Quentin Guillard

Attaque sur le protocole TAZ V3

Principe de l'attaque :
Un attaquant Charlie fait en sorte que Alice engage une conversation avec lui. L'attaquant va réaliser une conversation « normale » avec Bob en utilisant le nonce de A (N_a), pour faire croire à ce dernier qu'il effectue une conversation avec Alice.
Lors de l'étape (4), Alice est capable de récupérer correctement N_b car chiffré symétriquement à l'aide de son nonce N_a et renvoie donc le hash de N_b à Charlie en pensant qu'il s'agit simplement du hash d'un nonce généré par ce dernier.
À l'étape (6) Charlie peut donc directement envoyer le hash de N_b à Bob qui pense avoir reçu ce message de Alice.

(1) A→ C: $\{N_a\}_{pub(C)}$
(2) C(A)→ B: $\{N_a\}_{pub(B)}$
(3) B →A: $\{\{N_b\}_{Na}\}_{pub(A)}$, hash$\{N_a\}$: Le message est intercepté par C
(4) C →A: $\{\{N_b\}_{Na}\}_{pub(A)}$, hash$\{N_a\}$
(5) A →C: hash(N_b)
(6) C(A) →B: hash(N_b)

Conclusion :
À la fin de l'échange, Bob pense avoir communiqué avec Alice tout le long alors qu'il s'agissait en réalité de Alice.S