RFC 5191 : Protocol for Carrying Authentication for Network Access (PANA)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 mai 2008

Date de publication du RFC : Mai 2008

https://www.bortzmeyer.org/5191.html

PANA est un protocole conçu pour transporter un protocole d'authentification lors d'accès à un réseau, EAP. Le RFC 5193 [1] donne une vision de haut niveau de PANA, notre RFC 5191, quant à lui, définit en détail le protocole. Comme l'indiquent les appartenances des auteurs, PANA et EAP sont surtout utilisés dans le monde de la téléphonie mobile.

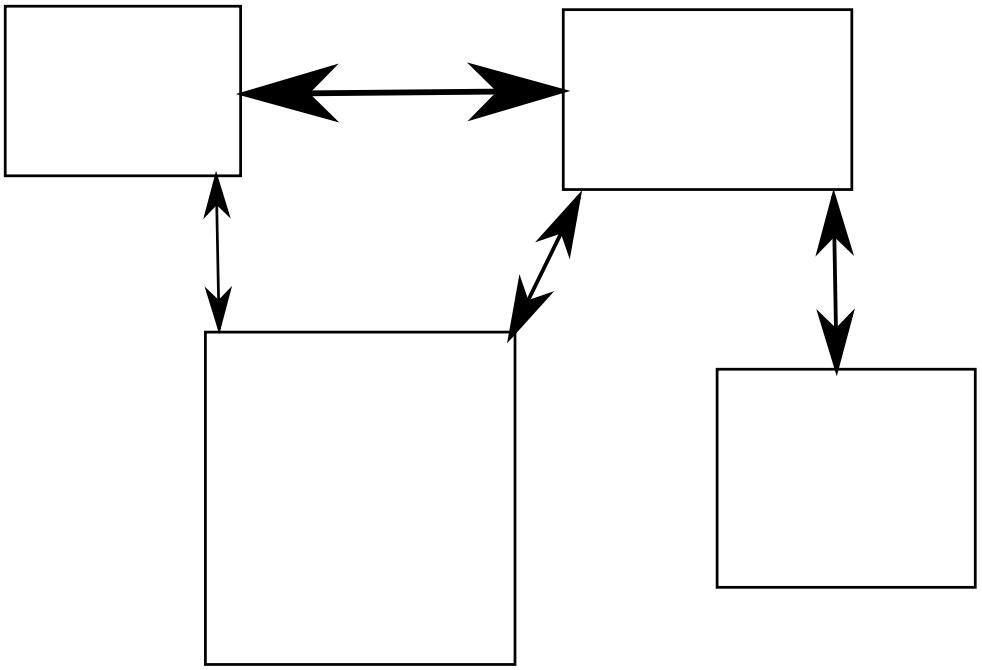
PANA est assez simple : les messages EAP (RFC 3748) sont encapsulés dans les messages PANA, qui sont transportés sur UDP. PANA ne fait pas d'authentification lui-même, il transporte juste des paquets. Les méthodes d'authenfication sont donc complètement extérieures à PANA.

La section 2 décrit la terminologie de PANA, pour laquelle il vaut mieux se référer au RFC 5193. La machine qui veut accéder au réseau (par exemple un téléphone portable) est le client PANA, le **PaC**. La machine avec laquelle elle parle est le serveur PANA, le **PAA**. Pour prendre sa décision, ce serveur va souvent parler à un serveur AAA, par exemple avec la protocole Radius (RFC 2865). Une fois l'authentification terminée, le trafic réel passera par un routeur ou autre machine d'accès, l'**EP**. Souvent, EP et PAA seront dans la même boîte et communiqueront via une API

La section 3 résume le protocole : les dialogues PANA sont composés de requêtes et de réponses, chaque message portant ou ou plusieurs AVP. Le transport utilisé est UDP, choisi pour sa simplicité de mise en œuvre.

Puis la section 4 détaille le protocole. Le PaC ou le PAA peuvent être à l'origine du dialogue. Lorsque le PaC veut s'authentifier (section 4.1), il envoie une requête `PANA-Client-Initiation` au PAA.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5193.txt`



Notez que le mécanisme de découverte du PANA n'est pas spécifié ici (une solution possible est décrite dans le RFC 5192). Le PAA répond alors avec une `PANA-Auth-Request`, qui porte la charge EAP. Un échange de messages `PANA-Auth-Answer` et `PANA-Auth-Request` suivra alors, jusqu'à ce qu'EAP aie terminé. (La liste complète des messages possibles figure dans la section 7.) Si l'authentification est un succès, le dernier message peut également contenir des consignes pour le PaC comme de reconfigurer son adresse IP. Les autres sous-sections de la section traitent de la ré-authentification en cours de session ou bien de la terminaison de la session.

La section 5 précise les règles de traitement des messages, notamment en cas de perte de paquets (UDP ne promettant pas de délivrer tous les paquets). Chaque participant au dialogue PANA doit maintenir une séquence numérotée des paquets, pour pouvoir détecter et corriger une perte. La même section explique aussi comment s'assurer de l'intégrité des messages, via un hachage cryptographique.

Le format exact des messages est normalisé dans les sections 6 et 8, qui présentent les AVP, qui sont très proches de ceux du RFC 3588.

Vu le but de PANA, transporter un protocole d'authentification, il n'est pas étonnant que la section sur la sécurité soit détaillée. Cette section 11 du RFC explique donc les mécanismes qui, de concert avec ceux d'EAP, vont permettre d'utiliser PANA même sur un réseau peu sûr.