Isfahan University of Technology
Information Technology Engineering- 1397
Dr. Manshaei
Homework 2: Network Security and Peer-to-Peer Networking
Deadline: Friday Aban 18th at 23:00

Please review related section of "Computer Networking" by Kurose and Ross.
We only accept the homework **delivered via lms (lms.iut.ac.ir), before the deadline**.
Any cheating will result in a 'fail' in all assignments(not just in this assignment).
Homework sessions will take place on **Sundays at 12:30, in Class 33**.
Feel free to contact TA at: j.daneshamooz@ec.iut.ac.ir.

1. Network programming:

Preliminaries:

Alise wants to order a laptop from Amazon online shop. You should provide security for this communication. There are 3 nodes in this scenario:

- Certificate Authority(CA)
- Customer(Alice)
- The on-line shop server (Amazon server)

All these nodes have a pair of asymmetric key and they should be able to carry out asymmetric cryptography function. These nodes communicate using socket connection. We suppose that in this scenario, the connection between CA and Alice and the connection between CA and Amazon server is secure.

Overall Scenario:

Certificate: Alice and Amazon server need to mutually authenticate each other and exchange a shared symmetric key using public key cryptography. For the sake of preventing impersonation (remember pizza prank), we use a certificate authority. So, Alice and Amazon server send their public key and an identifier (like a name) to the CA and get the corresponding certificate. In this process, Alice and Amazon server also get the public key of CA. *You can use X.509 as PKI standard or design a simple PKI standard by yourself and implement it.*
Key Exchange: After that, Alice initiates a socket connection to Amazon server. They both exchange their public key and verify identity of each other using the respective certificate. After that, Amazon server sends a symmetric key to Alice. The symmetric key should be encrypted with Alice's public key.
Secure Communication: Alice encrypts a message with this symmetric key using symmetric cryptography and sends the cipher to the server. Amazon server decrypts the cipher and prints the message on console.

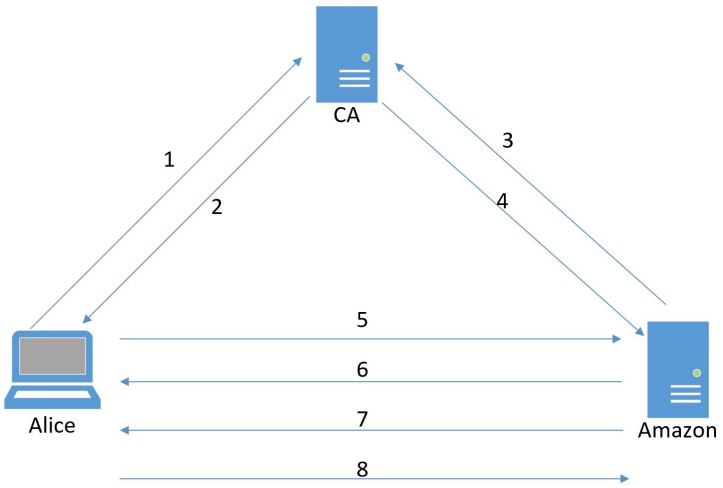

Figure 1: Simple visual scenario

1) Alice requests for certificate
2) CA sends corresponding certificate to Alice and CA's public key
3) Amazon server requests for certificate
4) CA sends corresponding certificate to Amazon server and CA's public key
5 and 6)Alice and Amazon server share public key and authenticate each other
7)Amazon server sends symmetric key to Alice(the key should be encrypted with Alice's public key)
8)Alice encrypts her message with symmetric key, then sends the cipher to Amazon server

Non-Functional Requirements:

- The program should be written by C, C++, Java or Python.
- You should use **RSA(key length = 1024)** as asymmetric cryptography algorithm, **AES** as symmetric cryptography algorithm.

Deliverables:

- Source code of client(Alice), server(Amazon) and certificate authority server
- A document that explain everything briefly

Please deliver all files in a single zip file. Include your overall design, logic of your program and data flow in your document. Explain new ideas or changes you considered.

Bonus

- Adding integrity to whole or a part of communication
- Preventing replay attack (e.g, using nonce)
- CA and Amazon server support more than one connection (thread programming)
- Nodes generate public key and request certificate only once(saving RSA keys, certificate and public key of CA in a file)

2. SSL and IPSec are both designed to provide security over the network.

a) What are the significant similarities and differences between these two protocols?

b) What are the primary advantages of IPSec over SSL?

3. Suppose that we modify WEP so that it encrypts each packet using RC4 with the key K, where K is the same key that is used for authentication. Is this a good idea? Why or why not?

4. Provide a filter table and a connection table for a stateful firewall that is as restrictive as possible but accomplishes the following:

a) Allows all internal users to establish HTTP connection

b) Allows remote SSH to an internal server at 176.101.51.123

c) Allows all external users to surf the company web at 176.101.51.110

5. Suppose Alice and Bob are communicating over an SSL session. Suppose an attacker, who does not have any of the shared keys, inserts a bogus TCP segment into a packet stream with correct TCP checksum and sequence numbers (and correct IP addresses and port numbers). Will SSL at the receiving side accept the bogus packet and pass the payload to the receiving application? Why or why not?

6. Suppose Bob joins a BitTorrent torrent, but he does not want to upload any data to any other peers (so called free-riding).

a) Bob claims that he can receive a complete copy of the file that is shared by the swarm. Is Bob's claim possible? Why or why not?

b) Bob further claims that he can further make his âĂIJfree-ridingâĂİ more efficient by using a collection of multiple computers (with distinct IP addresses) in the computer lab in his department. How can he do that?

7. Suppose that a new Peer 9 wants to join the following DHT. Peer 9 initially only knows Peer 3's IP address. What steps should be taken by Peer 9?