Hardware-Oriented Security and Trust
ECE 4156 A / ECE 6156 A
Spring 2025

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

Homework 6, 110 pts. (ECE 4156) 110 pts. (ECE 6156)
Due Friday March 7 prior to 11:55pm

Problems 2 and 3 on this homework have individual solutions per student and so no overall solution will be provided. Thus, only problem 1 on this homework has a solution below.

Problems 2 and 3 on this homework cover the RSA asymmetric encryption algorithm. You should have enough information in the RSA lecture notes and textbooks for the course to solve this homework, therefore you are **not** allowed to look for direct answers to these questions using the internet (but you may use a calculator with a modulus function). You also may **not** consult anyone else except for the professor and teaching assistant for the course. The goal is for you to find your own RSA keys and use them to encrypt and decrypt.

1) (25 pts.) Consider the Needham-Schroeder protocol as presented in the lecture notes where A is an identifier for Alice, B is an identifier for Bob, $E_A()$ is encryption with a symmetric key held by Alice, $E_B()$ is encryption with a symmetric key held by Bob, K is a symmetric key, and both N_A and N_B are nonces:

1) Alice to Trent: A, B, N_A
2) Trent to Alice: $E_A(N_A, B, K, E_B(K, A))$
3) Alice to Bob: $E_B(K, A)$
4) Bob to Alice: $E_K(N_B)$
5) Alice to Bob: $E_K(N_B-1)$

Please note that we are using **symmetric** keys! Now suppose that for "efficiency" the identifiers A and B are omitted from encryption in steps 2 and 3 of the protocol with the result as follows:

1) Alice to Trent: A, B, N_A
2) Trent to Alice: $E_A(N_A, K, E_B(K))$
3) Alice to Bob: $A, E_B(K)$
4) Bob to Alice: $E_K(N_B)$
5) Alice to Bob: $E_K(N_B-1)$

Without breaking any keys (i.e., none of the symmetric keys of others held by Trent are discovered by Mallory), is it possible for Mallory to carry out a Man-in-the-Middle (MitM) attack on the "efficient" modified protocol above? If so, show the steps in detail. If not, give

at least one clear reason why not and show some attempted steps which fail to successfully carry out a MitM attack. Some assumptions are likely to be needed for your answer; if so, please clearly state any assumption you require.

Solution 1

Yes, it is possible for Mallory to carry out a Man-in-the-Middle (MitM) attack on the "efficient" modified protocol above. It is assumed that Mallory can intercept messages between Alice and Bob and can impersonate either of them. Multiple successful MitM attacks are possible and two such scenarios are explained below.

In this first scenario Mallory initiates sessions with Bob and Alice. This MitM attack is carried out successfully because the trusted party Trent provides an encrypted message which does not include any identifier information. Mallory pretends to be Bob or Alice as necessary during communications.

1. *Mallory to Trent: M,A,R_M*
2. *Trent to Mallory: $E_M(R_M,K,E_A(K))$*
3. *Mallory (pretending to be Bob) to Alice: $B,E_A(K)$*
4. *Alice to Mallory (Alice assumes Mallory is Bob): $E_K(N_A)$*
5. *Mallory (Alice believes the message is from Bob) to Alice: $E_K(N_A-1)$*

Similarly, Mallory can pretend to be Alice while communicating with Bob.

1. *Mallory to Trent: M,B,N_M*
2. *Trent to Mallory: $E_M(R_M, K,E_B(K))$*
3. *Mallory (Bob believes the message is from Alice) to Bob: $A,E_B(K)$*
4. *Bob to Mallory (Bob assumes Mallory is Alice): $E_K(N_B)$*
5. *Mallory (Bob assumes the message is from Alice) to Bob: $E_K(N_B-1)$*

Solution 2

The solution provided above assumes that neither Alice nor Bob initiates the session. What if Alice were to initiate the session, could Mallory still carry out a Man-in-the-Middle Attack?

Yes, it is still possible for Mallory to carry out a MitM attack in this second scenario. It is assumed that Mallory can reset a connection, intercept messages and impersonate Alice / Bob.

1. *Mallory to Trent: M,B,N_{M1}*
2. *Trent to Mallory: $E_M(N_{M1},K_1,E_A(K_1))$*
3. *Mallory to Trent: M,B,N_{M2}*
4. *Trent to Mallory: $E_M(N_{M2},K_2,E_B(K_2))$*

Note that Mallory is now prepared to act if either Bob or Alice initiates a session! Let us suppose that Alice does so:

5. *Alice to Trent (intercepted by Mallory): A,B,R_A*
6. *Mallory resets the connection*
7. *Mallory (impersonating Bob) to Alice: $B,E_A(K_1)$*
8. *Alice to Bob (intercepted by Mallory): $E_{K1}(N_A)$*
9. *Mallory to Alice: $E_{K1}(N_A-1)$*

Now Mallory completes the MitM by pretending to be Alice to set up a session with Bob using the second key, K_2:

10. *Mallory (impersonating Alice) to Bob: $A,E_B(K_2)$*
11. *Bob to Alice (intercepted by Mallory): $E_{K2}(N_B)$*
12. *Mallory to Bob: $E_{K2}(N_B-1)$*

Now Mallory has access to communicate with both Alice and Bob. It is perfectly in the middle of the network.

Note that the above successful attack makes one additional assumption: after the reset and before Alice can resend her request to Trent, Mallory pretends to be Bob wanting to communicate with Alice. Alice wanted to communicate with Bob anyway and so decides to simply accept Bob's request (the request comes from Mallory) instead of reinitiating a session through Trent.

As was stated on the previous page, the main reason it is possible for Mallory to successfully carry out a MitM attack is that Trent provides an encrypted symmetric key (e.g., $E_A(K_1)$) which does not include any identity information, so Mallory can pretend to be Bob or Alice without holding Bob's secret symmetric key or Alice's secret symmetric key.