RFC 4766 : Intrusion Detection Message Exchange Requirements

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 mars 2007

Date de publication du RFC : Mars 2007

https://www.bortzmeyer.org/4766.html

L'Internet d'aujourd'hui est un coupe-gorge où les attaques sont de plus en plus fréquentes et de plus en plus complexes ? Raison de plus pour échanger de l'information entre ceux qui se chargent de défendre le réseau. Cela nécessitera un format standard d'échange, dont ce RFC dresse le cahier des charges.

Le groupe de travail IDWG de l'IETF était chargé de réaliser ce format d'échanges standard, qui devait permettre d'échanger sous une forme normalisée les informations sur les attaques ou les repérages trop appuyés ("*port scan*", par exemple). Actuellement, les outils d'analyse comme les IDS et les programmes utilisés par les responsables de la sécurité ne communiquent qu'avec des formats non normalisés. C'est gênant et c'est encore plus gênant lorsqu'on veut communiquer cette information à d'autres entités (police, CERT, autres victimes) ou bien lorsqu'on veut l'archiver.

Outre le format des données, le groupe travaillait aussi sur un protocole d'échange de ces données et notre RFC couvre les deux.

D'où ce cahier des charges qui prévoit que le nouveau format :

— Transmette des faits, pas des méthodes de détection,
— Attribue à chaque évenement de sécurité un identificateur unique,
— Puisse transporter des données de type non spécifié (car le RFC ne peut pas tout prévoir),
— Indique la source et la destination de l'attaque,
— Indique l'analyseur (typiquement un IDS) qui a fait le rapport,
— Indique le degré de confiance que l'analyseur a dans sa propre analyse,
— Indique évidemment l'heure,
— Fournisse un mécanisme d'extension, pour indiquer des données structurées non prévues à l'origine.

Le protocole, quant à lui, doit fournir la confidentialité, l'intégrité des données transmises et leur authentification.

Le groupe de travail a malheureusement échoué et les deux RFC décrivant le protocole ont été publiés « en l'état », avec le simple statut d'« Expérimental ». Ce sont le RFC 4765 [1] pour le format et le RFC 4767.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4765.txt