Ro-Sham-Bo
HW5 - CNS Sapienza

Edoardo Puglisi 1649359

5/12/2019

Contents

1 Overview

Design a protocol that guarantee the perfect execution of the "Rock-Paper-Scissor" game between two users in a network composed only by them two (no men-in-the-middle attacks). The users will cheat if the protocol will admit a way to do it.

2 Protocol explanation

2.1 Initialization

Both users have a public key P_i and a secret key K_i. When the game starts the two users exchange their public keys for future authentication. Both start with score = (0,0).

2.2 The Game

Alice (A) will be the one who started the game, while Bob (B) is her adversary. On every turn A will generate a secret session key S_i.

1. A chooses a move: $move_A$
2. A $\rightarrow$ B: $M_{A1} = [K_A(S_A(move_A) + t_i + score)]$
   A encrypts her move with her session key and attach the score plus a timestamp, then encrypts all with her secret key (can be decrypted with public key).
3. B $\rightarrow$ A: $M_{B1} = [K_B(M_{A1}), K_B(move_B + score + t_{i+1}))]$
   B encrypts with his secret key the previous message and his move attached with augmented timestamp and score.
4. A $\rightarrow$ B: $M_{A2} = [S_A, newscore, K_A(M_{B1}[1]), M_{B1}[0]]$
   At this time A has all the necessary to understand who won. She send to B the new score, her session key so B can verify too and the proof of the new score: her move "accepted" by B (encrypted with K_B) and the move of B "accepted" by her.
5. B $\rightarrow$ A: $M_{B2} = [newscore, M_{A2}[2], M_{A1}]$
   B checks the score and send his proof of it: A's move and his move accepted by her.

At next round score = newscore. Reached 2 out of 3 wins the game ends.

2.3 Cheating control

Anticipate move: the first move is sent encrypted so B can't cheat on it.

Cheat on score: none of the user can cheat on score because at every step (in every message) the score is send as parameter and "accepted" when the receiver send the answer back. Eg. at step 2, A sends *score* to B that accept it as real result when at step 3 he sends back the same *score* encrypted with his secret key.

No repudiation: every move is encrypted with the private key of the owner: none can create a ciphertext equal to it without the personal secret key.

No message repetition: every message (ciphertext) is the result of a message with a timestamp attached on it. This guarantee that messages can't be resend on future rounds.