

# Description of the Needham Schroeder public key protocol and its attack

The Needham Schroeder public key protocol  $P_{NSPK}$  can be described as follows.

$$\begin{aligned} A &\rightarrow B : \{ \langle A, N_a \rangle \}_{\text{pub}(B)} \\ B &\rightarrow A : \{ \langle N_a, N_b \rangle \}_{\text{pub}(A)} \\ A &\rightarrow B : \{ N_b \}_{\text{pub}(B)} \end{aligned}$$

**Initial knowledge:** We suppose that agents  $A$  and  $B$  initially know public keys  $\text{pub}(C)$  of agent  $C$ , for any agent  $C$ .

**Data generated during the protocol:**  $N_a$  is a nonce generated by  $A$ .  $N_b$  is a nonce generated by  $B$ .

**Protocol description:** Alice starts the protocol by sending her identity  $A$  together with a freshly generated random number  $N_a$ . This message is encrypted using an asymmetric encryption algorithm with  $B$ 's public key (denoted  $\text{pub}(B)$ ). We suppose that only agent Bob (whose identity is  $B$ ) knows the secret key corresponding to  $\text{pub}(B)$ .

Next Bob receives the message  $\{A, N_a\}_{\text{pub}(B)}$  sent by Alice. Using his private key, Bob decrypts the message. He sends the received nonce  $N_a$  together with a freshly generated nonce  $N_b$  encrypted with  $A$ 's public key ( $\text{pub}(A)$ ) to Alice.

Finally Alice receives the message  $\{N_a, N_b\}_{\text{pub}(A)}$ . She decrypts the message and checks that the nonce  $N_a$  corresponds to the nonce previously generated and sent to Bob. She sends the nonce  $N_b$  to Bob encrypted with Bob's public key. Upon reception of this message Bob decrypts it and checks that the nonce corresponds to the one previously generated.

**Security properties:**

- *Authentication:* When Bob receives the last message ( $\{N_b\}_{\text{pub}(B)}$ ), this message was indeed sent by Alice.
- *Confidentiality:* Both Alice and Bob are the only to know  $N_b$ .

**Cost of the protocol:**

$$\begin{aligned} f(P_{NSPK}) &= f(\{ \langle A, N_a \rangle \}_{\text{pub}(B)}) + f(\{ \langle N_a, N_b \rangle \}_{\text{pub}(A)}) + f(\{ N_b \}_{\text{pub}(B)}) \\ &= 54 + 54 + 3 \\ &= 111 \end{aligned}$$

(Note that the NSPK protocol was not designed with the cost function in mind.)

### Attack on the Needham-Schroeder protocol

17 years after the publication of the protocol Gavin Lowe discovered an attack that may occur in the presence of an active adversary. The attack has been coined *man-in-the-middle attack*. It is illustrated in figure 1. Agent  $A$  starts a session with a dishonest agent  $C$ . Agent  $C$  uses this message to fake being  $A$  to  $B$ .  $B$  responds to  $A$ . As  $B$ 's message contains the nonce  $N_a$ ,  $A$  accepts the message thinking it originates from  $C$ . Therefore  $A$  sends to  $C$  the nonce  $N_b$  encrypted with  $C$ 's public key.  $C$  can recover the nonce  $N_b$  and end the protocol with  $B$  who thinks having executed the protocol with  $B$ .

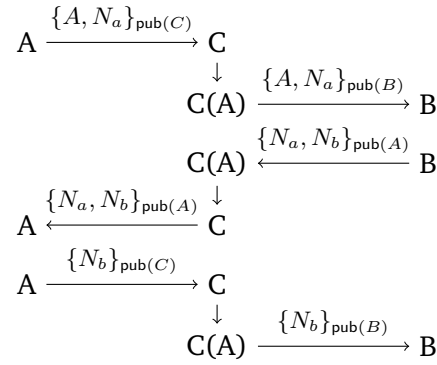


Figure 1: Lowe's attack on the Needham Schroeder public key protocol.