Attaque sur le protocole Azote

Johan Tombre, Vivien Maintenant, Paul Gellenoncourt

Description de l'attaque :
A va souhaiter communiquer avec B mais C va bloquer les messages de A vers B et va se placer au centre (A parlera avec C et C avec B).
Sur le premier message de A, l'attaquant va juste modifier l'entête pour mettre son nom et l'envoyer à B.
Lorsque B répond, C déchiffre N_b et le chiffre avec la clé publique de A avant de l'envoyer à A en se faisant passer pour B.
A envoie ensuite le secret chiffrer par N_a et N_b mais C intercepte le message afin de remplacer l'identité de A par le sien et l'envoie à B.
B répond avec le secret chiffré par la clé publique de C. C peut alors déchiffrer le secret puis le chiffrer avec la clé publique de A en se faisant passer pour B.

$A \rightarrow B : A, \{N_a\}_{pub(B)}$ bloqué par C
$C \rightarrow B : C, \{N_a\}_{pub(B)}$
$B \rightarrow C : Hash(N_a), \{N_b\}_{pub(C)}$
$C(B) \rightarrow A : Hash(N_a), \{N_b\}_{pub(A)}$
$A \rightarrow B : \{\{scrt\}_{Nb}\}_{Na}$ bloqué par C
$C \rightarrow B : \{\{scrt\}_{Nb}\}_{Na}$
$B \rightarrow C : \{scrt\}_{pub(C)}$
$C(B) \rightarrow A : \{scrt\}_{pub(A)}$

Conclusion : Lorsque le protocole finit, A pense avoir réalisé un échange avec B alors qu'il a communiqué avec C. B, quant à lui, pense avoir réalisé un échange normal avec C.