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

Final Exam

January 19, 2004

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

a. What is the major limitation of traditional substitution ciphers? How do the modern block ciphers address it?

b. Is a fixed or a random IV preferable in a CBC-MAC computation? Why?

c. What is the "guessable plaintext" problem in RSA encryption? Is it also a problem for ElGamal encryption? Why/why not?

d. How is the salt used in Lamport's one-time password protocol? Describe two advantages of using a salt in this protocol.

e. What is the advantage of EKE over Kerberos as a password-based authentication protocol?

f. 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?

g. Why is a separate SPI used for each direction of an IPsec connection?

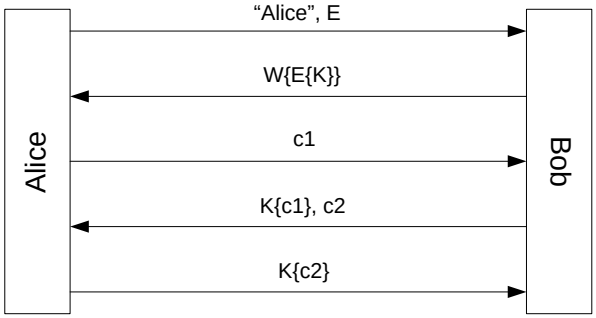
h. What is the replay protection mechanism in AH and ESP? Explain it briefly.

i. Consider Bellovin's cut-and-paste attack on ESP encryption to read encrypted data. If IPv6 is in use between the source and destination machines in the attack, UDP checksum verification will be mandatory and the attacker will not get the decrypted plaintext if the verification fails. Describe how the attacker can circumvent this problem.

j. What is a packet filtering firewall? How do stateful inspection firewalls differ from packet filtering firewalls?

Turn the page

Question 2. (*20 pts.*) Consider the following EKE-type protocol, where E is a per-session public key generated by Alice's terminal, W is the shared secret derived from Alice's password, and K is the session key to be used.



a. Why is it desirable to have E change over sessions rather than keeping it as a long term key of the terminal? (Hint: Consider the protocol's security when a past session key K is compromised.)

b. Why is this protocol not secure?

c. Describe a simple modification to secure this protocol while still having Alice transmit E unencrypted.

Question 3. (*20 pts.*)

a. Describe how message authentication/integrity is provided in PEM.

b. Show that CBC-MAC is not one-way when the key is known. (I.e., for a given y and k, it is possible to find m such that CBC-MAC$_k(m) = y$.)

c. Assume PEM is being used with secret interchange keys (i.e., the long term keys) and with CBC-MAC in the MIC computation. Alice sends an ENCRYPTED message to Bob and Carol. Describe how Bob, having received that message, can send forged messages in Alice's name to Carol.

d. Assume PEM is being used with public interchange keys and with CBC-MAC in the MIC computation. Alice sends an ENCRYPTED message to Bob. Describe how Bob, having received Alice's message, can send forged messages in Alice's name to any third party.

Good luck