Group 1

Berkay Kebeci	21102706
Selçuk Gülcan	21101231

CS470 Project Proposal

We would like to implement one-to-one communication system with password authentication. There will be no chat server, clients will communicate each other directly. Here are description of some abbreviations used in protocol diagrams.

C_A = Client A (port number 5001)
C_B = Client B (port number 5002)
AS = Authentication Server (port number 7777)
TGS = Ticket Granting Server (port number 7778)

K_{KDC} = Symmetric key shared by AS and TGS
K_A = Password of client A (Client A and AS know this information)
K_B = Password of client B
K_{AB} = Symmetric key shared by client A and B and it is used for communication
S_A = Session key of client A
TGT = Ticket granting ticket containing S_A and id_A ($K_{KDC}\{S_A,id_A\}$)

Note: We consider that id of clients are port numbers. That is, id_A=5001 and id_B=5002.

Login Protocol

1. Client A sends his id and hashed password to AS.
2. AS checks this hash value with its own hash value of client A password.
3. AS sends S_A and TGT to client A after encrypting them over K_A .

Connection Protocol

1. Client A sends his id, id of client B,TGT (he received it from AS) and current timestamp encrypted under S_A to TGS
2. TGS decrypts TGT and checks if id_A and S_A are matched with TGT.
3. TGS sends $S_A\{id_B,K_{AB}, K_B\{id_A,K_{AB}\} \}$ ($K_B\{id,K_{AB}\}$ id the ticket of B)

Communication

1. Client A sends $K_B\{id_A,K_{AB}\}$, $K_{AB}\{timestamp\}$ to client B.
2. Client B sends $K_{AB}\{timestamp+1\}$

Now, client A and client B has K_{AB}. Then can communicate by using K_{AB}.

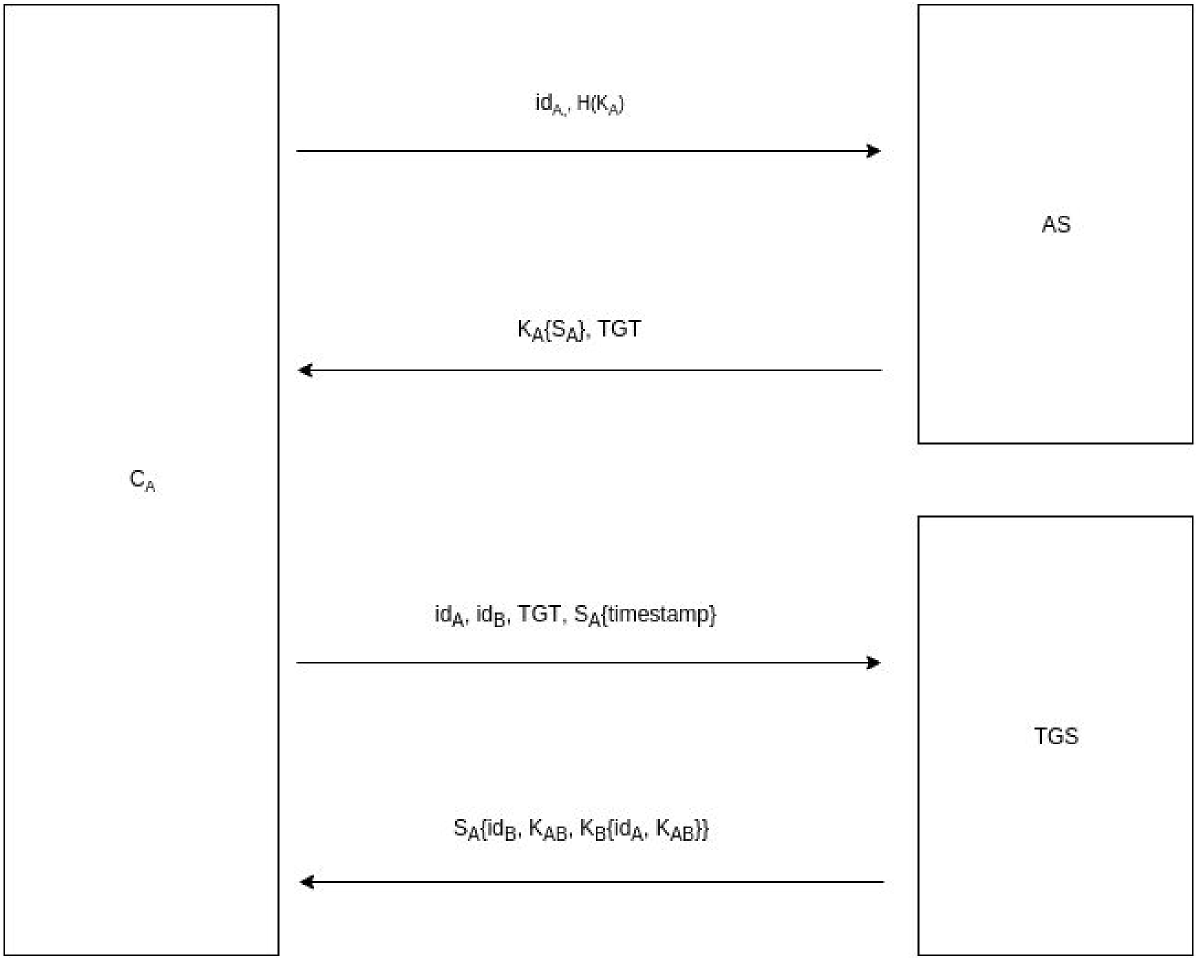
$id_{A,}$, $H(K_A)$
AS
$K_A\{S_A\}$, TGT
C_A
id_A, id_B, TGT, $S_A\{timestamp\}$
TGS
$S_A\{id_B, K_{AB}, K_B\{id_A, K_{AB}\}\}$

Figure 1 - Login and Connection Protocol

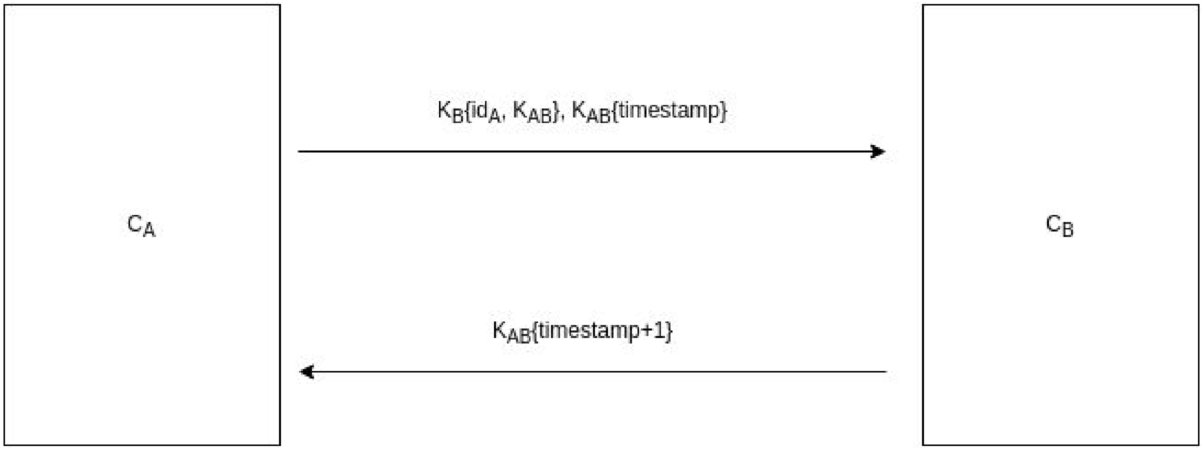

Figure 2 - Communication