RFC 5386 : Better-Than-Nothing-Security: An Unauthenticated Mode of IPsec

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 novembre 2008

Date de publication du RFC : Novembre 2008

https://www.bortzmeyer.org/5386.html

Le protocole BTNS ("*Better Than Nothing Security*"), expliqué dans le RFC 5387 [1], est normalisé dans ce RFC 5386. Il permet d'utiliser IPsec sans authentification des autres machines, ce qui pourrait simplifier son déploiement.

BTNS ne change pas le protocole IPsec (RFC 4301), ni les protocoles associés comme IKE (RFC 4306). Sur le câble, ce sont les mêmes paquets qui passent, les changements se concentrant sur les machines terminales, dans la PAD ("*Peer Authentication Database*", section 4.4.3 du RFC 4301) et la SPD ("*Security Policy Database*", section 4.4.1 du RFC 4301).

Ce RFC reste assez court car il ne normalise pas encore toutes les idées prévues dans le RFC 5387 comme par exemple la liaison entre une SA ("*Security Association*") IPsec et une connexion dans les couches hautes (cf. section 4.1) ou comme la mémoire des SA précédentes, pour n'avoir à faire confiance à un inconnu que la première fois (cf. section 4.2, qui propose un futur mécanisme analogue à celui de SSH).

La section 2 décrit BTNS par rapport à l'IPsec traditionnel. Le principal changement est que, **après** l'examen de toutes les entrées de la PAD, une implémentation de BTNS peut simplement accepter un pair uniquement pour sa clé publique, ou même pour n'importe quelle clé (cas où on accepte les connexions de tout le monde).

La section 3 décrit quelques exemples de scénarios avec BTNS. Ainsi, 3.3 décrit un serveur NFS qui veut protéger le trafic NFS avec IPsec, tout en acceptant n'importe quel client NFS (accepter au niveau IPsec : les couches hautes peuvent toujours imposer une authentification). La PAD ("*Peer Authentication Database*") ressemblera à :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5387.txt

```
Rule Remote ID        IDs allowed  SPD Search by
---- ---------        -----------  -------------
 1   PUBLICKEY:any    ANY          by-IP
```

(Une seule règle, accepter tout le monde. Une telle règle n'était pas possible en IPsec avant BTNS.) Et la SPD ("*Security Policy Database*") pourra être :

```
Rule Local Remote Next Layer BTNS  Action
       addr  addr   Protocol   ok
---- ----- ------ ---------- ----  ----------------------
 1    [C]    ANY      ANY      yes  PROTECT(ESP,transport,
            with                                integr+conf)
            port
            2049

 2    [C]    ANY      ANY      N/A  BYPASS
```

(Utilisation IPsec, avec protection ESP pour le port 2049 (NFS) et ne pas toucher aux autres applications.)

La section 4 revient sur les problèmes de sécurité déjà étudiées dans la section 5 du RFC 5387. BTNS est notamment vulnérable aux attaques d'un attaquant situé au milieu.