Attaque sur le protocole Proto-chorale

Johan Tombre, Vivien Maintenant, Paul Gellenoncourt

Description de l'attaque : On suppose que A a par le passé réalisé un échange utilisant ce protocole avec C. L'attaquant C connaît donc $\{C\}_{sk(Kas)}$. L'attaquant va donc, lors de l'envoi du premier message pour B par A, remplacer le message $\{B\}_{sk(Kas)}$ par $\{C\}_{sk(Kas)}$. Le serveur va donc penser qu'il s'agit d'un échange entre A et C. La suite des interactions impliquant le serveur se passe ensuite normalement, A ne remarquant pas que c'est avec C qu'il communique. Cela permet à C de prendre connaissance de K.
Dans la seconde partie du protocole, C va bloquer tous les messages envoyés par A pour B mais renvoyer les réponses $\{B\}_{pubA}$ et $\{B\}_{sj(K)}$ au moment voulu.
A la fin du protocole, tout s'est passé normalement aux yeux de A mais c'est à C qu'il communique et non B.

A —> S : A, {B}sk(Kas) bloqué par C

C(A) $A \rightarrow S : A, \{C\}_{sk(Kas)}$

$S \rightarrow A : \{A\}_{sk(Kas)}$

$A \rightarrow S : A, \{K\}_{sk(Kas)}$

$S \rightarrow C : \{<K,A>\}_{sk(Kcs)}$

$A \rightarrow B : \{A\}_{pub(B)}$ *bloqué par C*

C(B) $C \rightarrow A : \{B\}_{pub(A)}$

$A \rightarrow B : \{h(K)\}_{pub(B)}$ *bloqué par C*

C(B) $C \rightarrow A : \{B\}_{sk(K)}$

$A \rightarrow B : \{A\}_{sk(K)}$ *bloqué par C*

Remarques : On notera que C sait que A souhaite parler à B grâce aux entêtes des messages non visibles ici et que A ne sait pas que C lui répond car C aura modifié ses entêtes de message pour se faire passer pour B.