Hacettepe University Computer Enginnering Department

BBM 465 Information Security Lab.

Experiment 5

Due Date: 08/01/2021
Subject: Security Authentication System
Programming Language: Java

Introduction

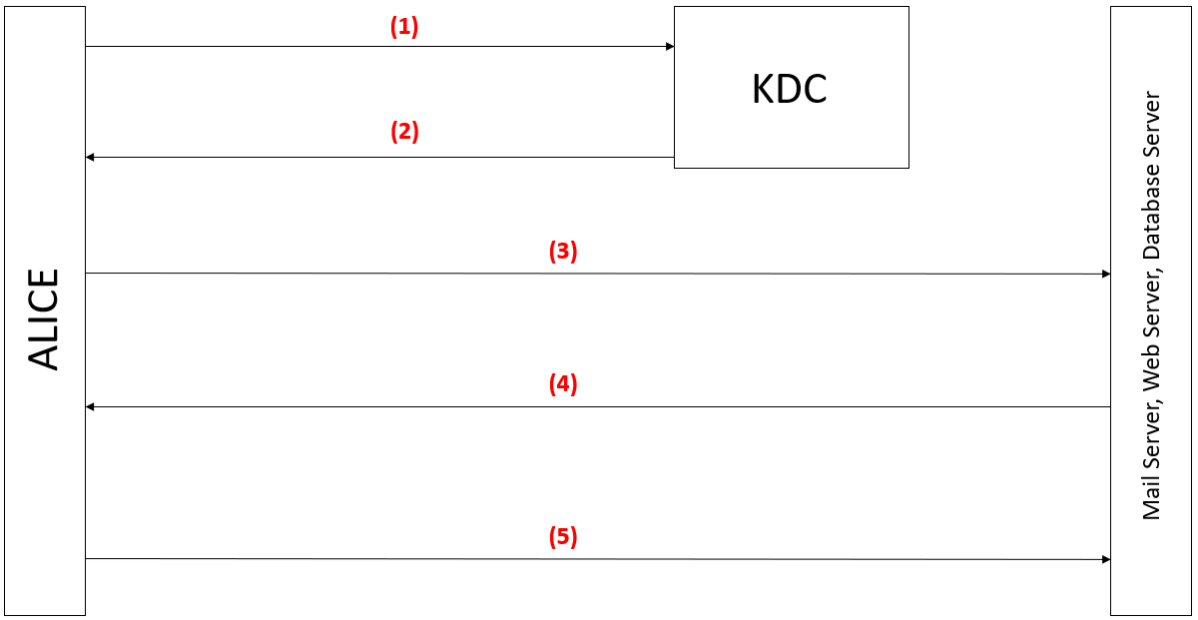
In this experiment; you are expected to design an authentication system like Needham-Schroeder protocol with public-private key cryptosystem. For this scenario, you are expected to create five network elements:

- KDC (Key Distribution Center) Server
- Mail Server
- Web Server
- Database Server
- A Client Program for the user “Alice”

All these programs will communicate through client-server socket communication. Network ports for KDC, Mail Server, Web Server and Database Server must be 3000, 3001, 3002, 3003 respectively.

The definitions and abbreviations that will be used throughout the assignment paper are as follows:

- KDC = KDC Server,
- “Alice” = ID of Alice
- “Mail”|“Web”|“Database” = IDs of Mail,Web,Database Server
- Pass = Password of Alice
- P_A = Alice’s Public Key
- R_A = Alice’s Private Key
- P_{KDC} = KDC’s Public Key
- R_{KDC} = KDC’s Private Key
- P_{Mail} = Mail Server’s Public Key
- R_{Mail} = Mail Server’s Private Key
- P_{Web} = Web Server’s Public Key
- R_{Web} = Web Server’s Private Key
- P_{DB} = Database Server’s Public Key
- R_{DB} = Database Server’s Private Key
- K_A = Session Key Produced by KDC for Alice
- TS_i = i^{th} timestamp value
- N_i = i^{th} nonce value
- Ticket = Ticket message



In the specific scenario above, please suppose that Alice is trying to communicate with the Mail Server. This scheme is also valid for the scenarios in which, whenever Alice tries to communicate with the Web Server or the Database Server. In the above scenario, message contents and their explanations are as follows:

1. **Alice, P_{KDC}("Alice", Pass, "Mail", TS1) ->** Explanation: Alice sends KDC her id with a content encrypted with the public key of KDC. The encrypted message includes her id, her password, id of Mail Server and a timestamp. KDC decrypts Alice message with its own private key. Then, in the second message, KDC sends a message and ticket information back to Alice.
2. **P_A(K_A, "Mail", TS2), Ticket = P_{Mail} ("Alice", "Mail", TS2, K_A) ->** Explanation: KDC's message has two parts. First part is encrpyted with public key of Alice and includes session key (K_A), ID of Mail Server and a timestamp. Second part contains a ticket encrypted with public key of Mail Server and includes IDs of Alice and mail Server, same timestamp and session key values. Alice decrypts the first part of message with her own private key and gets the session key and also stores the ticket.
3. **Alice**, **Ticket**, **K_A(N_1) ->** Explanation: Alice sends her id, the ticket, and a nonce value encrypted with the session key to the Mail Server. Mail Server decrypts ticket with its own private key and learns the session key and verifies the correctness of the information in the ticket. Mail Server also decrypts the encrypted N_1value with the session key.
4. **K_A (N_1+1, N_2) ->** Explanation: Mail Server sends N_1+1 and N_2 values encrypted with the session key. Alice decrypts the message from Mail Server with session key and verifies the correctness of N_1+1 value.
5. **K_A (N_2+1) ->** Explanation: If N_1+1 value is correct, Alice sends back a message to the Mail server. Message is encrypted with the session key and includes N_2+1 value.

Implementation Details

- You are expected to implement this assignment in Java by using socket programming.
- Additionally, all of KDC, Alice, Mail Server, Web Server and Database Server programs must also create a log file having names "KDC_Log.txt", "Alice_Log.txt", "Mail_Log.txt", "Web_Log.txt", "Database_Log.txt", which show a log of operations and messages.

- Each log file belongs to the client program and server programs must include every detail whenever client or server processing or sending the information with a timestamp information. The sample log files for the above scenario will be posted later on Piazza.
- When KDC is executed, it checks whether public-private keys exist for Alice and other servers. If they do not exist, KDC creates five public/private key pairs for Mail, Web, Database servers, Alice, and KDC itself. KDC also creates a random password with alphabet letter and numeric characters. KDC saves SHA1 hash of the password (in base64 format) in a file named "passwd". KDC also prints the plaintext password to its log file.
- For each public key, KDC creates a public key certificate in X.509 format using Keytool [1,2]. These public key certificates should be signed with KDC's private key (Thus, KDC's certificate is a self-signed certificate). All certificates are stored in a directory named "cert". The programs in the system will use these certificates to learn public keys of each other. Additionally, private keys should be stored in base64 format as separate files in a directory named "keys".
- When the client program (Alice) is executed, a password is requested from the user. Then, a server name is requested. In this step, the user should enter "Mail", "Web" or "Database", otherwise the program should request the choice again. Then, the client connects to KDC and gets the session key and ticket as described above. After getting the ticket, the client connects to the requested server ("Mail", "Web" or "Database") and does the remaining authentication procedures above. All these operations must be logged by the programs.

Policy

All work on assignments must be done with your own group unless stated otherwise. You are encouraged to discuss with your classmates about the given assignments, but these discussions should be carried out in an abstract way. That is, discussions related to a particular solution to a specific problem (either in actual code or in the pseudocode) will not be tolerated. In short, turning in someone else's work (from internet), in whole or in part, as your own will be considered as a violation of academic integrity. Please note that the former condition also holds for the material found on the web as everything on the web has been written by someone else.

Notes:

- You will make your submissions via submit system (https://submit.cs.hacettepe.edu.tr)
- You can ask questions about the experiment via Piazza group (piazza.com/hacettepe.edu.tr/fall2020/bbm465).

<Group number>.zip
|--- code
|---*.java

References

[1] Java keytool: https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html

[2] Package javax.crypto : https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html