Utilisation de la notion de Provenance pour la détection d'intrusion

Encadrant : Eric Totel

Les attaques contre les systèmes informatiques deviennent de plus en plus complexes. Il est nécessaire d'offrir des outils à l'analyste pour mieux détecter et comprendre les attaques. Bates et al., « Trustworthy Whole-System Provenance for the Linux Kernel » ont développé un système sous Linux permettant de suivre les informations dans le système pour pouvoir déterminer d'où provient une information. Ces travaux ont mené à un article sur les enjeux de l'utilisation de cette notion de provenance en détection d'intrusion.

Le but de ce projet est de mettre en place sous Linux les modules de provenance et de montrer s'il a un sens en détection d'intrusion, ou non.

Références

Bates, Adam, Dave (Jing) Tian, Kevin R. B. Butler, et Thomas Moyer. « Trustworthy Whole-System Provenance for the Linux Kernel », 319-34, 2015. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/bates.

Han, Xueyuan, Thomas Pasquier, et Margo Seltzer. « Provenance-Based Intrusion Detection: Opportunities and Challenges ». *ArXiv:1806.00934 [Cs]*, 3 juin 2018. http://arxiv.org/abs/1806.00934.