L'équipe Proto-Chorale attaque le protocole Protocoolv2

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de cette attaque pour C est d'envoyer $\{K\}_{bc}$ à B en se faisant passer pour A.

2 Scénario de l'attaque

A entame une discussion avec C et une discussion avec B :

- $A \rightarrow S : A, B$
- $A \rightarrow S : A, C$

C va ensuite inverser les entêtes des deux messages que A reçoit :

- $S \rightarrow A : \{N_2\}_{ksa}$ entête de B
- $S \rightarrow A : \{N_1\}_{ksa}$ entête de C

Les reçus se font normalement pour B et C :

- $S \rightarrow B : \{N_1, A\}_{ksb}$
- $S \rightarrow C : \{N_2, A\}_{ksc}$, **C peut ainsi lire** N_2

A envoie ses deux clés à B et C, l'envoi pour B sera bloqué :

- $A \rightarrow B : \{N_2, K_{ab}\}_{pub(B)}$, **message bloqué par C**
- $A \rightarrow C : \{N_1, K_{ac}\}_{pub(C)}$, **C peut ainsi lire** N_1

C connaît N_1 et N_2, et peut donc simuler une fin de protocole normale aux yeux de A et B, mais en choisissant la clé reçue par B :

- $C(B) \rightarrow A : \{N_2\}_{pub(A)}$, **A termine satisfait**
- $C \rightarrow B : \{N_1, K_{bc}\}_{pub(B)}$
- $B \rightarrow A : \{N_1\}_{pub(A)}$, **message est bloqué par C. B termine satisfait en ayant reçu la mauvaise clé**

3 Conclusion

La propriété d'authentification n'est pas respectée.