Protocoles de sécurité et vérification

attaque sur BitSentinels

Garance Frolla
Ely Marthouret
Ewan Decima

Équipe : ASKO OM8464A2

Septembre / Novembre 2025

Contents

1 Protocole étudié **2**

2 Description synthétique de l'attaque **2**
2.1 Hypothèses 2
2.2 Déroulement de l'attaque 2

3 Conséquences et conclusion **3**

1 Protocole étudié

Nous considérons la trace suivante :

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

L'intrus I écoute les communications entre A et B et intercepte tous les termes chiffrés $\{|K|\}_{Kas}$. Avec le temps, on suppose que I connaît une ancienne clé K^* ainsi que le chiffrement associé $\{|K^*|\}_{Kas}$.

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^* et le chiffré correspondant $\{K^*\}_{Kas}$.

2.2 Déroulement de l'attaque

1. **Message 1 (initial) :** B lance une session classique en envoyant à S les éléments $\{N_b\}_{pub(S)}$, ; $\{|B|\}_{N_b}$, $\{|A|\}_{N_b}$. Ici B pense initier une session fraîche avec A.
2. **Message 2 (S envoie une clé fraîche) :** Le serveur S transmet à A (mais le message est intercepté par I qui se fait passer pour A vis-à-vis de S) : $\{|N_b|\}_{Kas}$, $\{|B|\}_{N_b}$, $\{|K|\}_{Kas}$. Ce message contient une clé fraîche K chiffrée sous le mécanisme Kas.
3. **Message 3 (substitution par I) :** L'intrus I, qui a déjà en sa possession une ancienne clé K^* (prélevée dans une communication antérieure), relaye au destinataire final A un message falsifié : $\{|N_b|\}_{Kas}$, $\{|B|\}_{N_b}$, $\{|K^*|\}_{Kas}$. Autrement dit, I remplace la portion chiffrée $\{|K|\}_{Kas}$ par $\{|K^*|\}_{Kas}$.
4. **Message 4 (A transmet l'ancienne clé à B) :** Convaincu d'avoir reçu une clé valable, A envoie à B : $\{N_b\}_{pub(B)}$, $\{K^*\}_{pub(B)}$. B reçoit donc l'ancienne clé K^* chiffrée pour lui.
5. **Message 5 (B renvoie le nonce chiffré par K^*) :** B poursuit le protocole en renvoyant $\{|N_b|\}_{K^*}$. La session suit donc, mais sur la clé ancienne K^* compromise.

3 Conséquences et conclusion

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

- A pense détenir une clé K fraîche fournie par S mais a en fait accepté K^* transmis par I.
- B croit communiquer avec A avec une clé valide et fraîche, alors qu'il s'agit de K^*.
- I peut lire toutes les communications ultérieures chiffrées avec K^*.