L'équipe Proto-Chorale attaque le protocole A-TeamV2

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de l'attaque pour C est d'utiliser un message que A lui a destiné en l'envoyant à B comme si c'était lui qui l'avait fait.

2 Scénario de l'attaque

A entame un conversation normale avec C, que ce dernier va exploiter :

1. $A \rightarrow C : \{A, N_a\}_{pub(C)}$
2. $C \rightarrow B : \{A, N_a\}_{pub(B)}$
3. $B \rightarrow A : \{N_a\}_{N_b}, \{N_b\}_{pub(A)}$
4. $A \rightarrow C : \{secret\}_{N_b}$ **A pense toujours parler à C**
5. $C \rightarrow B : \{secret\}_{N_b}$ **B pense toujours parler à A, alors que le secret ne lui est absolument pas destiné**

3 Conclusion

La propriété d'authentification n'est ici pas respectée.