L'équipe Proto-Chorale attaque le protocole TAZv2

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de cette attaque pour C est de connaître scrt. On considère au vu de la sécurité sur les destinataires/envoyeurs que C ne voit que les messages directement reçus ou envoyés par B, et sait juste que c'est A qui lui parle (donc a vu le premier message partir de A, puis arriver chez B). On ne va par conséquent lire ou modifier aucun message entre A et S.

2 Scénario de l'attaque

A la suite d'un échange normal avec le serveur, A a envoyé à B un nonce Na :

- $A \rightarrow S : \{Na\}_{pub(B)}, \{B\}_{k_{AS}}$
- $S \rightarrow B : \{Na\}_{pub(B)}, \{A\}_{k_{BS}}$

De même, C entame une discussion avec le serveur, en lui renvoyant $\{Na\}_{pub(B)}$ qu'il a vu passer précédemment. C ne se cache pas dans l'échange :

1. $C \rightarrow S : \{Na\}_{pub(B)}, \{B\}_{k_{CS}}$
2. $S \rightarrow B : \{Na\}_{pub(B)}, \{C\}_{k_{BS}}$

1. $B \rightarrow S : \{Nc\}_{pub(C)}, \{C\}_{k_{BS}}$
2. $S \rightarrow C : \{Nc\}_{pub(C)}, \{B\}_{k_{CS}}$

B tente ensuite de répondre au serveur dans sa discussion avec A, mais C bloque le message. Cependant, C a intercepté $\{A\}_{k_{BS}}$, qu'il utilise dans sa propre conversation avec le serveur :

1. $B \rightarrow S : \{Nb\}_{pub(A)}, \{A\}_{k_{BS}}$ **bloqué**
2. $C \rightarrow S : \{Nc\}_{pub(A)}, \{A\}_{k_{BS}}$
3. $S \rightarrow A : \{Nc\}_{pub(A)}, \{B\}_{k_{AS}}$

Comme B sait qu'il discute à la fois avec A et avec C, C va bloquer le message de A contenant le secret et le renvoyer à sa place. B pensera que le secret de A est celui de C, d'autant plus que pour B, sa discussion avec A se fait avec Na et Nb, et sa discussion avec C se fait avec Na et Nc :

1. $A \rightarrow B : \{\{scrt\}_{Nc}\}_{Na}$ **bloqué**
2. $C \rightarrow B : \{\{scrt\}_{Nc}\}_{Na}$

B renverra le secret déchiffré à C :

1. $B \rightarrow C : \{scrt\}_{pub(C)}$ **C peut donc lire scrt**
2. $C \rightarrow A : \{scrt\}_{pub(A)}$