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

Final Exam

January 6, 2007

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

a. 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?

b. What is the "guessable plaintext" problem in public key encryption? Does it also apply to ElGamal encryption? Why/why not?

c. As MACs can be produced from hash functions, consider producing a hash function from CBC-MAC, where the CBC checksum of a message is computed using a fixed key and IV. Would this hash function be secure? Why/why not?

d. Consider "randomized hashing" where a signer to sign a message m first generates a sufficiently long (say 128-bit) random r, computes $H(r\|m)$, and signs it along with r. Would collision resistance be a requirement for H in this case? Why/why not?

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

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

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

h. In a user authentication system, why is it preferable to use the password as an encryption key in a challenge-response fashion rather than sending a cleartext hash of it? What is the limitation of this approach, which EKE-type strong password protocols aim to solve?

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. Describe briefly Bellovin's connection hijacking attack on IPsec encryption without authentication. Why is the TCP sequence number a source of complication in this attack? How can it be tackled?

k. What are some of the major problems in IKE which IKEv2 aims to solve? Name three of them and describe how IKEv2 deals with each.

l. What are the relative advantages and disadvantages of S/MIME and PGP? What are the environments that would favor each?

Turn the page

Question 2. (*20 pts.*) Explain the following points regarding Tuomas Aura's talk on Mobile IPv6 security:

a. What is the problem with the binding updates when no authentication is present?

b. What is the approach of Aura et al. to this problem?

c. What is the basic solution they propose?

d. What is the problem with this solution when satellite links are common?

e. What would be a simple solution to prevent such passive attacks? (without any major changes to the basic setting such as adding a PKI)

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