Security Protocols and Verification

Description of PSS Protocol

Dyvia Pugo, Marcella Scholze, Sylvie Sidler

October 3, 2025

1 Description of the PSS Protocol

The PSS Protocol is described as follows:

1. $B \to A : N_B$
2. $A \to B : \{K_{AB}, A, N_A, N_B\}_{pk(B)}$
3. $B \to A : \{|\{N_B, N_A - 1\}_{pk(A)}|\}_{K_{AB}}$
4. $A \to B : \{N_B - 1\}_{K_{AB}}$

Initial knowledge

At the beginning of the protocol:

- A and B know each other's public keys, $pk(A)$ and $pk(B)$, respectively.
- A and B know their own private keys, $sk(A)$ and $sk(B)$, which correspond to their public keys.

Values generated during the protocol execution

- K_{AB}: session key, generated by A.
- N_A: Nonce generated by A.
- N_B: Nonce generated by B.

Protocol description

The protocol proceeds with the following messages:

1. $B \rightarrow A : N_B$.
   B initiates the protocol by sending a fresh nonce N_B to A, requesting key establishment.

2. $A \rightarrow B : \{K_{AB}, A, N_A, N_B\}_{pk(B)}$.
   A generates a session key K_{AB} and her own nonce N_A. A sends the session key K_{AB}, her identity A, and the two nonces (N_A, N_B) to B, all encrypted under B's public key, $pk(B)$. Only B can decrypt this message to recover K_{AB}, A, N_A, and N_B.

3. $B \rightarrow A : \{|\{N_B, N_A - 1\}_{pk(A)}|\}_{K_{AB}}$

   B decrypts the second message using his private key $sk(B)$, thus retrieving K_{AB} and N_A. B then encrypts his original nonce N_B and a value derived from A's nonce ($N_A - 1$) using the established session key K_{AB} and $pk(A)$.

4. $A \rightarrow B : \{N_B - 1\}_{K_{AB}}$.
   A decrypts the third message and verifies B's identity and knowledge of K_{AB} by checking $N_A - 1$. A completes the challenge by sending $N_B - 1$, encrypted with K_{AB}, proving to B that A knows K_{AB} and received B's nonce N_B.

Cost calculation

1. $B \rightarrow A : N_B$
   $f(N_B) = 1$
   Cost(message 1) $= 1$

2. $A \rightarrow B : \{K_{AB}, A, N_A, N_B\}_{pk(B)}$
   $f(K_{AB}, A, N_A, N_B) = f((K_{AB}, (A, (N_A, N_B))))$

   $f((N_A, N_B)) = 50 + f(N_A) + f(N_B) = 50 + 1 + 1 = 52$

   $f((A, (N_A, N_B))) = 50 + f(A) + 52 = 50 + 1 + 52 = 103$

   $f((K_{AB}, (A, (N_A, N_B)))) = 50 + f(K_{AB}) + 103 = 50 + 1 + 103 = 154$

   $f(\{K_{AB}, A, N_A, N_B\}_{pk(B)}) = 1 + f((K_{AB}, (A, (N_A, N_B)))) + f(pk(B)) = 1 + 154 + 1 = 156$

   Cost(message 2) $= 156$

3. $B \to A : \{|\{N_B, N_A - 1\}_{pk(A)}|\}_{K_{AB}}$

   $f((N_B, N_A - 1)) = 50 + f(N_B) + f(N_A - 1) = 50 + 1 + 1 = 52$

   $f(\{(N_B, N_A - 1)\}_{pk(A)}) = 10 + f((N_B, N_A - 1)) + f(pk(A)) = 1 + 52 + 1 = 54$

   $f(\{|\{N_B, N_A - 1\}_{pk(A)}|\}_{K_{AB}}) = 10 + f(\{(N_B, N_A - 1)\}_{pk(A)}) + f(K_{AB}) = 10 + 54 + 1 = 65$

   Cost(message 3) $= 65$

4. $A \to B : \{N_B - 1\}_{K_{AB}}$

   $f(N_B - 1) = 1$

   $f(\{N_B - 1\}_{K_{AB}}) = 10 + f(N_B - 1) + f(K_{AB}) = 10 + 1 + 1 = 12$

   Cost(message 4) $= 12$

$$\boxed{c(P) = 1 + 156 + 65 + 12 = 234}$$