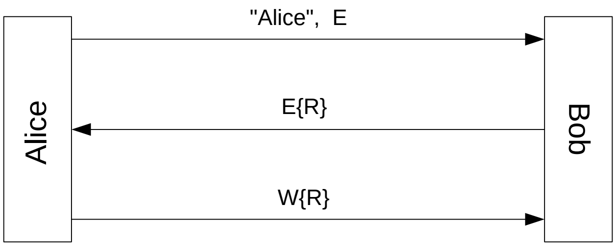
j. Would the solution to part (i) suffice for an attacker to use TCP as the transport protocol in the attack? Explain briefly.

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

l. What was the most significant handicap of PEM for a practical deployment? How does PGP handle this issue?

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.*) A protocol to establish a fresh session key using long-term, certified Diffie-Hellman public keys is the protocol of Yacobi and Shmuely. The protocol, in a slightly modified form, is as follows:

- The system has a common prime modulus p and a generator g. Each party i has a long-term private key $\alpha_i \in Z_{p-1}$ and a public key $P_i = g^{\alpha_i} \bmod p$.
- To establish a session key between i and j, party i generates a random $R_i \in Z_{p-1}$, computes $X_i = \alpha_i + R_i \bmod p - 1$, and sends X_i to j. Similarly, j computes a random $R_j \in Z_{p-1}$, $X_j = \alpha_j + R_j \bmod p - 1$, and sends X_j to i.
- i computes the session key as
$$K_{i,j} = (g^{X_j} P_j^{-1})^{R_i} \bmod p$$
and j computes
$$K_{j,i} = (g^{X_i} P_i^{-1})^{R_j} \bmod p.$$

a. Show that the protocol is correct (i.e., $K_{i,j} = K_{j,i}$).

b. Discuss the security of this protocol. (E.g., can an attacker break a private key or a session key, or can actively impersonate a party, etc.)

c. Show that the Yacobi-Shmuely protocol does not have security in the face of broken session keys. (Hint: Show that an attacker who has broken a session key $K_{i,j}$ is able to impersonate any of the two parties to the other.)

Good luck