Attaque sur le protocole TAZ

Johan Tombre, Vivien Maintenant, Paul Gellenoncourt

Description de l'attaque :
A initie une communication avec C. C déchiffre le nonce N_a avec sa clé publique et le chiffre avec la clé publique de B avant de le lui envoyer (en se faisant passer pour A).
B répond normalement à A. A pense avoir reçu cette réponse de C et transmet pour finir le hash de N_b . C va simplement transmettre ce message à B en se faisant passer pour A.
Les en-têtes indiquant l'émetteur du message ne sont pas explicités dans le protocole mais on sous-entend que C adapte ces en-têtes pour voler l'identité de A.

$$A \rightarrow C : \{N_a\}_{pub(C)}$$
$$C(A) \rightarrow B : \{N_a\}_{pub(B)}$$
$$B \rightarrow A : \{\{N_b\}_{Na}\}_{pub(A)}, hash(N_a)$$
$$A \rightarrow C : hash(N_b)$$
$$C(A) \rightarrow B : hash(N_b)$$

Conclusion : Lorsque le protocole finit, B pense avoir réalisé un échange avec A, alors que les messages viennent de C. A, quant à lui, pense avoir réalisé un échange normal avec C. En réalité, c'est avec B qu'il a échangé les nonces.