Protocole de sécurisation de gestion à distance d'un radar automatique de route

Pierre-Marie JUNGES, Florent NOSARI

19 décembre 2017

1 Présentation du protocole

1.1 But

Le but de ce protocole est de permettre la gestion à distance d'un radar automatique de route pas les autorité compétentes en ayant la certitude que les informations soient authentiques (i.e. qu'elles proviennent bien des relevés fait par le radar), que seul le gestionnaire puisse accéder au données du radar, que seul le gestionnaire puisque contrôler le radar et que toutes les informations qui transitent entre les deux soient confidentielles (i.e. qu'une tierce personne ne puisse pas y avoir accès).

En résumé :

— Les informations qui transitent doivent être confidentielles et authentiques
— Seul le gestionnaire peut contrôler le radar et accéder au données du radar

1.2 Déroulement

Le protocole est initié par le gestionnaire du radar, celui-ci utilise de la cryptographie asymétrique dans un premier temps dans le but d'échanger un clé secrète commune et continuer en cryptographie symétrique. L'authentification se fait à l'aide d'un serveur d'authentification.

L'algorithme d'échange est décrit ci-dessous :

Soient G le gestionnaire avec PKg sa clé publique et SKg sa clé privé
R le radar avec PKr sa clé publique et SKr sa clé privé
S le serveur avec PKs sa clé publique et SKs sa clé privé
K la clé secrète partagé lors d'une session

N_1 et N_2 des nonces
M un message quelconque

Les connaissances initiales sont les suivantes :

$G : \{G, R, S, SKg, PKg, PKs\}$
$R : \{R, S, SKr, PKr, PKs\}$
$S : \{S, R, SKs, PKs, PKr\}$

Le gestionnaire initie le protocole en envoyant une nonce N_1, l'identité du radar R et sont mot de passe $PSWD$ le tout chiffré par PKs.
$G \rightarrow \{N_1.R.PSWD\}\_PKs \longrightarrow S$

Si l'identité du gestionnaire est vérifiée alors le serveur envoie au radar une demande de connexion à G accompagné d'une clé secrète K, le tout chiffré par PKr et envoie K à G.
$S \rightarrow \{N_1.K\}\_PKg \longrightarrow G$
$S \rightarrow \{G.K\}\_PKr \longrightarrow R$

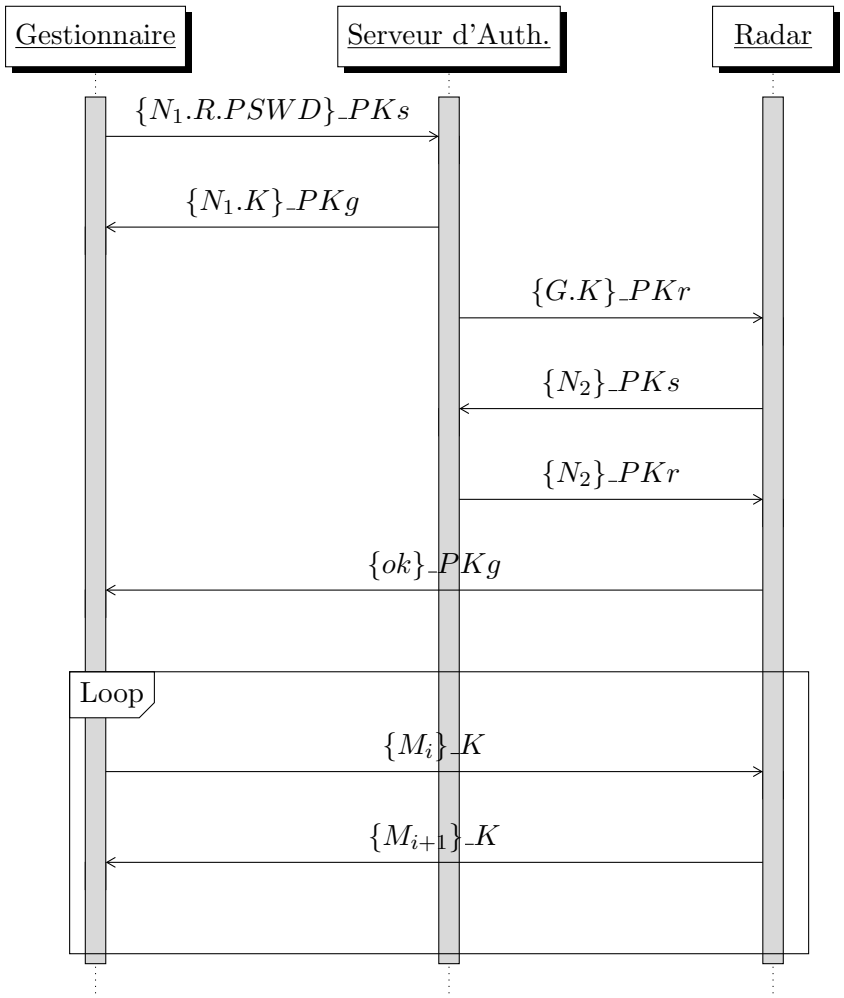
Le radar répond au serveur par un nonce N chiffré par PKs pour confirmé l'identité du serveur.
$S \longleftarrow \{N\}\_PKs \leftarrow R$

Le serveur confirme son identité au radar en renvoyant le nonce N chiffré par PKr.
$S \rightarrow \{N\}\_PKg \longrightarrow R$

Une fois l'identité du serveur vérifié, le radar indique à G que tout est ok pour communiquer.
$G \longleftarrow \{ok\}\_PKg \leftarrow R$

Une fois la clé secrète partagé, G et R l'utilise pour s'envoyer des messages M.

$G \leftrightarrow \{M\}\_K \leftrightarrow R$


Gestionnaire
Serveur d'Auth.
Radar
$\{N_1.R.PSWD\}\_PKs$
$\{N_1.K\}\_PKg$
$\{G.K\}\_PKr$
$\{N_2\}\_PKs$
$\{N_2\}\_PKr$
$\{ok\}\_PKg$
Loop
$\{M_i\}\_K$
$\{M_{i+1}\}\_K$