RFC 8248 : Security Automation and Continuous Monitoring (SACM) Requirements

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 septembre 2017

Date de publication du RFC : Septembre 2017

https://www.bortzmeyer.org/8248.html

Le groupe de travail SACM <https://datatracker.ietf.org/wg/sacm/about/> de l'IETF bosse sur une architecture, un modèle de données, et des protocoles pour suivre l'état de la sécurité de ses machines. Ceci est son deuxième RFC, qui vise à définir le cahier des charges de la future solution.

Le cœur de cette idée est l'évaluation de la sécurité sur chaque machine du réseau. Il faut la déterminer, et acheminer le résultat jusqu'aux responsables de la sécurité. Cela nécessite donc un modèle de données (comment on décrit « la sécurité d'une machine » ?) puis un protocole permettant de gérer un très grand nombre de machines. Parmi les informations à récolter sur chaque machine, on trouvera évidemment la liste des logiciels installés, les logiciels serveurs en activité qui écoutent sur le réseau, l'état de la mise à jour (« pas pu joindre le dépôt officiel de logiciels depuis N jours »), etc. Le cahier des charges décrit dans ce RFC part des scénarios d'usage du RFC 7632 [1]. Ce sont souvent de grandes généralités. On est loin de mécanismes concrets.

La section 2 forme l'essentiel de ce RFC, avec la liste des exigences du cahier des charges. Je ne vais en citer que quelques unes. La première, nommée G-001 (« G » préfixe les exigences générales sur l'ensemble du système SACM), demande que toute la solution SACM soit extensible, pour les futurs besoins. G-003 est la possibilité de passage à l'échelle. Par exemple, les messages échangés peuvent aller de quelques lignes à, peut-être plusieurs gigaoctets si on fait une analyse détaillée d'une machine. Et il peut y avoir beaucoup de machine avec des échanges fréquents (le RFC n'est pas plus précis sur les chiffres).

Les données traitées sont évidemment sensibles, et G-006 demande que la solution permette évidemment de préserver la confidentialité des données.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7632.txt

Les exigences sur l'architecture de la future solution sont préfixées de « ARCH ». Ainsi, ARCH-009 insiste sur l'importance d'une bonne synchronisation temporelle de toutes les machines. Un journal des connexions/déconnexions des utilisateurs, par exemple, n'aurait guère d'intérêt si l'horloge qui sert à l'estampiller n'est pas exacte.

D'autres sections décrivent les exigences pour le modèle de données et pour les protocoles, je vous laisse les découvrir.