Le système d'exploitation Qubes ; plus sûr ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 mai 2010. Dernière mise à jour le 26 mai 2010

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

La sécurité du PC de M. Michu, lorsque ce PC est connecté à l'Internet, est très menacée, c'est bien connu. Dès que M. Michu surfe, lit son courrier (« *"Enlarge your penis and make money fast!!!"* »), ou télécharge une vidéo, son PC est infecté, son numéro de carte bleue est transmis à la division financière de l'APL, ses données personnelles aux spammeurs ukrainiens et sa machine, devenue un zombie, va participer aux attaques DoS contre le site Web de Chantal Jouanno. Peut-on améliorer la sécurité de ce pauvre ordinateur par des moyens techniques, par exemple par de meilleurs systèmes d'exploitation ? C'est ce que pensent les promoteurs du système Qubes <http://www.qubes-os.org/>.

Une grande partie de la vulnérabilité du PC de M. Michu vient du système d'exploitation utilisé, MS-Windows, véritable nid à "*malware*", notamment par l'absence de protections sérieuses (celles qui existent, par exemple la séparation du rôle Administrateur, ne sont souvent pas utilisées). A priori, faire plus sûr que Windows ne semble pas un exploit insurmontable.

Néanmoins, le problème est plus complexe que cela. Imaginons qu'on remplace MS-Windows par un système sérieux, par exemple un Unix. Certes, le piratage du compte de M. Michu ne donnera pas au pirate l'accès `root`. Mais une faille dans le navigateur (et le navigateur, étant une usine à gaz très complexe, a forcément des failles) donnera quand même accès à Facebook, aux comptes bancaires, etc.

Il existe aujourd'hui des dizaines de projets de recherche sur ce thème des « systèmes d'exploitation sûrs ». Certains ne dépasseront pas le stade du "*vaporware*" (cela sera sans doute le cas d'Ethos <http://www.zdnet.com/blog/security/researchers-get-funding-to-build-new-secure-os/6087> : plus il y a de PowerPoint, moins il y a de réalisations concrètes). Tous reposent sur l'idée de virtualisation et de compartimentalisation du système en plusieurs sous-systèmes relativement étanches entre eux. L'idée est que M. Michu surfera sur des sites de cul depuis une VM (machine virtuelle), accèdera à Facebook depuis une autre, se connectera à sa banque depuis une troisième, etc. Ainsi, la compromission de la VM « sites de cul » n'entrainera pas d'attaques sur le compte en banque. Ce concept se rapproche de celui utilisé dans le domaine militaire avec la séparation des ressources selon leur niveau de sécurité (« Très secret », « Secret », « Confidentiel », etc). Vouloir faire du logiciel sans bogues étant illusoire, le travail se concentre sur la limitation des dégâts en cas de bogue.

Sur le papier, c'est très séduisant. Dans la pratique, toute la difficulté est de permettre quand même une communication entre les VM. Car, sinon, on ne pourra pas envoyer une image depuis la VM « sites de cul » vers la VM « réseaux sociaux ». Et beaucoup de bonnes idées en terme de sécurité ont été des échecs car on ne prêtait pas suffisamment attention à l'utilisabilité.

Le système Qubes <http://www.qubes-os.org/>, fondé sur Linux pour le noyau et Xen pour la virtualisation, s'attaque à ce problème en prévoyant une interface graphique partagée par toutes les VM mais avec une communication sous-jacente passant par un protocole nouveau, très simple et mis en œuvre par du code sévèrement audité. L'article « "*Qubes OS architecture*" <http://qubes-os.org/files/doc/arch-spec-0.3.pdf> » décrit l'architecture générale de Qubes, avec beaucoup de détails pratiques (contrairement à d'autres projets qui n'ont fait que des conférences de presse).

Cette compartimentalisation laisse un autre problème, encore plus difficile : une VM infectée peut être dangereuse pour l'Internet, même si elle ne peut pas attaquer les autres VM.

Outre le site officiel, les curieux trouveront une bonne introduction dans l'interview de Joanna Rutkowska <http://www.securabit.com/2010/05/20/interview-with-joanna-rutkowska/>, une des conceptrices (et une experte en attaques contre les processeurs), les développeurs trouveront plus de détails à jour sur le Trac <http://www.qubes-os.org/trac/wiki>. Un excellent exemple de découpage d'une installation Qubes en domaines de sécurité variée est donné dans « "*Partitioning my digital life into security domains*" <http://theinvisiblethings.blogspot.com/2011/03/partitioning-my-digital-life-into.html> ». Autre document intéressant, un interview de Joanna Rutkowska <http://www.securabit.com/2010/05/20/interview-with-joanna-rutkowska/>. Un très bon compte-rendu d'essaie de Qubes a été publié sur LinuxFr <https://linuxfr.org/news/qubesos-1-0>.