Network Security

Project 2.1

Man-in-the-middle Attack

Instructor: Shiuhpyng Shieh

TA：E-Lin Ho, Jui-Chien Jao

1. Description

In this project, you will play a role of an attacker between user Alice and bank Bob to perform the man-in-the-middle attack. To simplify the project, the following assumptions are made:

1) The connection between Alice and Bob has been successfully intercepted with ARP spoofing conducted by the attacker (you).
2) The PKI (Public Key Infrastructure) does not exist so that both the certificates of Alice and Bob may not be trusted.
3) To initiate the communication between Alice and Bob, simply send your student ID to Alice.

Based on these assumptions, you need to implement a socket program to hijack (receive→sniff/forge→forward) the network packets delivered through the connection for the eavesdropping and the content forgery purposes. That is, when Alice issues a request for her amount of money in bank to Bob, you can either sniffed her private information responded by Bob or even forge the request to make Bob leak other information wanted.

The purpose of this project is to make you understand that the encryption, even with authentication, would be useless if you don't check whether the received public key actually belongs to the person you think or not, and it would be worse if the authentication is so simple that Attacker can also generate it.

The protocol is illustrated by Fig. 1 in page 2.

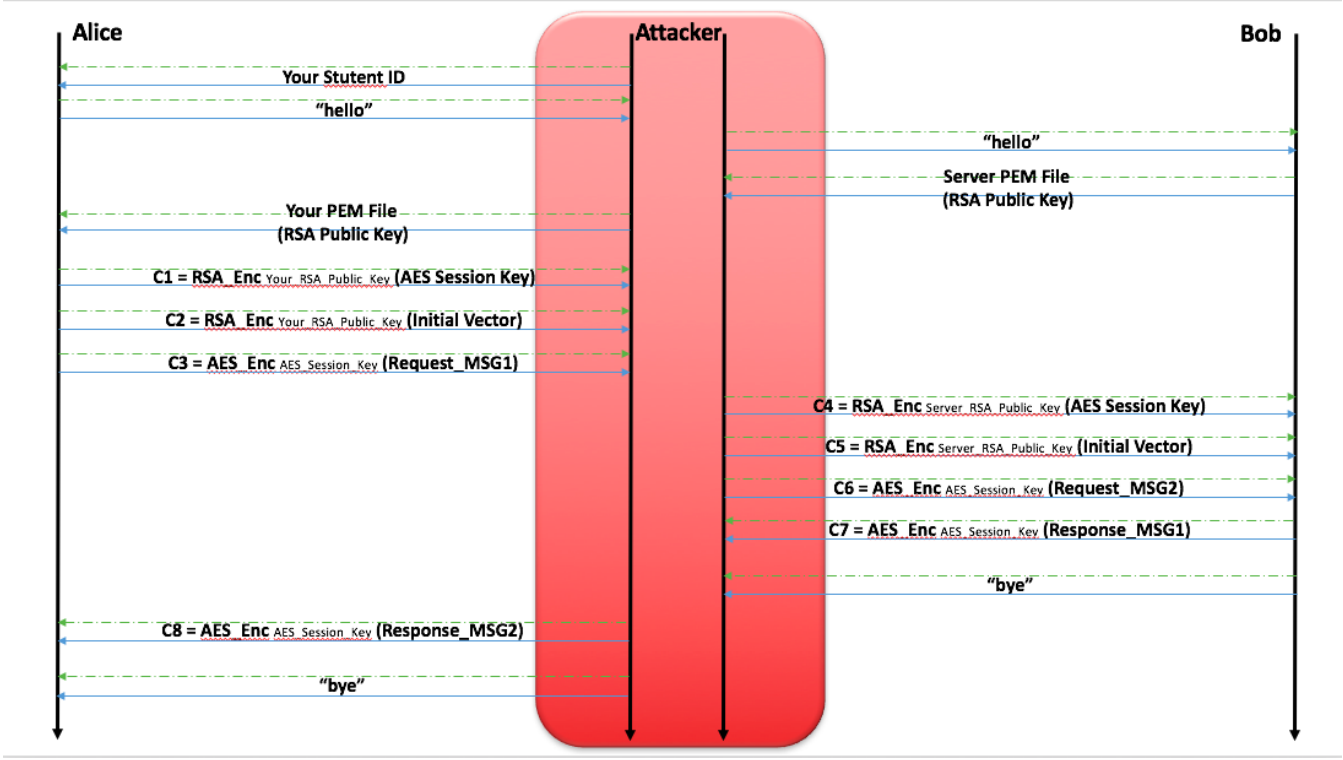

Fig. 1 The protocol of project 2.1

As shown in Fig. 1, there are two parts of the protocol. A message of your student ID delivered to Alice starts the following communications.

Their addresses are below:

Alice: "140.113.194.88:50000"

Bob: "140.113.194.88:50500"

Protocol between Alice and Attacker:

In the beginning, Alice sends a "hello" message to Attacker and Attacker sends his/her RSA public key PEM file back to Alice. Next, Alice will send the AES key and Initial Vector of CBC-mode encrypted by attacker's RSA public key back to Attacker. After that, Alice sends a request message encrypted by AES to Attacker, and the Attacker can just send the entire message to Bob or he/she can read the contents of the request message by decrypting it. After Attacker has received the response message encrypted by AES from Bob, Attacker sends the encrypted response message and a plaintext of "bye" to Alice.

Protocol between Attacker and Bob:

This protocol is almost the same as the former, just replacing the role of Alice and Attacker in the former with Attacker and Bob respectively.

2. Reminder

a) Request and Response message:

Both of the request and the response messages are JSON-format, and the kinds of items are totally the same as the other but the contents of items may be different. All the names of items will be listed in quotes (“”). In the JSON-format message, “Account_Money” means the amount of money of “Account_ID” in bank Bob. If you do not modify the request message received from Alice and send to Bob directly, you would see the amount of money of Alice in the “Account_Money” of response message, while if you edit “Account_ID” to your student ID and modify the value of “Authentication_Code” correctly, the “Account_Money” of the response message will be the amount of money of yours. The amount of money is uniquely generated from the student ID(“Account_ID”), so the result of every student is different from each other. The method of producing “Authentication_Code” has been mentioned in the class and there will be a hint in “Feedback” of response message if you send a wrong “Authentication_Code”.

b) The response message you send to Alice should be corresponded to the request message Alice sends to you.

c) Every message should be sent after the total number of bytes of it.

d) There will be a timeout setting for every connection.

e) The details of RSA and AES cryptosystem are the same as previous projects.

3. Deliverables

Each student must work individually and submit **a compress file named by your student ID, e.g., “<YOUR_STUDENT_ID.zip>”** containing:

a) The source code of your program named by your student ID.

b) A report, .txt, Word or PDF, named by your student ID includes:

- The amount of money of Alice.
- The amount of money of yours.
- What is ARP spoofing?
- The details of the way that you generate the “Authentication_Code”.
- The commands or the steps for compiling and executing your program.

If you have any question, please contact TA as soon as possible.

Any anomaly connection such DDoS will be traced for penalty.

Deadline: 2016/11/13 (Sun.) 23:59:59