Protocoles de sécurité et vérification

attaque sur PROTOxyde d'alCO(o)L

Garance Frolla
Ely Marthouret
Ewan Decima

Équipe : ASKO OM8464A2

Septembre / Novembre 2025

Contents

1 Protocole étudié

Votre protocole:

1. $A \rightarrow S : A, \{|N_A, B|\}_{K\{AS\}}$
2. $S \rightarrow B : S, \{|N_A, A|\}_{K\{BS\}}$
3. $B \rightarrow A : B, \{N_A, N_B\}_{pub(A)}$
4. $A \rightarrow B : A, \{K, N_B\}_{pub(B)}$
5. $B \rightarrow A : B, N_B$

L'intrus I écoute les communications entre A et B et intercepte tous les termes. Avec le temps, on suppose que I connaît une ancienne clé K^*.

2 Description synthétique de l'attaque

2.1 Hypothèses

- I est capable d'intercepter et de relayer des messages
- I a obtenu, lors d'une session précédente, une ancienne clé K^*.
- Il est écrit dans vos spécifications : "Protocol fails on any side because of : incorrect content of message (pattern matching fails), incorrect key used, incorrect Nonces, etc. (as seen in classes) - then the Protocol "state" goes back to the first state it can be in."
  Mais vous ne dites pas que les agents verifient la fraîcheur des Nonces lorsqu'ils les reçoivent et ils ne vérifient pas non plus que c'est une ancienne clé ou pas (incorrect key peut juste faire référence au format ou de qui elle semble venir). Nous allons nous baser sur cette ambiguité.

2.2 Déroulement de l'attaque

Attaque : I rejoue une ancienne session en prenant le rôle de A. Les Nonces sont anciens et la clé K aussi

1. $I(A) \rightarrow S : A, \{|N_A^*, B|\}_{K\{AS\}}$
2. $S \rightarrow B : S, \{|N_A^*, A|\}_{K\{BS\}}$
3. $B \rightarrow I(A) : B, \{N_A^*, N_B^*\}_{pub(A)}$
4. $I(A) \rightarrow B : A, \{K^*, N_B^*\}_{pub(B)}$
5. $B \rightarrow A : B, N_B^*$

3 Conséquences et conclusion

À la fin de l'attaque, B croit avoir établi une communication sécurisée avec A pour la session. En réalité, la clé utilisée est une clé ancienne K^* supposée compromise.

- B pense détenir une clé K fraîche fournie par A mais a en fait accepté K^* transmis par I.
- I peut lire toutes les communications ultérieures chiffrées avec K^*.