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

Final Exam

January 16, 2012

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

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

b. Consider the RSA algorithm where the modulus n is a large prime rather than a composite number. Would the encryption be secure? Why/why not?

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

d. Name one advantage and one disadvantage of using a challenge-response authentication protocol (with strong, randomly generated cryptographic keys) for user authentication instead of an ordinary password protocol.

e. Where a client and a server share a password, it is always possible to use the password as the encryption key in a symmetric-key challenge-response protocol. What is the advantage of such an authentication protocol over ordinary password protocols? What is the advantage of EKE-type strong password protocols over this kind of challenge-response password protocols?

f. Describe how the Kerberos login protocol works. Is it secure against offline password guessing with passive eavesdropping? Explain why.

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

h. What is the purpose of a cookie in a public-key based authentication protocol like IKE? Why is it desirable to have the cookie stateless?

i. What is a replay attack? Describe the replay protection mechanism in AH and ESP. Explain how it works briefly.

j. What is NAT? Why is it problematic for IPsec AH?

k. What is the advantage of using 3D-Secure in on-line purchases instead of simple e-commerce over SSL?

l. Where would you prefer using an anarchical PKI over an hierarchical one? Where would you prefer an hierarchical one?

Question 2. (*20 pts.*) Describe the advantages and potential weaknesses of each of the following password login protocols:

a. Send pwd, compare against $h(pwd)$.

b. Send $h(pwd)$, compare against $h(pwd)$.

c. Send $h(pwd)$, compare against $h(h(pwd))$.

d. Use $h(pwd)$ as the key in a C-R protocol; server stores $h(pwd)$.

(Hint: Attacks may aim to recover the password or to impersonate the user without the actual password. Attackers may be capable of eavesdropping or breaking into the server's database. Passwords may or may not be breakable by a dictionary attack.)

Question 3. (*20 pts.*) A DH-based key exchange protocol for wireless mobile networks was a proposal by Park: The system has a common prime modulus p and a generator g. Each party i has a long-term private key $\alpha_i \in \mathbb{Z}_{p-1}$ and a public key $P_i = g^{\alpha_i} \bmod p$. To establish a session key between a mobile subscriber M and a base station B, the following protocol is executed (with all arithmetic in $\mathbb{Z}_p$):

$$\begin{aligned} B \to M &: g^{\alpha_B + R_B} \\ M \to B &: \alpha_M + R_M \end{aligned}$$

where R_B and R_M are one-time random secrets. B calculates the session key as $K_{MB} = (g^{\alpha_M + R_M} P_M^{-1})^{R_B}$ and M calculates it as $K_{MB} = (g^{\alpha_B + R_B} P_B^{-1})^{R_M}$. Then they complete the authentication with a challenge-response by K_{MB}.

Park's protocol was based on an earlier protocol by Yacobi and Shmuely, where both parties send $\alpha_i + R_i$; however Park made the station send $g^{\alpha_B + R_B}$ to reduce the load on the mobile side.

a. Show that Park's protocol is correct in the sense that B and M calculate the same K_{MB} value.

b. Show that an attacker who has compromised a session key from a previous run, for which she has recorded the messages, can impersonate B. (Hint: Let the attacker replay B's message from the previous session.)

c. In fact this protocol can be broken without having any previous session keys compromised: Show how the attacker can impersonate B by just knowing his public key.

Good luck