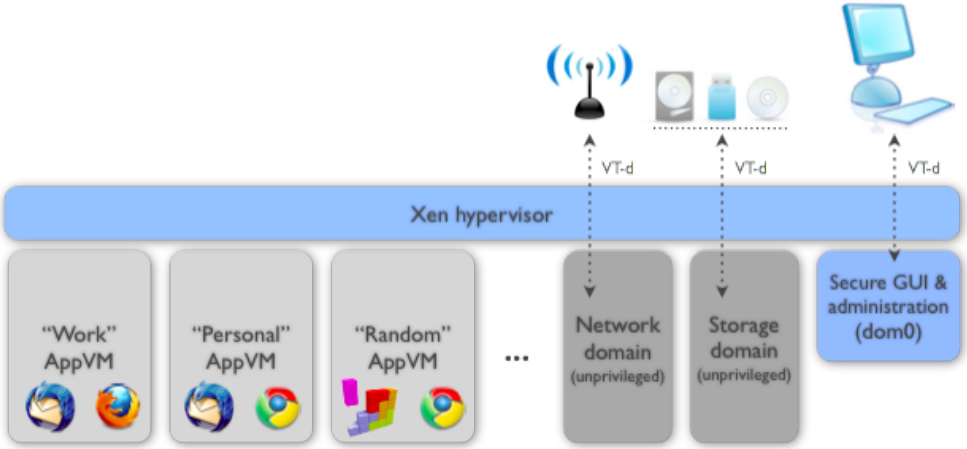
Qubes - le système d'exploitation qui peut vous protéger même si vous avez été piraté



Nous avions écrit sur l'importance du système d'exploitation Tails à tous les journalistes de la NSA, la semaine dernière, mais il existe aussi un autre système d'exploitation peu connu que les journalistes devraient envisager d'utiliser si ils se trouvent dans des situations à haut risque. Il s'appelle Qubes.

J'utilise Qubes seulement depuis quelques semaines, mais je sens que mon système d'exploitation est maintenant une forteresse numérique. Je vais essayer d'expliquer pourquoi et comment Qubes diffère de Tails.

La conception de Qubes est basé sur une loi importante du logiciel : tous les programmes contiennent des bugs. Certains d'entre eux sont des failles de sécurité. Votre ordinateur peut être piraté par le visionnage d'une vidéo Flash ou en utilisant javascript dans votre navigateur Web : il est probable que ce soit que la façon dont les programmes QUANTUM / FOXACID de la NSA piratent les personnes. Votre ordinateur pourrait également être piraté par l'ouverture d'un fichier PDF ou un document Microsoft Word ou LibreOffice, ou tout simplement par l'affichage d'un JPG ou GIF.

Si un morceau de logiciel est compromis, c'est l'ensemble de votre ordinateur qui est compromis. L'attaquant peut alors regarder vos fichiers, voir vos frappes au clavier, prendre des captures d'écrans, voler vos clés de chiffrement, et lire les e-mails que vous tapez avant même que vous ayez une chance de les chiffrer.

Les développeurs peuvent (et doivent) essayer de rendre leurs logiciels plus sûr, mais les logiciels ne seront jamais parfait. Essayer de ne pas se faire piraté est difficile quand vous avez des adversaires puissants, mais il faut pouvoir faire son travail. Assez proche de l'absence de connexion à Internet, la meilleure façon de rester en sécurité est de minimiser les dommages causés lorsque vous serez éventuellement piraté et de mettre en "sandbox"/"bac à sable" les programmes les plus vulnérables, les compartimentant du reste de votre ordinateur. Qubes rend cette chose possible de la façon la plus simple que n'importe quel autre système d'exploitation que j'ai pu utilisé.

Qubes utilise des machines virtuelles pour vous permettre de gérer des "domaines de sécurité" séparés. Une machine virtuelle (VM) est essentiellement un système d'exploitation minuscule qui tourne à l'intérieur de votre système d'exploitation réel. Si votre VM est piraté, l'attaquant est en mesure d'accéder aux fichiers et de lire les frappes claviers au sein de cette VM, mais pas dans les 'autres machines virtuelles ou sur votre ordinateur hôte. Dans Qubes tous les logiciels (en plus de l'environnement de bureau) sont en cours d'exécution à l'intérieur de machines virtuelles, et vous pouvez facilement et efficacement en faire autant que nécessaire. Il est également conçu de manière à ce que si l'on est infecte une VM avec des logiciels malveillants, les logiciels malveillants ne seront plus

là la prochaine fois que vous redémarrez votre VM.

Par exemple, vous pouvez utiliser Pidgin, une application de messagerie instantanée avec fonction de chiffrement OTR, pour discuter avec des personnes en toute sécurité. Mais Pidgin est tristement célèbre pour ses vulnérabilités de corruption mémoire : le genre de bug que les attaquants peuvent utiliser pour prendre contrôle de votre ordinateur, en vous envoyant un message particulier. (Toutes les vulnérabilités de Pidgin connus du public ont été corrigées si vous utilisez la dernière version, mais il ya toujours la possibilité qu'il existe des vulnérabilités qui n'ont jamais été signalées aux développeurs. Elles sont appelées vulnérabilités "zero day", et des organismes comme la NSA et le FBI dépensent beaucoup d'argent pour acheter des informations à leur sujet).

Pour utiliser Pidgin aussi sûrement que possible, vous pouvez créer un AppVM (le mot Qubes pour désigner une VM exécutant des applications spécifiques) que vous utilisez uniquement pour Pidgin. Si un attaquant utilisant une faille zero-day de Pidgin vous envoie un message bizarre pour tenter de prendre le contrôle de votre ordinateur, tout ce qu'il aura effectivement pu faire et de prendre le contrôle du Pidgin virtualisé. Le pire que l'attaquant puisse faire est de voler vos clés OTR et d'espionner vos conversations en ligne. Tout le reste se trouvant sur votre ordinateur, tels que vos documents de travail, votre clé PGP, et votre base de données de mots de passe, restera à l'abri de l'attaquant.

Un autre exemple qui serait utile aux journalistes : si vous écrivez un article au sujet des documents sensibles, vous pouvez créer un AppVM dédié qui contiendra ces documents, et tous les fichiers ou projets liés. Si vous ouvrez un document dans cette AppVM, et que ce document tente de contacter quelqu'un pour l'alerter qu'il a été ouvert, il va échouer parce que ce AppVM n'a pas accès à Internet. Et si vous ouvrez un document malveillant qui hacks cette AppVM, le malware ne sera pas en mesure d'exfiltrer un de vos fichiers, car il n'aura pas accès à Internet. Et enfin, si une autre partie de vos ordinateurs est compromis, comme votre navigateur Web, les attaquants n'auront pas accès à ces fichiers de travail sensibles.

Vous pouvez aussi facilement utiliser des "machines virtuelles jetable", des AppVMs que vous créez dans un but spécifique et pour ensuite les supprimer lorsque vous avez terminé avec eux, pour ouvrir des documents auxquels vous ne faîtes pas confiance. Si le PDF que l'on vous a envoyé par courriel est réellement malveillant et essaie de prendre le contrôle de votre ordinateur, il ne le fera que sur la VM jetable. Mais si ce document contient quelque chose d'utile, vous serez toujours en mesure de le lire.

Vous pouvez le faire sur un seul ordinateur en utilisant un gestionnaire de bureau unique. C'est l'une des fonctionnalités les plus puissantes sur Qubes.

Vous pouvez toujours choisir d'isoler un logiciel sur des systèmes d'exploitation traditionnels en utilisant des outils comme VirtualBox ou VMWare, mais il vous sera impossible de faire un aussi bon travail de verrouillage de votre ordinateur que vous pouvez le faire avec Qubes.

L'état actuel du projet

En ce moment, vous devez être technophiles afin de tirer parti de tous les avantages de Qubes. Et ce n'est pas compliqué si vous êtes déjà un nerd Linux. Je pense que cela peut être amélioré, mais Qubes ne serai jamais un outil de sécurité que l'on "allume et oublie". Dans le domaine de la sécurité, chaque besoin utilisateur dépend entièrement de ses préférences et ses besoins de sécurité. Mais si vous connaissez vos besoins et comprenez comment utiliser et configurer les AppVMs pour les adapter, vous serez en mesure d'utiliser votre ordinateur en toute sécurité, dans une sécurité beaucoup plus élevé que si vous utilisiez un système d'exploitation traditionnel.

Un des usages qui pourrait être grandement améliorée est celui du support matériel au sein des machines virtuelles. J'ai passé des heures à essayer de comprendre comment faire fonctionner la webcam interne de mon ordinateur portable au sein d'une AppVM. La solution finalement fini par être de donner le contrôle de mon contrôleur USB à l'AppVM et de modifier les permissions sur / dev/video0 afin qu'il soit accessible en écriture à l'intérieur de la AppVM - au détriment d'avoir accès à un des ports USB, et en créant donc d'autres problèmes de sécurité liées à l'USB (que les OS normaux ont par défaut). Les problèmes matériels continuent pour moi : les clés USB fonctionnent très bien, mais les cartes ethernet USB non ; je ne peux pas facilement importer des photos depuis mon téléphone Android. J'ai assez de patience, de recherche google, et d'expérience Linux pour les résoudre, mais je pense que de nombreux utilisateurs seront perdus.

Qubes vs Tails ?

Qubes et Tails sont fondamentalement différents dans leurs cas d'utilisation. Ils sont tous les deux très important, et j'utilise les deux systèmes d'exploitation tous les jours.

Tails permet de rester anonyme. Lorsque vous l'utilisez sur un ordinateur, il ne laisse pas de trace comme quoi il a démarré. Il change votre adresse MAC avant de vous connecter à un réseau, et il oblige tout le trafic réseau à passer par Tor, veille à ce que vous ne ferez pas d'erreur technique laissant fuiter accidentellement votre adresse IP. Lorsque vous utilisez le navigateur Web fournit dans Tails, votre trafic ressemble exactement à celui de tous les autres utilisateurs de Tor.

Qubes est pour être sécurisé tout en étant capable d'utiliser une grande variété de logiciels qui pourraient contenir des failles de vulnérabilités zero-day, mais ce n'est pas pour rester anonyme. Qubes supporte des astuces de modification du réseau, comme faire un AppVM où tout le trafic est obligé de passer par Tor, mais il n'intègre pas la plupart des techniques d'anonymisation pour lesquelles Tails excelle.

L'essentiel

Pour une sécurité maximale, je recommande aux gens d'utiliser Qubes sur leur ordinateur pour tous leurs besoins, non anonymes, de tous les jours : relever ses mails, le Chat, utiliser les réseaux sociaux et la navigation sur le web, développement de logiciels, faire de la recherche, la rédaction d'articles. Si faites tout votre travail dans des AppVMs qui exécutent Linux (et éventuellement dans des AppVMs qui exécutent Windows), vous aurez les versions les les plus récentes et les meilleurs outils pour travailler avec, et il est simple d'installer de nouveaux logiciels. Pour des besoins plus sensibles où l'anonymat est important, vous pouvez utiliser le Tor Browser Bundle à l'intérieur d'un AppVM.

Et pour les besoins les plus sensibles, comme les journalistes visés par la NSA, vous devez utiliser Tails.