RFC 4058 : Protocol for Carrying Authentication for Network Access (PANA) Requirements

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 janvier 2007

Date de publication du RFC : Mai 2005

https://www.bortzmeyer.org/4058.html

Beaucoup de protocoles IETF ont besoin de faire de l'authentification. Traditionnellement, chacun le fait à sa manière et introduit ses propres bogues. D'où l'effort actuel de rationalisation dont le projet PANA, introduit par ce RFC, est une partie.

Actuellement, il existe de nombreux protocoles pour gérer l'authentification du client qui veut accéder à un réseau. Par exemple, si on veut empêcher que toute machine qui se connecte à un commutateur Ethernet puisse envoyer des paquets, on peut utiliser 802.1X. De même, lorsqu'on se connecte à un point chaud WiFi ou depuis sa chambre d'hôtel, on est souvent redirigé vers une page Web d'authentification (technique du « portail captif »). Ces protocoles sont souvent spécifiques à un type de média particulier et chacun d'eux « réinvente la roue » en redéveloppant fonctions et protocole les utilisant. Or, en matière de sécurité, cette approche est dangereuse : chaque protocole va devoir faire l'objet d'une analyse de sécurité séparée. D'où l'idée de factoriser certaines fonctions courantes et c'est le but du projet PANA.

Notre RFC expose le cahier des charges pour PANA : le futur protocole servira uniquement de transport au vrai protocole d'authentification, par exemple EAP (RFC 3748 [1]). PANA circulera sur IP, ce qui garantit son indépendance par rapport au média.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3748.txt