Protocoles de Sécurité et Vérification
Description du Protocole

15 octobre 2025

1 Attaque du protocole ASKO OM8464A2 V1 par BitSentinels

Un attaquant I va se faire passer pour A auprès de B. I commence à envoyer un nonce qu'il connaît chiffré avec la clé K' qu'il va ensuite transmettre à B :

$$I \to B : \quad \{|A, N_I|\}_{K'}$$

I suit le protocole et envoie à S le message signifiant qu'il veut parler avec B avec un timestamp τ et un lifetime λ valide :

$$I \to S : \quad \{|B, \tau, \lambda, K'|\}_{K_{IS}}$$

Dans le précedent message I n'a pas communiqué son interlocuteur avec S. Par conséquence, S peut communiquer avec n'importe qui, par exemple B. De plus, S ne sait pas de qui vient le message qu'il a reçu, il peut choisir un expéditeur aléatoire, par exemple A. On a alors :

$$S \to I : \quad \{|A, \tau, \lambda, K'|\}_{K_{BS}}$$

B reçoit le message et le déchiffre. Il pense que A lui a envoyé la clé K'. Il peut lire premier message de A (qui avait envoyé par I). Il peut alors confirmer la réception de la clé, message que I va intercepter.

$$B \to I : \quad \{|N_I + 1|\}_{K'}$$

B pense avoir communiqué avec A alors qu'il communiquait avec I. La clé que B pense avoir reçu de A lui vient de I.

2 Contacter BitSentinels

— Vincent Poudroux : vincent.poudroux@etu.telecomnancy.univ-lorraine.fr
— Loïc Fontaine : loic.fontaine@etu.telecomnancy.univ-lorraine.fr
— Corentin Billard : corentin.billard@telecomnancy.eu