2019-2020

Four in a Row

Cybersecurity Project Documentation

Nicola Barsanti Gianluca Tumminelli

Contents

Software Description **3**

Service Architecture **4**
Network Design 4
Security Design 4

Protocol Architecture **5**
The cheater problem 6

Protocol Analysis **8**
Certificate Protocol 9
Login Protocol 10
Logout Protocol 12
User List Protocol 13
Rank List Protocol 14
Challenge Protocol 15
Withdraw Protocol 18
Move Protocol 18
Chat Protocol 20
Disconnect Protocol 21

UML Diagram **22**

User Manual 23

Software Description

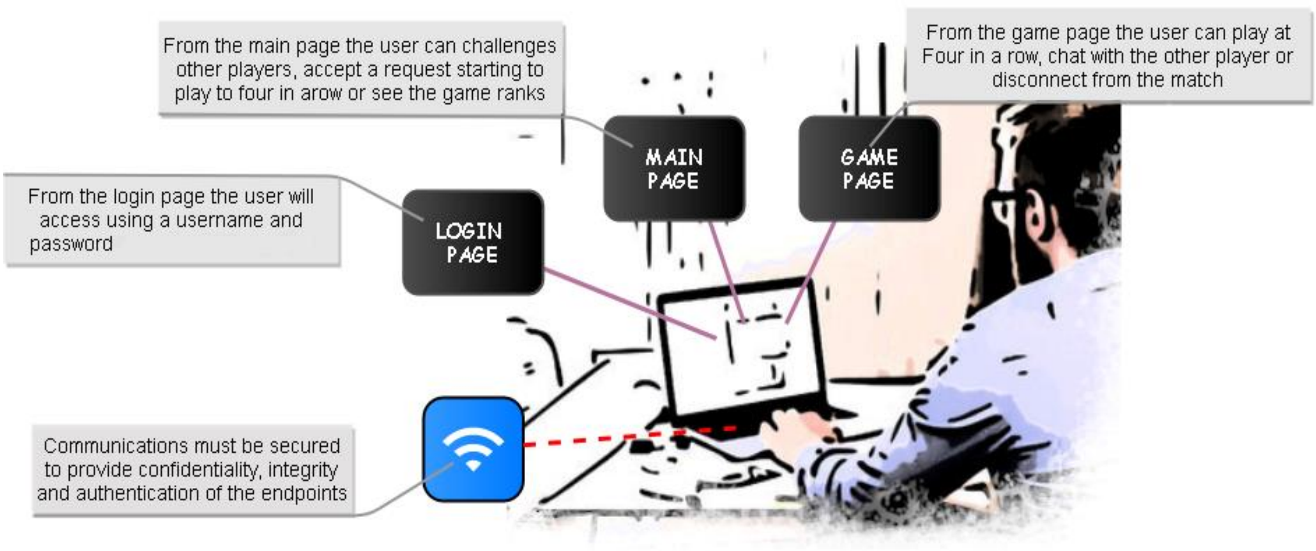
This paper will document the development of the application **Four in a Row Online** which is a multiplayer online-only videogame accessed by a prompt interface.

Each user registered into the service can access the application by a *Login Page* giving a username and a valid password.

Then, from the *Main Page,* he can see all the active users, his pending challenge requests and a rank where will be showed the results of all the users of the service. He can also accept or reject one of the challenge requests or, choosing an available user, challenge him.

The implemented game is the classic *Four in a Row*, the game is based on a shared Gameboard in which the first player who puts four token in a row wins. The game is divided in rounds of 15 seconds and each time only one player can choose a column and put it a token. During a match the players can also talk to each other using a chat or disconnect from the match returning to the *Main Page*.

The confidential information of the users must be protected from be stolen by malicious attackers. Each message authenticity must be proved and the service must be robust to malicious and non-malicious threads.



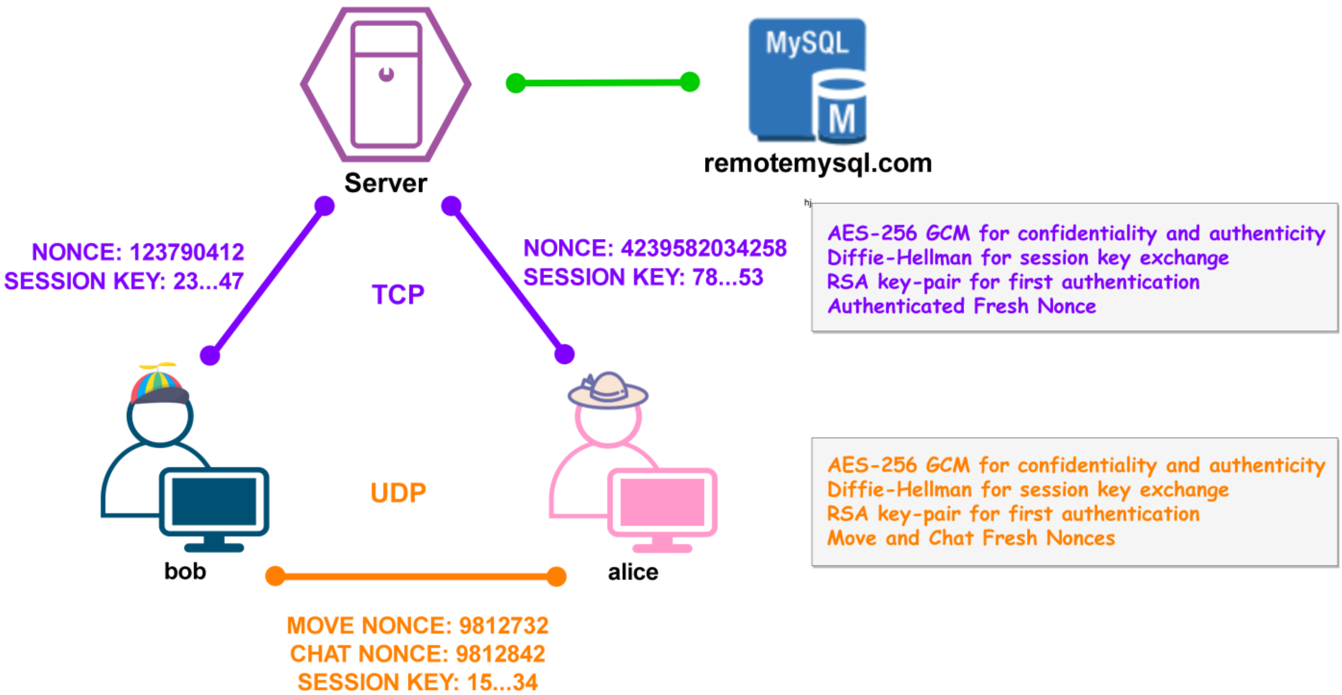
Service Architecture

Network Design

The application is delivered by an hybrid communication approach. Each user will have a p2p communication implemented in UDP, to play a match with other players and client-server communication implemented in TCP, to log into the service and perform all the available operations.

Security Design

Each communication channel will be protected by an AES-256 session key which will be used to encrypt confidential information and authenticate the messages. All the users have also a RSA key-pair to authenticate themselves to the service and to other users until the generation of a channel session keys using the Diffie-Hellman key-establishment protocol. To guarantee the freshness of the messages each message, except the first one to request the server PEM certificate, will have a fresh nonce authorized by the server and it will be incremented after every completed request to guarantee protection from reply-attack.



Protocol Architecture

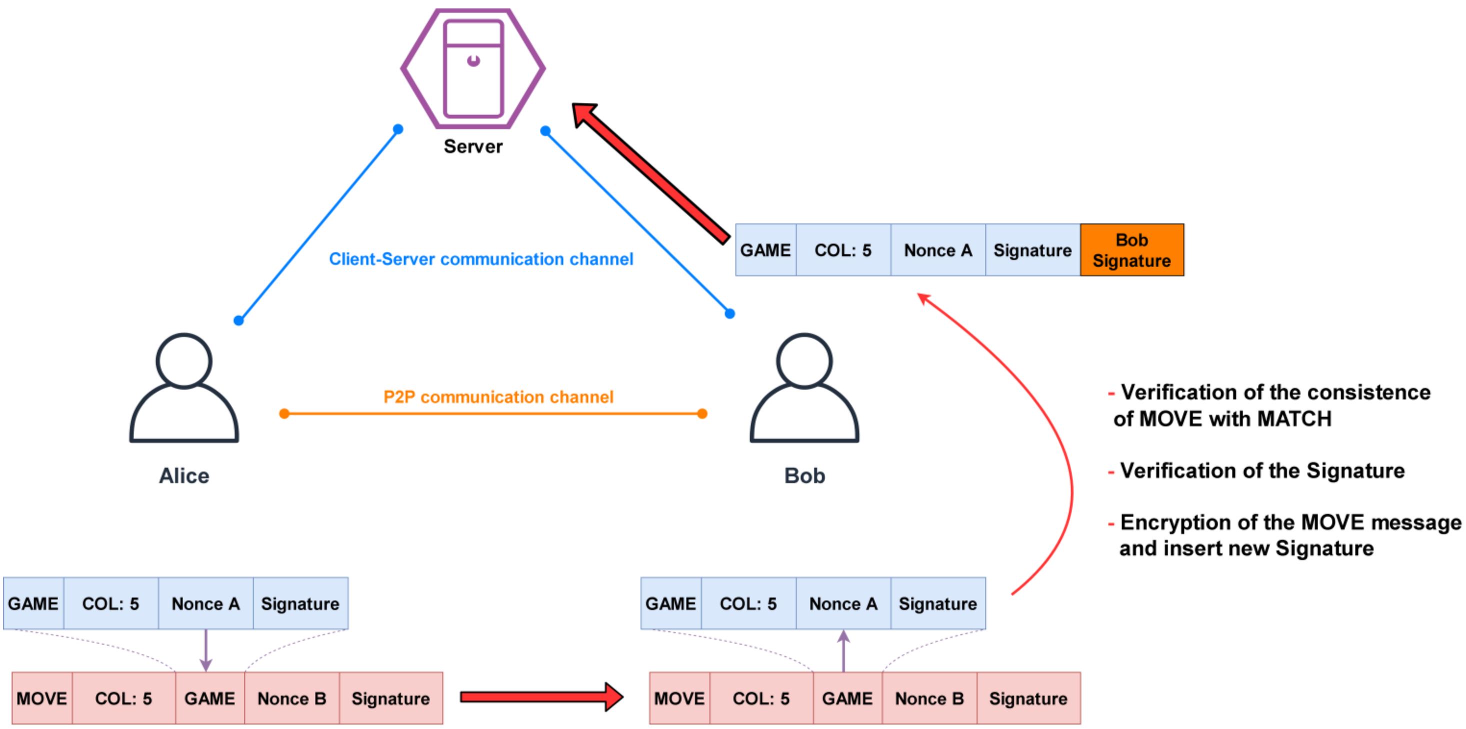
The service is based on a mono-threaded server in which by a shrewd implementation we gives the impression of a multi-threaded service. In particular the communication exchanges must be designed to be in a request-response way with no dead-time spent by the server to attempt some responses to complete an interaction(otherwise meanwhile the server is waiting all the users will wait too generating delays in the requests commitment). To perform its operation we have designed 11 possible types of request to the server:

- **CERTIFICATE**: *request the server certificate and an authorized nonce*
- **KEY EXCHANGE**: *create a session key to communicate privately*
- **LOGIN**: *access the service giving a username*
- **LOGOUT**: *leave the service*
- **USER LIST**: *request the connected users of the service*
- **RANK LIST**: *request the game ranking*
- **CHALLENGE**: *match a connected user*
- **ACCEPT**: *accept a received user challenge*
- **REJECT**: *reject a received user challenge*
- **GAME PARAM:** *gives the parameters needed to start a match*
- **DISCONNECT**: *leave a match*

And 3 possible types of message that can be exchanged by the users during the playing of a match:

- **KEY EXCHANGE**: *create a session key to communicate privately*
- **MOVE**: *send the next game move of the user*
- **CHAT**: *send a message from the users during a match*

The game is played in a distinct environment which hides to the server the progress of the match which it has no control. For this reason the users could cheat attributing to themselves the victory of the game and the service has no information to detect who is cheating and what is the correct result of the game risking of invalidating the ranking table by incorrect results. To remove this problem we have to give some form of control to the server and to do so we have introduced another message(GAME) sent to the server during the play of a match, the message will contain the chosen move and a signature made by the user which has sent the move. The message is then sent to the other client attached to the MOVE message. The client is in charge to verify the consistence of the GAME message and then send it to the server which is now able to know the match progress and automatically detect its ending and identify the winner. In our design the column chosen by the gamer is hidden, for coherence we have decided to encrypt and insert a new signature on the message to the server.



Protocol Analysis

In the following section there will be described in detail the exchange of the application messages and their structure. We have designed four extra postulates to manage particular situations not covered by the base postulates. During all the analysis with the symbol H we mean an HMAC obtained by some message fields specified with the subscript notation. During the ban analysis we will consider it equivalent to the encryption of all the included fields.

Certificate Postulate

We need a postulate to link the receive of a server authorized certificate to the obtaining of a valid user public key.

$$\frac{\xmapsto{K_q} S, \{H_{\xmapsto{K_q} Q}\}_{K_{ca}^{-1}}, \#(N), \{H_{all}\}_{K_q^{-1}}}{P \mid\equiv \xmapsto{K_q} Q, P \mid\equiv Q \mid\equiv \xmapsto{K_q} Q}$$

Signature Postulate

To simplify the BAN Analysis we have made a simple postulate to link the presence of a signature of all the fields of the message to their trustability.

$$\frac{P \mid\equiv \xmapsto{k} Q, P \triangleleft X, \{H_{all}\}_k}{P \mid\equiv Q \mid\sim X}$$

$$\frac{P \mid\equiv P \xleftrightarrow{k} Q, P \triangleleft X, \{H_{all}\}_K}{P \mid\equiv Q \mid\sim X}$$

Diffie-Hellman Postulates

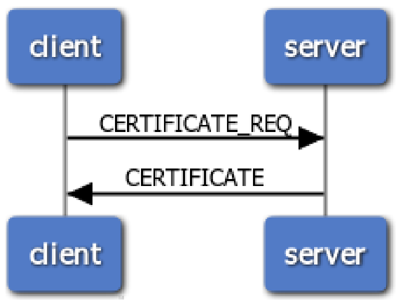
We need a postulate to link the possession of two Diffie-Hellman parameters to the generation of a shared session key. To simplify the analysis we consider the message and the key the two components to be shared by the two parts independently from what they really are(key,messages)

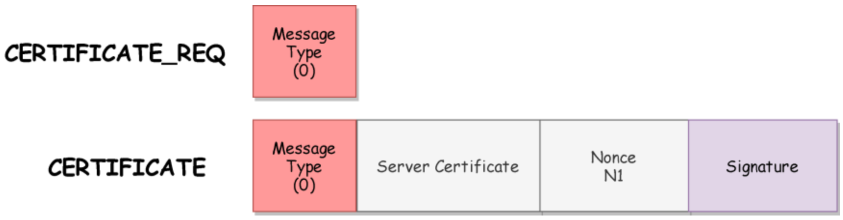
$$\frac{P \mid\equiv D_1, P \mid\equiv D_2}{P \mid\equiv A \xleftrightarrow{K_{AB}} B}$$

We need a postulate to link the freshness of the Diffie-Hellman parameters to the freshness of the shared session key

$$\frac{P \mid\equiv \#(D_1), P \mid\equiv \#(D_2)}{P \mid\equiv \#(P \xleftrightarrow{K_{pq}} Q)}$$

The protocol is used during the client initialization to obtain the server certificate and an authenticated fresh nonce. It is designed to be the first protocol which the clients will execute, as a result of that we have decided to use it also to give the first nonce that the clients will use to generate verifiable fresh information to perform their requests. In this way we prevent randomly chosen nonces susceptible to be a vulnerability for replay attack. The message doesn't require any kind of protection, this is the reason why all the fields are not encrypted and no signature is applied on the request message.





BAN Logic Analysis

Real Protocol

$$M_1 \quad C \rightarrow S: \; M$$
$$M_2 \quad S \rightarrow C: \; M, (C_s, \{H_{C_s}\}_{K_{ca}^{-1}}), N_1, \{H_{all}\}_{K_s^{-1}}$$

Goals

$$C \mid\equiv \xmapsto{K_s} S$$
$$C \mid\equiv S \mid\equiv \xmapsto{K_s} S$$

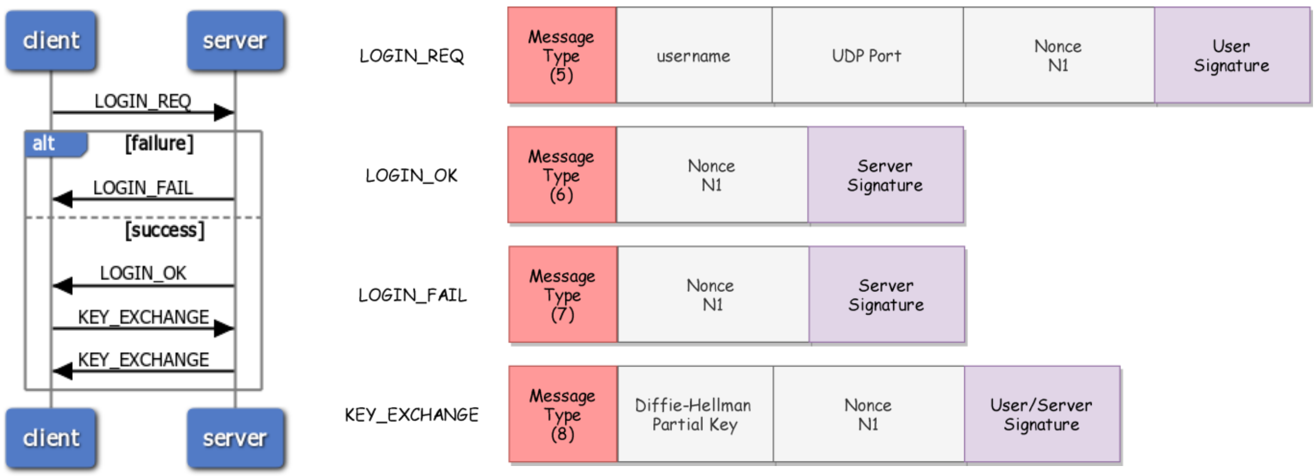
Ideal Protocol

$$M_2 \quad S \rightarrow C : \xmapsto{K_s} S, \{H_{\xmapsto{K_s} S}\}_{K_{ca}^{-1}}, \#(N_1), \{H_{all}\}_{K_s^{-1}}$$

Analysis

M2	$\dfrac{C \triangleleft (\xmapsto{K_S} S, \{H_{\xmapsto{K_s} S}\}_{K_s^{-1}}), \#N_1, \{H_{all}\}_{K_s^{-1}}}{\boxed{C \mid\equiv \xmapsto{K_s} S}, \boxed{C \mid\equiv S \mid\equiv \xmapsto{K_s} S}}$	The client has received the server certificate which is validated by the CA. Moreover the message is fresh due to the nonce field and it contains a signature made by the server RSA private key. We can apply the **certificate postulate** to derive that the certificate belongs to the server

The protocol is used by the clients to access to the application. The clients have to give a proof of their authenticity by sending a fresh message containing a signature made by their private RSA key. If the server doesn't recognize a user the protocol will end with a LOGIN_FAIL message. Otherwise the client and server will proceed with the creation of a session key generated by the Diffie-Hellman key-generation algorithm.



BAN Logic Analysis

Real Protocol

$$M_1 \quad C \rightarrow S: \; M, U, P, N_1, \{H_{all}\}_{K_c^{-1}}$$
$$M_2 \quad S \rightarrow C: \; M, N_1, \{H_{all}\}_{K_s^{-1}}$$
$$M_3 \quad C \rightarrow S: \; M, D_1, N_1, \{H_{all}\}_{K_c^{-1}}$$
$$M_4 \quad S \rightarrow C: \; M, D_2, N_1, \{H_{all}\}_{K_s^{-1}}$$

Ideal Protocol

$$M_1 \quad C \rightarrow S: \; M, \#(N_1), \{H_{all}\}_{K_c^{-1}}$$
$$M_2 \quad S \rightarrow C: \; M, \#(N_1), \{H_{all}\}_{K_s^{-1}}$$
$$M_3 \quad C \rightarrow S: \; M, \#(D_1, N_1), \{H_{all}\}_{K_c^{-1}}$$
$$M_4 \quad S \rightarrow C: \; M, \#(D_2, N_1), \{H_{all}\}_{K_s^{-1}}$$

Goals

$$C \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S \qquad C \mid\equiv S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S$$
$$S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} B \qquad S \mid\equiv C \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S$$
$$S \mid\equiv C \mid\equiv U, P$$
$$C \mid\equiv S \mid\equiv N_1$$

Assumptions

$$C \mid\equiv \overset{K_s}{\mapsto} S \qquad C \mid\equiv S \mid\equiv \overset{K_s}{\mapsto} S$$
$$S \mid\equiv \overset{K_c}{\mapsto} C \qquad S \mid\equiv C \mid\equiv \overset{K_c}{\mapsto} C$$

Analysis

M1

$$\frac{S \mid\equiv \overset{K_c}{\mapsto} C, \; S \triangleleft \{H_{all}\}_{K_c^{-1}}}{S \mid\equiv C \mid\sim (U, P, \#(N_1))}$$

The server has received a message containing a signature made by all the fields with the client private RSA key. We can apply the **signature postulate** to derive that the server will believes that the client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the server will believes that only the client could have sent that message

$$\frac{S \mid\equiv \#(N_1), \; S \mid\equiv C \mid\sim (U, P, N_1)}{\boxed{S \mid\equiv C \mid\equiv U, P}}$$

M2

$$\frac{C \mid\equiv \overset{K_s}{\longmapsto} S, C \triangleleft \{H_{all}\}_{K_s^{-1}}}{C \mid\equiv S \mid\sim (\#(N_1))}$$

The client has received a message containing a signature made by all the fields with the client private RSA key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message

$$\frac{C \mid\equiv \#(N_1), C \mid\equiv S \mid\sim N_1}{\boxed{C \mid\equiv S \mid\equiv N_1}}$$

M3

$$\frac{S \mid\equiv \overset{K_c}{\longmapsto} C, S \triangleleft \{H_{all}\}_{K_c^{-1}}}{S \mid\equiv C \mid\sim \#(D_1, N_1)}$$

The server has received a message containing a signature made by all the fields with the client private RSA key. We can apply the **signature postulate** to derive that the server will believes that the client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the server will believes that only the client could have sent that message

$$\frac{S \mid\equiv \#(D_1, N_1), S \mid\equiv C \mid\sim (D_1, N_1)}{S \mid\equiv C \mid\equiv D_1}$$

M4

$$\frac{C \mid\equiv \overset{K_s}{\longmapsto} S, C \triangleleft \{H_{all}\}_{K_s^{-1}}}{C \mid\equiv S \mid\sim \#(D_2, N_1)}$$

The client has received an HMAC encrypted by the server certificate. We can apply the **second message meaning postulate** to derive that it believes the message is sent by the server

The received HMAC contains a fresh timestamp, so it is fresh and we can apply the **nonce verification postulate** to derivate that the client believes that only the server could have sent the message

$$\frac{C \mid\equiv \#(D_2, N_1), C \mid\equiv S \mid\sim (D_2, N_1)}{C \mid\equiv S \mid\equiv D_2}$$

$$\frac{C \mid\equiv D_1, C \mid\equiv S \mid\equiv D_2}{\boxed{C \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S}}$$

We have the two Diffie-hellman components, we can use the **first Diffie-Hellman postulate** to derive that the client has generate the shared session key

We have almost one fresh Diffie-Hellman partial key, we can use the **second Diffie-Hellman postulate** to derive that the shared key is unique and believing to that session

$$\frac{C \mid\equiv \#(D_1), C \mid\equiv S \mid\equiv D_2}{\boxed{C \mid\equiv S \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S)}}$$

$$\frac{S \mid\equiv D_2, S \mid\equiv C \mid\equiv D_1}{\boxed{S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S}}$$

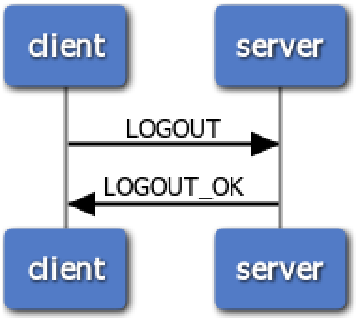
We have the two Diffie-hellman components, we can use the **first Diffie-Hellman postulate** to derive that the client has generate the shared session key

We have almost one fresh Diffie-Hellman partial key, we can use the **second Diffie-Hellman postulate** to derive that the shared key is unique and believing to that session

$$\frac{S \mid\equiv \#(D_2), S \mid\equiv C \mid\equiv D_1}{\boxed{S \mid\equiv C \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S)}}$$

Logout Protocol

The protocol will be used by the clients to quit from the application. The messages requires only authenticity and protection to reply attack so they have a signature made by AES256 GCM based on a fresh nonce.



LOGOUT	Message Type (10)	Nonce N1	AES Signature
LOGOUT_OK	Message Type (11)	Nonce N1	AES Signature

BAN Logic Analysis

Real Protocol

$$M_1 \quad C \rightarrow S: \; M, N_1, \{H_{all}\}_{K}cs$$
$$M_2 \quad S \rightarrow C: \; M, N_1, \{H_{all}\}_{K}cs$$

Ideal Protocol

$$M_1 \quad C \rightarrow S: \; \#(N_1), \{H_{all}\}_{K}cs$$
$$M_2 \quad S \rightarrow C: \; \#(N_1), \{H_{all}\}_{K}cs$$

Goals

$$S \mid\equiv C \mid\equiv N_1$$
$$C \mid\equiv S \mid\equiv N_1$$

Assumptions

$$C \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S$$
$$S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S$$

Analysis

M1

$$\frac{S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S, S \triangleleft \{H_{all}\}_{K_{cs}}}{S \mid\equiv C \mid\sim N_1}$$

The server has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the server will believes that the client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the server will believes that only the client could have sent that message

$$\frac{S \mid\equiv \#(N_1), S \mid\equiv C \mid\sim \{N_1\}}{\boxed{S \mid\equiv C \mid\equiv N_1}}$$

M2

$$\frac{C \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S, C \triangleleft \{H_{all}\}_{K_{cs}}}{C \mid\equiv S \mid\sim N_1}$$

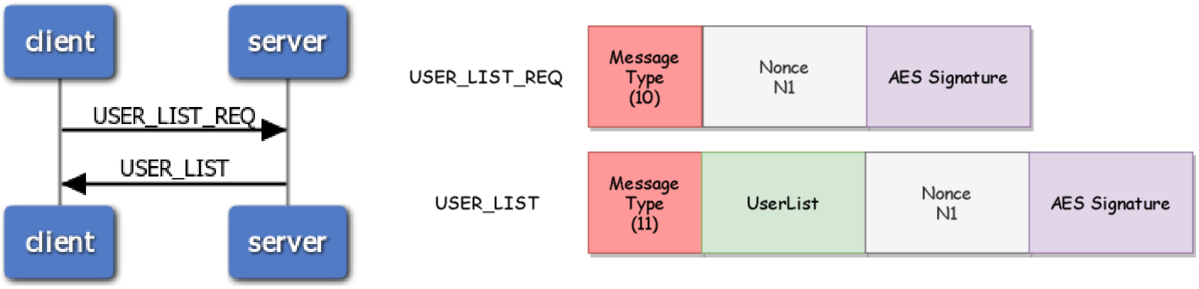
The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message

$$\frac{C \mid\equiv \#(N_1), C \mid\equiv S \mid\sim N_1}{\boxed{C \mid\equiv S \mid\equiv N_1}}$$

User List Protocol

The protocol will be used from the clients to obtain a list of the users currently available to be challenged. The user list requires to be confidential and it will be encrypted. All the other fields requires only authentication and will be protected by a signature based on a fresh nonce and made by AES256 GCM.



BAN Logic Analysis

Real Protocol

$M_1 \quad C \rightarrow S: \ M, N_1, \{H_{all}\}_{K_{cs}}$

$M_2 \quad S \rightarrow C: \ M, N_1, \{L, H_{all}\}_{K_{cs}}$

Ideal Protocol

$M_1 \quad C \rightarrow S: \ N_1, \{H_{all}\}_{K_{cs}}$

$M_2 \quad S \rightarrow C: \ N_1, \{L, H_{all}\}_{K_{cs}}$

Goals

$C \mid\equiv S \mid\equiv L$

$S \mid\equiv C \mid\equiv N_1$

Assumptions

$C \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S$

$S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S$

Analysis

M1

$$\frac{S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S, S \triangleleft \{N_1, H_{all}\}_{K_{cs}}}{S \mid\equiv C \mid\sim \{N_1, H_{all}\}}$$

The server has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the server will believes that the client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the server will believes that only the client could have sent that message

$$\frac{S \mid\equiv \#(C \overset{K_{cs}}{\longleftrightarrow} S), S \mid\equiv C \mid\sim N_1}{\boxed{S \mid\equiv C \mid\equiv N_1}}$$

M2

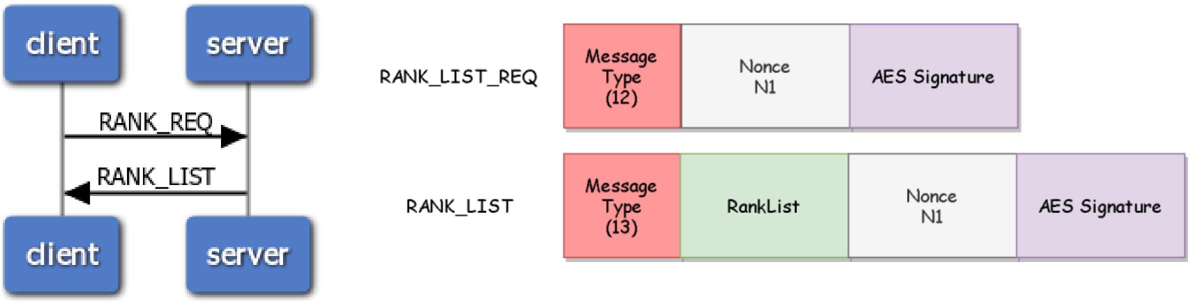
$$\frac{C \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S, C \triangleleft \{H_{all}\}_{K_{cs}}}{C \mid\equiv S \mid\sim (N_1, L)}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message

$$\frac{C \mid\equiv \#(N_1), C \mid\equiv S \mid\sim (N_1, L)}{\boxed{C \mid\equiv S \mid\equiv L}}$$

The protocol will be used from the clients to obtain a list of the users game statistics. The rank list requires to be confidential and it will be encrypted. All the other fields requires only authentication and will be protected by a signature based on a fresh nonce and made by AES256 GCM.



BAN Logic Analysis

Real Protocol

$M_1 \quad C \rightarrow S: \; M, N_1, \{H_{all}\}_{K_{cs}}$

$M_2 \quad S \rightarrow C: \; M, N_1, \{L, H_{all}\}_{K_{cs}}$

Ideal Protocol

$M_1 \quad C \rightarrow S: \; N_1, \{H_{all}\}_{K_{cs}}$

$M_2 \quad S \rightarrow C: \; N_1, \{L, H_{all}\}_{K_{cs}}$

Goals

$C \mid\equiv S \mid\equiv L$

$S \mid\equiv C \mid\equiv N_1$

Assumptions

$C \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S$

$S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S$

Analysis

M1

$$\frac{S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S, \; S \triangleleft \{N_1, H_{all}\}_{K_{cs}}}{S \mid\equiv C \mid\sim \{N_1, H_{all}\}}$$

The server has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the server will believes that the client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the server will believes that only the client could have sent that message

$$\frac{S \mid\equiv \#(C \overset{K_{cs}}{\longleftrightarrow} S), \; S \mid\equiv C \mid\sim N_1}{\boxed{S \mid\equiv C \mid\equiv N_1}}$$

M2

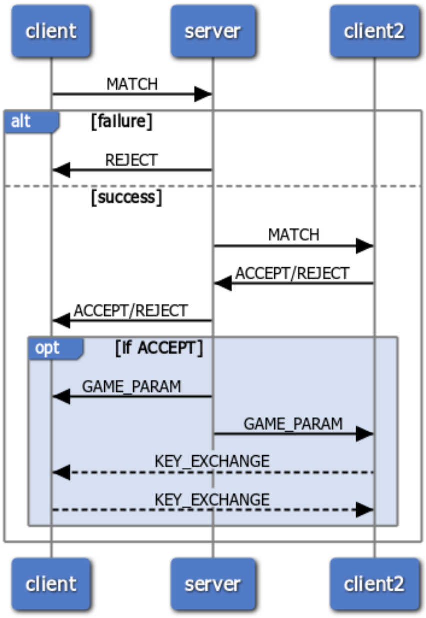
$$\frac{C \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S, \; C \triangleleft \{H_{all}\}_{K_{cs}}}{C \mid\equiv S \mid\sim (N_1, L)}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message

$$\frac{C \mid\equiv \#(N_1), \; C \mid\equiv S \mid\sim (N_1, L)}{\boxed{C \mid\equiv S \mid\equiv L}}$$

The protocol will be used from the clients to request to another player to join a game. The messages requires authenticity so a signature based on a fresh nonce and made by AES256 GCM is applied on each message. The only fields that require confidentiality are the net information of the users and so they will be encrypted.



MATCH

Message Type (14)	Username C2	Nonce N1	AES Signature

ACCEPT

Message Type (15)	Username C1	Username C2	Nonce N1	AES Signature

REJECT

Message Type (16)	Username C1	Username C2	Nonce N1	AES Signature

GAME_PARAM

Message Type (19)	User PubKey	Net Informations	Nonce N1	AES Signature

KEY_EXCHANGE

Message Type (8)	Diffie-Hellman Partial Key	Nonce N1	RSA Signature

BAN Logic Analysis

Real Protocol

$$
\begin{array}{ll}
M_1 & C_1 \rightarrow S: \ M, C_2, N_1, \{H_{all}\}_{K_{sc_1}} \\
M_2 & S \rightarrow C_2: \ M, C_1, N_1, \{H_{all}\}_{K_{sc_2}} \\
M_3 & C_2 \rightarrow S: \ M, C_1, C_2, N_1, \{H_{all}\}_{K_{sc_2}} \\
M_4 & S \rightarrow C_1: \ M, C_1, C, 2, N_1, \{H_{all}\}_{K_{sc_1}} \\
M_5 & S \rightarrow C_1: \ M, K_{C_2}, N_1, \{I_{C_2}, H_{all}\}_{K_{sc_1}} \\
M_6 & S \rightarrow C_2: \ M, K_{C_1}, N_1, \{I_{C_1}, H_{all}\}_{K_{sc_1}} \\
M_7 & C_2 \rightarrow C_1: \ M, D_1, N_1, \{H_{all}\}_{K_{c_2}^{-1}} \\
M_8 & C_1 \rightarrow C_2: \ M, D_2, N_1, \{H_{all}\}_{K_{c_1}^{-1}}
\end{array}
$$

Goals

$$
\begin{array}{lll}
S \mid\equiv C_1 \mid\equiv' C_2' & S \mid\equiv C_2 \mid\equiv' C_1' & \\
C_1 \mid\equiv S \mid\equiv' C_2' & C_1 \mid\equiv S \mid\equiv \overset{c_2}{\longmapsto} C_2, I_{C_2} & C_1 \mid\equiv C_2 \mid\equiv C_1 \overset{c_1 c_2}{\longleftrightarrow} C_2 \\
C_2 \mid\equiv S \mid\equiv' C_1' & C_2 \mid\equiv S \mid\equiv \overset{c_1}{\longmapsto} C_1, I_{C_1} & C_2 \mid\equiv C_1 \mid\equiv C_1 \overset{c_1 c_2}{\longleftrightarrow} C_2
\end{array}
$$

Ideal Protocol

$$
\begin{array}{ll}
M_1 & C_1 \rightarrow S: \ \#(N_1), \{H_{all}\}_{K_{sc_1}} \\
M_2 & S \rightarrow C_2: \ \#(N_1), \{H_{all}\}_{K_{sc_2}} \\
M_3 & C_2 \rightarrow S: \ \#(N_1), \{H_{all}\}_{K_{sc_2}} \\
M_4 & S \rightarrow C_1: \ \#(N_1), \{H_{all}\}_{K_{sc_1}} \\
M_5 & S \rightarrow C_1: \overset{C_2}{\longmapsto} C_2, \#(N_1), \{I_{C_2}, H_{all}\}_{K_{sc_1}} \\
M_6 & S \rightarrow C_2: \overset{C_1}{\longmapsto} C_1, \#(N_1), \{I_{C_1}, H_{all}\}_{K_{sc_1}} \\
M_7 & C_2 \rightarrow C_1: \ \#(D_1, N_1), \{H_{all}\}_{K_{c_2}^{-1}} \\
M_8 & C_1 \rightarrow C_2: \ \#(D_2, N_1), \{H_{all}\}_{K_{c_1}^{-1}}
\end{array}
$$

Assumptions

$$
\begin{array}{ll}
C_1 \mid\equiv C_1 \overset{K_{cs_1}}{\longleftrightarrow} S & C_2 \mid\equiv C_2 \overset{K_{sc_2}}{\longleftrightarrow} S \\
S \mid\equiv C_1 \overset{K_{sc_1}}{\longleftrightarrow} S & S \mid\equiv C_2 \overset{K_{sc_2}}{\longleftrightarrow} S
\end{array}
$$

Analysis

M1

$$\frac{S \mid\equiv C_1 \overset{K_{sc_1}}{\longleftrightarrow} S, S \triangleleft N_1\{H_{all}\}_{K_{sc_1}}}{S \mid\equiv C_1 \mid\sim N_1}$$

The server has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the server will believes that the client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the server will believes that only the client could have sent that message

$$\frac{S \mid\equiv \#(N_1), S \mid\equiv C_1 \mid\sim (N_1, C_2)}{\boxed{S \mid\equiv C_1 \mid\equiv C_2}}$$

M2

$$\frac{C_2 \mid\equiv C_2 \overset{K_{sc_2}}{\longleftrightarrow} S, C_2 \triangleleft N_1, \{H_{all}\}_{K_{sc_2}}}{C_2 \mid\equiv S \mid\sim N_1}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message

$$\frac{C_2 \mid\equiv \#(N_1), C_2 \mid\equiv S \mid\sim (N_1, C_1)}{\boxed{C_2 \mid\equiv S \mid\equiv C_1}}$$

M3

$$\frac{S \mid\equiv C_2 \overset{K_{sc_2}}{\longleftrightarrow} S, C_2 \triangleleft N_1, \{H_{all}\}_{K_{sc_2}}}{S \mid\equiv C_2 \mid\sim C_1, C_2, N_1}$$

The server has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the server will believes that the client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the server will believes that only the client could have sent that message

$$\frac{S \mid\equiv \#(N_1), S \mid\equiv C_2 \mid\sim C_1, C_2, N_1}{\boxed{S \mid\equiv C_2 \mid\equiv C_1, C_2}}$$

M4

$$\frac{C_1 \mid\equiv C_1 \overset{K_{sc_1}}{\longleftrightarrow} S, C_1 \triangleleft N_1, \{H_{all}\}_{K_{sc_1}}}{C_1 \mid\equiv S \mid\sim N_1}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message

$$\frac{C_1 \mid\equiv \#(N_1), C_1 \mid\equiv S \mid\sim C_1, C_2, N_1}{\boxed{C_1 \mid\equiv S \mid\equiv C_1, C_2}}$$

M5

$$\frac{C_1 \mid\equiv C_1 \overset{K_{sc_1}}{\longleftrightarrow} S, C_1 \triangleleft N_1, \{H_{all}\}_{K_{sc_1}}}{C_1 \mid\equiv S \mid\sim N_1}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message

$$\frac{C_1 \mid\equiv \#(N_1), C_1 \mid\equiv S \mid\sim \overset{c_2}{\longmapsto} C_2, I_{c_2}, N_1}{\boxed{C_1 \mid\equiv S \mid\equiv \overset{c_2}{\longmapsto} C_2, I_{c_2}}}$$

M6

$$\frac{C_2 \mid\equiv C_1 \overset{K_{sc_2}}{\longleftrightarrow} S, C_2 \triangleleft N_1, \{H_{all}\}_{K_{sc_2}}}{C_2 \mid\equiv S \mid\sim N_1}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message

$$\frac{C_2 \mid\equiv \#(N_1), C_2 \mid\equiv S \mid\sim \overset{c_1}{\longmapsto} C_1, I_{c_1}, N_1}{\boxed{C_2 \mid\equiv S \mid\equiv \overset{c_1}{\longmapsto} C_1, I_{c_1}}}$$

M7

$$\frac{C_1 \mid\equiv \xmapsto{K_{c_2}} C_2, S \triangleleft \{H_{all}\}_{K_{c_2}^{-1}}}{S \mid\equiv C_2 \mid\sim \#(D_1, N_1)}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the other client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the other client could have sent that message

$$\frac{{}_1 \mid\equiv \#(D_1, N_1), C_1 \mid\equiv C_2 \mid\sim (D_1, N_1)}{\boxed{S \mid\equiv C \mid\equiv D_1}}$$

M8

$$\frac{C_2 \mid\equiv \xmapsto{K_{c_1}} C_1, C_2 \triangleleft \{H_{all}\}_{K_{c_1}^{-1}}}{C_2 \mid\equiv C_1 \mid\sim \#(D_2, N_1)}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the other client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the other client could have sent that message

$$\frac{C_2 \mid\equiv \#(D_2, N_1), C_2 \mid\equiv C_1 \mid\sim (D_2, N_1)}{C_2 \mid\equiv C_1 \mid\equiv D_2}$$

$$\frac{C_1 \mid\equiv D_1, C_1 \mid\equiv C_2 \mid\equiv D_2}{\boxed{C_1 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2}}$$

We have the two Diffie-Hellman components, we can use the first **Diffie-Hellman postulate** to derive that the client has generate the shared session key

We have almost one fresh Diffie-Hellman partial key, we can use the *second* **Diffie-Hellman postulate** to derive that the shared key is unique and believing to that session

$$\frac{\#(D_1), C_1 \mid\equiv C_2 \mid\equiv D_2}{\boxed{C_2 \mid\equiv (C_1 \xleftrightarrow{K_{c_1c_2}} C_2)}}$$

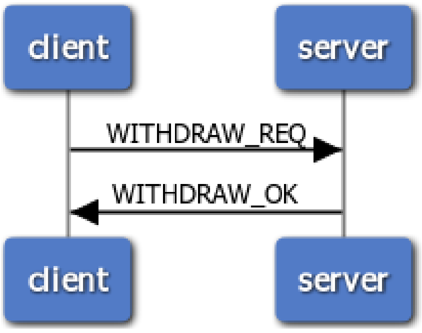
$$\frac{C_2 \mid\equiv D_2, C_2 \mid\equiv C_1 \mid\equiv D_1}{\boxed{C_2 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2}}$$

We have the two Diffie-Hellman components, we can use the first **Diffie-Hellman postulate** to derive that the client has generate the shared session key

We have almost one fresh Diffie-Hellman partial key, we can use the *second* **Diffie-Hellman postulate** to derive that the shared key is unique and believing to that session

$$\frac{C_2 \mid\equiv \#(D_2), C_2 \mid\equiv C_1 \mid\equiv D_1}{\boxed{C_1 \mid\equiv C_2 \mid\equiv (C_1 \xleftrightarrow{K_{c_1c_2}} C_2)}}$$

The protocol will be used from the clients to undo a previously sent challenge. The messages requires authenticity so a signature based on a fresh nonce and made by AES256 GCM is applied on each message.



WITHDRAW_REQ

Message Type (17)	Username	Nonce N1	AES Signature

WITHDRAW_OK

Message Type (18)	Nonce N1	AES Signature

BAN Logic Analysis

Real Protocol

$M_1 \quad C \to S : \; M, U, N_1, \{H_{all}\}_{K_{cs}}$

$M_2 \quad S \to C : \; M, N_1, \{H_{all}\}_{K_{cs}}$

Ideal Protocol

$M_1 \quad C \to S : \; \#(N_1), \{H_{all}\}_{K_{cs}}$

$M_2 \quad S \to C : \; \#(N_1), \{H_{all}\}_{K_{cs}}$

Goals

$C \mid\equiv S \mid\equiv N_1$

$S \mid\equiv C \mid\equiv U$

Assumptions

$C \mid\equiv \xleftrightarrow{K_{cs}} S$

$S \mid\equiv \xleftrightarrow{K_{cs}} S$

Analysis

M1

$$\frac{S \mid\equiv C \xleftrightarrow{K_{sc}} S, S \triangleleft N_1, \{H_{all}\}_{K_{sc}}}{S \mid\equiv C \mid\sim U}$$

The server has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the server will believes that the client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the server will believes that only the client could have sent that message

$$\frac{S \mid\equiv \#(N_1), S \mid\equiv C \mid\sim U, N_1}{\boxed{S \mid\equiv C \mid\equiv U}}$$

M2

$$\frac{C \mid\equiv C \xleftrightarrow{K_{sc}} S, C \triangleleft N_1, \{H_{all}\}_{K_{sc}}}{C \mid\equiv S \mid\sim N_1}$$

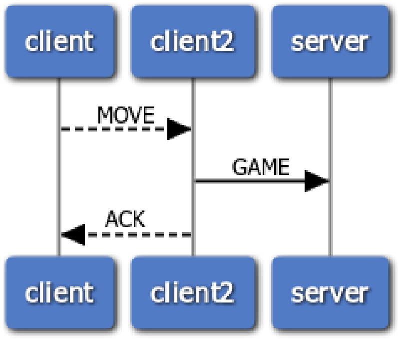
The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message

$$\frac{C \mid\equiv \#(N_1), C \mid\equiv S \mid\sim N_1}{\boxed{C \mid\equiv S \mid\equiv N_1}}$$

The protocol will be used from the clients to make a move during the match. The messages requires authenticity so a signature based on a fresh nonce and made by AES256 GCM is applied on each message. The only field that requires confidentiality is the chosen column of the user and so it will be encrypted.

(the send of the GAME message to the server is explained on pg.6)



MOVE	Message Type (21)	Current Token	Chosen Column	GAME message	Signature
GAME	Message Type (25)	Current Token	Signature	OptSignature	
ACK	Message Type (22)	Current Token	AES Signature		

BAN Logic Analysis

Real Protocol

$$M_1 \quad C_1 \to C_2 :\ M, CT, \{(C, G, H_{all}\}_{K_{c_1c_2}}$$
$$M_2 \quad C_2 \to S :\ M, N_1, \{H_{all}\}_{K_{c_1}}, \{C, H_{all}\}_{K_{sc_1}}$$
$$M_3 \quad C_2 \to C_1 :\ M, CT, \{H_{all}\}_{K_{c_1c_2}}$$

Ideal Protocol

$$M_1 \quad C_1 \to C_2 :\ \#(CT), \{(C, G, H_{all}\}_{K_{c_1c_2}}$$
$$M_2 \quad C_2 \to S :\ M, \#(N_1), \{H_{all}\}_{K_{c_1}}, \{CT, H_{all}\}_{K_{sc_1}}$$
$$M_3 \quad C_2 \to C_1 :\ \#(CT), \{H_{all}\}_{K_{c_1c_2}}$$

Goals

$$C_2 \mid\equiv C_1 \mid\equiv C, G$$
$$C_1 \mid\equiv C_2 \mid\equiv CT$$
$$S \mid\equiv C_1 \mid\equiv C$$

Assumptions

$$C_1 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2)$$
$$C_2 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2)$$
$$S \mid\equiv C_1 \xleftrightarrow{K_{sc_1}} S \qquad S \mid\equiv \overset{K_{c_1}}{\longmapsto} C_1$$

Analysis

M1

$$\frac{C_2 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2, C_2 \triangleleft CT, \{(H_{all}\}_{K_{c_1c_2}}}{C_2 \mid\equiv C_1 \mid\sim CT, C, G}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the other client has sent the fields of the mes-

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the other client could have sent that message

$$\frac{C_2 \mid\equiv \#(CT), C_2 \mid\equiv C_1 \mid\sim CT, C, G}{\boxed{C_2 \mid\equiv C_1 \mid\equiv C, G}}$$

M2

$$\frac{S \mid\equiv \overset{K_{c_1}}{\longmapsto} C_1, S \triangleleft \{(H_{all}\}_{\overset{K_{c_1}}{\longmapsto}}}{S \mid\equiv C_1 \mid\sim N_1, C}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the other client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the other client could have sent that message

$$\frac{S \mid\equiv \#(N_1), S \mid\equiv C_1 \mid\sim N_1, C}{\boxed{S \mid\equiv C_1 \mid\equiv C}}$$

M3	

$$\frac{C_1 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2, C_1 \triangleleft \{H_{all}\}_{K_{c_1c_2}}}{C_2 \mid\equiv C1 \mid\sim CT}$$

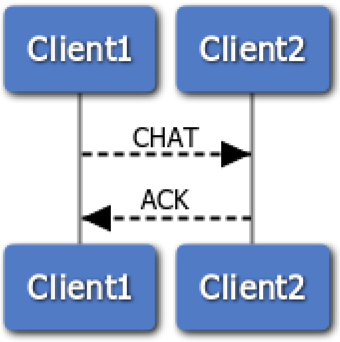
The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the other client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the other client could have sent that message

$$\frac{C_1 \mid\equiv \#(CT), C_1 \mid\equiv C_2 \mid\sim CT}{\boxed{C_2 \mid\equiv C_1 \mid\equiv CT}}$$

Chat Protocol

The protocol will be used from the clients to send a message the adversary during the match. The messages requires authenticity so a signature based on a fresh nonce and made by AES256 GCM is applied on each message. The only field that requires confidentiality is the sent message and so it will be encrypted



BAN Logic Analysis

Real Protocol

M_1	$C_1 \rightarrow C_2 : M, N_1, \{(C, H\}Kc_1c_2$
M_2	$C_2 \rightarrow C_1 : M, N_1, \{H_{all}\}_{K_{c_1c_2}}$

Goals

$C_2 \mid\equiv C_1 \mid\equiv C$

$C_1 \mid\equiv C_2 \mid\equiv N_1$

Ideal Protocol

M_1	$C_1 \rightarrow C_2 : \#(N_1), \{(C, H\}Kc_1c_2$
M_2	$C_2 \rightarrow C_1 : \#(N_1), \{H_{all}\}_{K_{c_1c_2}}$

Assumptions

$C_1 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2)$

$C_2 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2)$

Analysis

M1	

$$\frac{C_2 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2, C_2 \triangleleft N_1, \{(C, H\}_{K_{c_1c_2}}}{C_2 \mid\equiv C_1 \mid\sim N_1, C}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the other client has sent the fields of the mes-

The message contains a fresh field(nonce), se we can apply th **nonce verification postulate** to derive that the client will believes that only the other client could have sent that message

$$\frac{C_2 \mid\equiv \#(N_1), C_2 \mid\equiv C_1 \mid\sim N_1, C}{\boxed{C_2 \mid\equiv C_1 \mid\equiv C}}$$

M2

$$\frac{C_1 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2,\ C_1 \triangleleft N_1, \{H_{all}\}_{K_{c_1c_2}}}{C_1 \mid\equiv C_2 \mid\sim N_1}$$

The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the other client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the other client could have sent that message

$$\frac{C_1 \mid\equiv \#(N_1),\ C_1 \mid\equiv C_2 \mid\sim N_1}{\boxed{C_1 \mid\equiv C_2 \mid\equiv N_1}}$$

M3

$$\frac{C_1 \mid\equiv C_1 \xleftrightarrow{K_{c_1c_2}} C_2,\ C_1 \triangleleft N_1, \{H_{all}\}_{K_{c_1c_2}}}{C_1 \mid\equiv C_2 \mid\sim N_1}$$

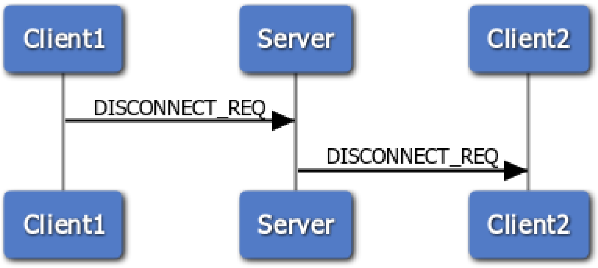
The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the other client has sent the fields of the message

The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the other client could have sent that message

$$\frac{C_1 \mid\equiv \#(N_1),\ C_1 \mid\equiv C_2 \mid\sim N_1}{\boxed{C_1 \mid\equiv C_2 \mid\equiv N_1}}$$

Disconnect Protocol

The protocol will be used from the clients to exit from a match. The messages requires authenticity so a signature based on a fresh nonce and made by AES256 GCM is applied on each message.



DISCONNECT_REQ	Message Type (23)	Nonce N1	AES Signature

BAN Logic Analysis

Real Protocol

$M_1 \quad C_1 \rightarrow S: \ M, N_1, \{(H_{all}\}_{KC_1S}$

$M_2 \quad S \rightarrow C_2: \ M, N_1, \{H_{all}\}_{K_{c_2s}}$

Ideal Protocol

$M_1 \quad C_1 \rightarrow C_2: \ \#(N_1), \{(H_{all}\}_{KC_1S}$

$M_2 \quad C_2 \rightarrow C_1: \ \#(N_1), \{(H_{all}\}_{KC_2S}$

Assumptions

$C_1 \mid\equiv C_1 \xleftrightarrow{K_{c_1s}} S$

$C_2 \mid\equiv C_2 \xleftrightarrow{K_{c_2s}} S$

$S \mid\equiv C_1 \xleftrightarrow{K_{c_1s}} S$

$S \mid\equiv C_2 \xleftrightarrow{K_{c_2s}} S$

Goals

$S \mid\equiv C_1 \mid\equiv N_1$

$C_2 \mid\equiv S \mid\equiv N_1$

Analysis

M1	$$\frac{S \mid\equiv C_1 \xleftrightarrow{K_{c_1s}} S, S \triangleleft N_1, \{(H\}_{K_{c_1s}}}{S \mid\equiv C_1 \mid\sim N_1}$$ The server has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the server will believes that the client has sent the fields of the message The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the server will believes that only the client could have sent that message $$\frac{S \mid\equiv \#(N_1), S \mid\equiv C_1 \mid\sim N_1}{\boxed{S \mid\equiv C_1 \mid\equiv N_1}}$$
M2	$$\frac{C_2 \mid\equiv C_2 \xleftrightarrow{K_{c_2s}} S, C_2 \triangleleft N_1, \{H_{all}\}_{K_{c_2s}}}{C_2 \mid\equiv S \mid\sim N_1}$$ The client has received a message containing a signature made by all the fields with the AES session key. We can apply the **signature postulate** to derive that the client will believes that the server has sent the fields of the message The message contains a fresh field(nonce), se we can apply the **nonce verification postulate** to derive that the client will believes that only the server could have sent that message $$\frac{C_2 \mid\equiv \#(N_1), C_2 \mid\equiv S \mid\sim N_1}{\boxed{C_2 \mid\equiv S \mid\equiv N_1}}$$

UML Diagram