Computer Security Department of Computer Science,
Dr. Simon Foley University College,
Symmetric Protocols Problem Set. Cork, Ireland.

1. Alice (A) wishes to communicate securely with Bob (B) and proposes a symmetric key K_{AB}, a copy of which she intends to give to Bob. Trent is a trusted third party who shares secret (symmetric) key K_{AT} with Alice and secret (symmetric) key K_{BT} with Bob. The following protocol is used to pass the key K_{AB} to Bob.

$$\begin{array}{lll} \text{Msg 1:} & A \rightarrow T: & (\{B\}_{K_{AT}}, \{K_{AB}\}_{K_{AT}}) \\ \text{Msg 2:} & T \rightarrow B: & (\{A\}_{K_{BT}}, \{K_{AB}\}_{K_{BT}}) \end{array}$$

   (a) Discuss any disadvantages in the operation of the above protocol. In particular, compare it with the operation of a Kerberos/Needham-Schroeder style protocol.

   (b) Suppose that principal B above is a Ticket Granting Server that controls access to, and shares a secret key with, the file server C. Propose and explain a protocol exchange between A and B that might result in A obtaining a ticket enabling it to authenticate/connect securely with C. Discuss any problems that your protocol design might have.

   (c) Illustrate how third user, Eve (who shares a secret key K_{ET} with Trent) can subvert the protocol and get a copy of a key K_{AB} that Alice gives to Bob using this protocol.

   (d) Illustrate how Eve can subvert the protocol and masquerade as Alice to Bob, even when Alice does not initiate a key exchange with Bob.

2. The following mutual authentication protocol has been designed to be resilient against reflection attacks. This is done by ensuring that the challenge from the initiator looks different from the challenge from the responder.

$$\begin{array}{lll} \text{Msg1} & A \rightarrow B: & \mathsf{I'm\ Alice}, R_2 \\ \text{Msg2} & B \rightarrow A: & R_1, \{\mathsf{Bob}, R_2\}_{K_{AB}} \\ \text{Msg3} & A \rightarrow B: & \{\mathsf{Alice}, R_1\}_{K_{AB}} \end{array}$$

   Suppose that a programmer implements the above protocol across a unix network, where principal names are eight (8) characters long and

triple DES-ECB is used for encryption. Outline a possible (reflection) attack on this protocol.

3. A programmer simplifies the Needham Schroeder protocol as follows.

$$\begin{array}{lll} \text{Msg1} & A \rightarrow T: & A, B \\ \text{Msg2} & T \rightarrow A: & \{B, K_{AB}, \{K_{AB}, A\}_{K_{BT}}\}_{K_{AT}} \\ \text{Msg3} & A \rightarrow B: & \{K_{AB}, A\}_{K_{BT}}, \{N'_A\}_{K_{AB}} \\ \text{Msg4} & B \rightarrow A: & \{N'_A - 1, N_B\}_{K_{AB}} \\ \text{Msg5} & A \rightarrow B: & \{N_B - 1\}_{K_{AB}} \end{array}$$

Suppose that Eve manages to steal Bob's key K_{BT}. Can the protocol be compromised even when Bob and Trent re-key (use a new, uncompromised key K_{BT})? Explain your answer.

4. A programmer (foolishly) decides to simplify the Kerberos protocol specification. The Kerberos server and ticket-granting servers are implemented by a single (trusted key) forwarding service T. The revised protocol is specified as:

$$\begin{array}{lll} \text{Message 1}: & A \rightarrow T & : B, \{K_{AB}\}_{K_{AT}} \\ \text{Message 2}: & T \rightarrow B & : A, \{K_{AB}\}_{K_{BT}} \end{array}$$

Assuming Alice A shares secret key K_{AT} with T then she uses this protocol to propose a session key K_{AB} to T so that a (temporary) secure channel based on K_{AB} may be established between A and the service B (a file system, for example).

   (a) It is the duty of T to authenticate requests from Alice. How might Alice's password be used for login and initial authentication in the protocol above?

   (b) It is the duty of T to mediate access requests, that is, to decide whether Alice may access certain services. How might this be achieved using the protocol above?

   (c) Illustrate how a legitimate user Eve can subvert the protocol and masquerade as another principal.

5. A programmer wants to use DES-CBC to support both integrity and confidentiality. He implements the following scheme. He computes a message authentication code MAC based on the last cipher block

generated from encrypting (DES-CBC) plaintext blocks $b_0, \ldots, p_{n-1}$. He then encrypts the stream of blocks $b_0, \ldots, p_{n-1}, MAC$ using DES-CBC. When decrypting, the MAC block can be used to check for integrity. Outline an attack on this scheme, whereby an attacker can corrupt the ciphertext blocks without being detected.

6. Why are authentication protocols such as Kerberos and Needham-Schroeder more *practical* than the wide-mouth frog protocol?

7. The following protocol is used by principal B to authenticate principal A.

$$\begin{array}{lll} \text{Msg1:} & A \rightarrow B & A \\ \text{Msg2:} & B \rightarrow A & N_B \\ \text{Msg3:} & A \rightarrow B & \{N_B\}_{K_{AS}} \\ \text{Msg4:} & B \rightarrow S & \{A, \{N_B\}_{K_{AS}}\}_{K_{BS}} \\ \text{Msg5:} & S \rightarrow B & \{N_B\}_{K_{BS}} \end{array}$$

   Symmetric keys K_{AS} and K_{BS} are shared between principals A and S, and between B and S, respectively. N_A and N_B represent nonces.

   (a) How well designed is this protocol? Explain your answer.

   (b) Outline a possible attack on this protocol [super hard].

8. Consider the following fragment from a Kerberos-like authentication protocol, whereby initiator A requests, and is granted, a ticket from Authentication Server S to be used with service B.

$$\begin{array}{lll} \text{Msg 1}: & A \rightarrow S: & A, B, N_a \\ \text{Msg 2}: & S \rightarrow A: & T_{ab}, \{B, L, N_a, K_{ab}\}_{K_a} \end{array}$$

   Principals A and B share long-term secret keys K_a and K_b with server S, respectively; N_a is a nonce; $\{\ldots\}_K$ represents symmetric key encryption with secret key K. The server issues a ticket $T_{ab} = \{A, L, K_{ab}\}_{K_b}$ for the session key K_{ab}, valid for time period specified by L.

   (a) Suppose that B above is a ticket granting service and, thus, T_{ab} is a ticket granting ticket. Propose and explain a suitable protocol exchange between A and B that will result in A obtaining a ticket for a file server C. Your solution should use (time based) authenticators to defend against replay attacks.

(b) With reference to your answer in (8a) above, discuss some of the advantages and disadvantages of using authenticators (versus challenge-response) as strategies for avoiding replay attacks.

(c) Suppose that T is a secure time service sharing secret key K_t with Authentication Server S. How might server C use T to set its (C's) clock at boot-up time?

(d) Suppose that A prefers not to synchronise her clock with T, yet wants to obtain tickets from B. Suggest a strategy that A can use to manage her skewed clock.