YASMS

PROTOCOL FORMALIZATION

CSCE 5930 | Information and Distributed Systems Security

American University in Cairo

Fall 2017

Group Members

Aley Baracat (ID no. 900140290)

Ahmed Nofal (ID no.900143136)

Yasmin ElDokany (ID no. 900131538)

Ziad Osama (ID no. 900130315)

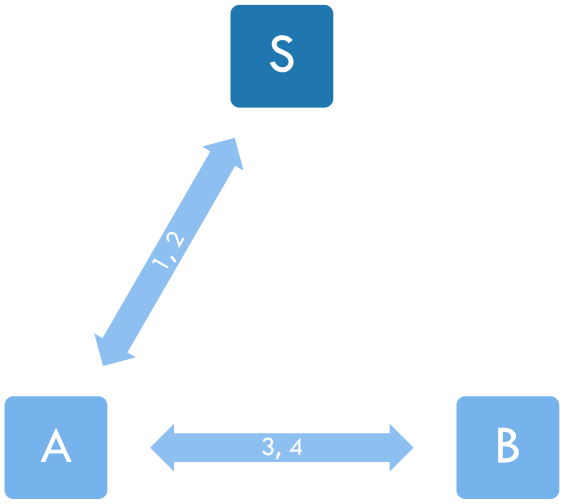
TABLE OF CONTENTS

AUTHENTICATION MESSAGES

In order to ensure mutual authentication between any two users of the YASMS system, the following protocol is implemented, which ensures that no message is sent without encapsulating a proof of its origin and freshness and prevents Man-in-the-Middle and impersonation attacks.

All authentication messages are ultimately encrypted by the public key of their intended recipient, and within each message, there is the identifying username of its sender, as well as that of the recipient, and the message content itself encrypted by the private key of the sender, which ensures proof of origin. The usernames are used to ensure identity consistency and to identify the public key of the message's sender in order to decrypt the message's content.

For the notations used below, A and B represent two system users initiating a chat session with each other, S represents the system's server and certificate authority, T_s is a timestamp issued by the server and L is a value representing the validity duration of the authentication messages.



1) $A \rightarrow S$: $\left\{A, B, \left\{A, B, \{N_{a2}\}_{k_A^{-1}}, L, N_{a1}\right\}_{k_A^{-1}}\right\}_{k_S}$

2) $S \rightarrow A$: $\left\{S, A, \{A, B, K_A, T_S, L, N_{a1}\}_{k_S^{-1}}\right\}_{k_A}, \left\{S, A, B, \left\{A, B, K_A, T_S, L, \left\{N_{a_2}\right\}_{k_A^{-1}}\right\}_{k_S^{-1}}\right\}_{k_B}$

3) $A \rightarrow B$: $\left\{S, A, B, \left\{A, B, K_A, T_S, L, \left\{N_{a_2}\right\}_{k_A^{-1}}\right\}_{k_S^{-1}}\right\}_{k_B}$

4) $B \rightarrow A$: $\left\{B, A, \left\{N_{a_2} + 1\right\}_{k_B^{-1}}, T_S, L\right\}_{k_A}$

PROOF USING BAN LOGIC

1) From the first message in the protocol:

For this message, the server checks the identity of A to make sure it is still an authenticated user and that k_A belongs to A.

2) From the second message in the protocol:

- $\because A \mid \equiv K_A^{-1}\ AND\ A \lhd \left\{S, A, \{A, B, K_A, T_S, L, N_{a1}\}_{k_S^{-1}}\right\}_{k_A}$
- $\therefore A \mid \equiv S \mid \sim S, A, \{A, B, K_B, T_S, L, N_a,\}_{k_S^{-1}}$ *(by the message meaning rule)*

- $\because A \mid \equiv K_s\ AND\ A \lhd \{A, B, K_B, T_S, L, N_a\}$
- $\therefore A \mid \equiv S \mid \sim A, B, K_B, T_S, L, N_a$ *(by the message meaning rule)*

- $\because A \mid \equiv \#N_a$
- $\therefore A \mid \equiv \#A, B, K_B, T_s, L$ *(by the freshness rule)*

- $\because A \mid \equiv \#K_B\ AND\ A \mid \equiv S \mid \sim A, B, K_B, T_S, L, N_a$
- $\therefore A \mid \equiv S \mid \equiv K_B$ *(by the nonce-verification rule)*

- $\because A \mid \equiv S \Longrightarrow K_B\ AND\ A \mid \equiv S \mid \equiv K_B$
- $\therefore \boldsymbol{A \mid \equiv K_B}$ *(by the jurisdiction rule)*

3) From the third message in the protocol:

- $\because B \mid \equiv K_B^{-1}\ AND\ B \lhd \left\{S, A, B, \left\{A, B, K_A, T_S, L, \left\{N_{a_2}\right\}_{k_A^{-1}}\right\}_{k_S^{-1}}\right\}_{k_B}$
- $\therefore B \mid \equiv S \mid \sim S, A, B, \left\{A, B, K_A, T_S, L, \left\{N_{a_2}\right\}_{k_A^{-1}}\right\}_{k_S^{-1}}$ *(by the message meaning rule)*

- $\because B \mid \equiv K_S\ AND\ B \lhd \left\{A, B, K_A, T_S, L, \left\{N_{a_2}\right\}_{k_A^{-1}}\right\}_{k_S^{-1}}$
- $\therefore B \mid \equiv S \mid \sim A, B, K_A, T_S, L, \left\{N_{a_2}\right\}_{k_A^{-1}}$ *(by the message meaning rule)*

- $\because B| \equiv \#(T_S + L)$
- $\therefore B| \equiv \#\, A, B, K_A, \{N_{a_2}\}_{k_A^{-1}}$ *(by the freshness rule)*

- $\because B\ | \equiv \#K_A\ AND\ \ B\ |\equiv S|\sim A, B, K_A, \{N_{a_2}\}_{k_A^{-1}}$
- $\therefore B| \equiv S\ | \equiv K_A$ *(by the nonce-verification rule)*

- $\because B|\equiv S\ \Longrightarrow K_A\ AND\ B| \equiv S| \equiv K_A$
- $\therefore \boldsymbol{B| \equiv K_A}$ *(by the jurisdiction rule)*

- Using protocol idealization for the third message is equivalent to:

$$\boldsymbol{A \rightarrow B: \left\{S, A, B, \left\{K_A, T_S, L, \{N_{a_2}\}_{k_A^{-1}}, K_B\right\}_{k_S^{-1}}\right\}_{k_B}}$$

  - $\because B| \equiv \#(T_S + L)$
  - $\therefore B| \equiv \#K_B$ *(by the freshness rule)*

  - $\because B\ | \equiv A\ |\sim K_B\ \ AND\ B| \equiv \#K_B$
  - $\therefore \boldsymbol{B|\equiv A| \equiv K_B}$ *(by the nonce-verification rule)*

4) From the fourth message in the protocol:

- Using protocol idealization for the fourth message is equivalent to:

$$\boldsymbol{B \rightarrow A: \left\{B, A, \{N_{a_2} + 1\}_{k_B^{-1}}, T_S, K, K_A\right\}_{k_A}}$$

  - $\because A\ | \equiv K_A^{-1} AND \because A \lhd \left\{B, A, \{N_{a_2} + 1\}_{k_B^{-1}}, T_S, L, K_A\right\}_{k_A}$
  - $\therefore A| \equiv B\ |\sim B, A, \{N_{a_2} + 1\}_{k_B^{-1}}, T_S, L, K_A$ *(by the message meaning rule)*

  - $\because A| \equiv \#(T_S + L)$
  - $\therefore A| \equiv \#K_A$ *(by the freshness rule)*

- $\because A| \equiv \#K_A \; AND \; A| \equiv B| \sim K_A$
- $\therefore \boldsymbol{A| \equiv B| \equiv K_A}$ *(by the nonce-verification rule)*

This proof ensures that A and B are mutually authenticated to each other, and can therefore begin establishing a shared key for their session, without the involvement of the server certificate authority.

SHARED KEY ESTABLISHMENT MESSAGES

For the notations used below, A and B represent two system users who are mutually authenticated to each other, T_{AB} is a timestamp issued by A for the duration of the session and L_{AB} is a value representing the validity duration of the session. A and B generate a shared key K_{AB} using the Diffie-Hellman key exchange protocol to be used for their consequent end-to-end encrypted chat messages.

1) $\boldsymbol{A \rightarrow B: \left\{ L_{AB}, T_{AB}, \{K_{AB}\}_{k_A^{-1}}, A, B \right\}_{k_B}}$

2) $\boldsymbol{B \rightarrow A: \left\{ \{K_{AB}\}_{k_B^{-1}}, L_{AB}, T_{AB}, B, A \right\}_{k_A}}$

PROOF USING BAN LOGIC

- $\because B| \equiv A| \equiv K_B \;\; AND \;\; B| \equiv K_A$
- $\because B \lhd L_{AB}, T_{AB}, \{K_{AB}\}_{k_A^{-1}}, A, B$
- $\therefore B| \equiv A \;|\sim L_{AB}, T_{AB}, \{K_{AB}\}_{k_A^{-1}}, A, B$ *(by the message meaning rule)*

- $\because B| \equiv \#(T_{AB} + L_{AB})$
- $\therefore B| \equiv \#K_{AB}$ *(by the freshness rule)*

- $\because B| \equiv A| \sim L_{AB}, T_{AB}, \{K_{AB}\}, A, B \;\; AND \; B| \equiv \#K_{AB}$
- $\therefore B| \equiv A| \equiv K_{AB}$ *(by the nonce-verification rule)*

- $\because B| \equiv A \Longrightarrow K_{AB} \;\; AND \; B| \equiv A| \equiv K_{AB}$
- $\therefore B| \equiv K_{AB}$ *(by the jurisdiction rule)*

The same is done for the second message to establish:

- $\therefore A| \equiv K_{AB}$ *(by the jurisdiction rule)*