ASKO-OM8464A2 Attack

14 octobre 2025

1 Protocole

1.1 Description de l'attaque

Dans un premier temps, X débute une instance du protocole (rôle A) avec Y (rôle B). Le protocole se déroule comme prévu avec un attaquant I écoutant l'échange :

$$X \to Y : \{X, N_X\}_{K_{XY}}$$
$$X \to S : \{Y, \tau, \lambda, K_{XY}\}_{K_{XS}}$$

Puis l'attaquant I interrompt le message de S vers Y :

$$S \to I(Y) : \{X, \tau, \lambda, K_{XY}\}_{K_{YS}}$$

I envoie ensuite une valeur quelconque V_I à X afin de clore l'échange entre X et Y par un échec du côté de X (X tente de déchiffrer le message et ne retrouve pas $N_X + 1$).

$$I(Y) \to X : V_I$$

I va ensuite tenter de se faire passer pour Y auprès de X.
I réutilise le premier message envoyé par X et commence une nouvelle itération du protocole avec X dans le rôle B et I dans le rôle A :

$$I(Y) \to X : \{X, N_X\}_{K_{XY}}$$

I utilise ensuite la valeur interceptée lors de la dernière itération du protocole :

$$I(Y) \to S : \{X, \tau, \lambda, K_{XY}\}_{K_{YS}}$$

S pense recevoir une demande de la part de Y.
Cette attaque fait l'hypothèse qu'il n'est pas déraisonnable de lancer la procédure une deuxième fois dans la limite de temps de la première instance du protocole.
Sous cette hypothèse, S accepte le message et envoie le message suivant à X :

$$S \to X : \{Y, \tau, \lambda, K_{XY}\}_{K_{XS}}$$

X reçoit le message est l'accepte sous la même hypothèse précédemment émise.
X pense alors recevoir un message de la part de Y avec la clé K_{XY} et déchiffre le premier message reçu et trouve les valeurs suivantes : X, N_X.
La description du protocole ne spécifie cependant pas de vérification du nom du correspondant présent dans le premier message du protocole.
Ainsi même si le message envoyé par I contient le nom X celui-ci n'est pas vérifié par X et celui-ci pense toujours être en correspondance avec Y.
X envoie ensuite le dernier message du protocole intercepté par I :

$$X \rightarrow I(Y) : \{N_X + 1\}_{K_{XY}}$$

Le secret n'est pas brisé, cependant X pense avoir effectué un échange complet avec Y et pense posséder une clé correspondant à Y.
Y lui ignore tout des deux instances du protocole.
L'authentification est brisée.