

Description du protocole de Needham-Schroeder et de son attaque

Le protocole de Needham-Schroeder à clefs publiques se décrit de la façon suivante :

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

Connaissances initiales : Au début du protocole, on suppose que les agents A et B connaissent la clef publique $\text{pub}(C)$ associée à l'agent C , pour tout agent C .

Valeurs générées au cours du protocole : N_a est un nonce généré par A . N_b est un nonce généré par B .

Description du protocole : À la première étape du protocole, l'agent Alice envoie son nom A et un nombre engendré aléatoirement N_a . Ce message est chiffré par un algorithme de chiffrement asymétrique avec la *clef publique* de B (notée $\text{pub}(B)$), c'est-à-dire que seul l'agent Bob connaît la clef privée correspondant à la clef $\text{pub}(B)$.

À la deuxième étape du protocole, Bob reçoit le message $\{A, N_a\}_{\text{pub}(B)}$ envoyé par Alice. Comme il a la clef privée (souvent notée $\text{prv}(B)$) lui permettant d'ouvrir le message, il renvoie le nonce d'Alice ainsi qu'un autre nonce N_b qu'il vient d'engendrer, le tout chiffré avec la clef publique $\text{pub}(A)$ d'Alice.

À la troisième étape du protocole, Alice reçoit le message $\{N_a, N_b\}_{\text{pub}(A)}$ et reconnaît son nonce N_a envoyé à Bob. Elle renvoie alors le nonce N_b , chiffré avec la clef publique de Bob.

Propriétés de sécurité :

- *Authentification* Lorsque Bob reçoit le dernier message $\{N_b\}_{\text{pub}(B)}$, il est sûr que celui-ci vient d'Alice.
- *Confidentialité* Les deux agents Alice et Bob sont seuls à connaître le nonce N_b .

Poids du protocole : 111

- Règle 1 : $50 + 1 + 1 + 1 + 1 = 54$
- Règle 2 : $50 + 1 + 1 + 1 + 1 = 54$
- Règle 3 : $1 + 1 + 1 = 3$

Attaque sur le protocole de Needham-Schroeder

G. Lowe a découvert une quinzaine d'années après la publication du protocole de Needham-Schroeder que ce dernier avait une faille en présence d'un intrus actif. Cette faille est souvent appelée « man-in-the-middle attack ». L'attaque est schématisée à la figure 1. L'agent A commence spontanément une conversation avec un agent C , malhonnête. L'agent C se sert de ce premier message pour se faire passer pour A auprès de B . Celui-ci répond donc à A . L'agent A , reconnaissant son nonce N_a pense que C vient de lui répondre. L'agent A , renvoie donc à C le nonce N_b que l'agent C n'aurait pas dû connaître. L'agent C termine alors le protocole avec B qui croit avoir parlé à A .

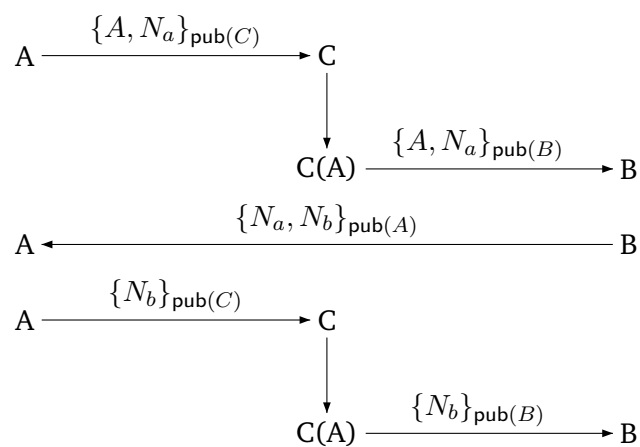


FIG. 1 – Attaque du protocole de Needham-Schroeder, due à G. Lowe.