Détecter et survivre aux intrusions : exploration de nouvelles approches de détection, de restauration, et de réponse aux intrusions

Ronny Chevalier[1]

La sécurité des ordinateurs repose classiquement sur des mécanismes de sécurité préventifs, tels que la cryptographie ou le contrôle d'accès, afin de réduire la probabilité qu'une attaque réussisse. Néanmoins, des intrusions surviennent toujours en raison, par exemple, de vulnérabilités résiduelles. Par conséquent, nous devons construire les ordinateurs afin qu'ils puissent non seulement prévenir, mais aussi détecter une intrusion et y survivre.

Dans cette thèse, nous nous intéressons au système d'exploitation (OS) et au logiciel embarqué dans le matériel (BIOS) dont dépend la sécurité des applications. Un OS est aujourd'hui capable de détecter des intrusions, mais sa capacité à y survivre (continuer à délivrer un service malgré une intrusion) est limitée. Nous proposons ainsi une approche où un OS vulnérable peut fournir un service dégradé, afin d'attendre la correction des vulnérabilités. Cette approche minimise l'impact sur la disponibilité tout en maximisant la sécurité. Un BIOS, en revanche, a une capacité de détection limitée alors que des attaquants tentent d'y implanter des logiciels malveillants. C'est pourquoi nous proposons une approche de détection au niveau du BIOS.

1. Thèse soutenue le 17 décembre 2019, préparée au sein de l'équipe CIDRE (équipe mixte CentraleSupélec, Inria, CNRS, Université de Rennes 1, et membre de l'IRISA) et du laboratoire de sécurité de HP Labs, sous la direction de Ludovic Mé (Inria), co-encadrée par Guillaume Hiet (CentraleSupélec) et Boris Balacheff (HP Labs), et en collaboration avec David Plaquin (HP Labs, Bristol, UK). Document disponible à l'adresse `https://hal.inria.fr/tel-02417644`.