

Méthode générique d'inversion du packing

Thématique : Sécurité/cryptologie

Institut : INRIA Nancy grand Est -- Nancy université.

Équipe / projet : EPI Carte -- Laboratoire de haute sécurité

Directeur de stage : Jean-Yves Marion <jean-yves.marion@loria.fr> (PR) et Matthieu Kaczmarek <matthieu.kaczmarek@loria.fr> (Ingénieur LHS-INRIA)

Directeur du laboratoire : Karl Tombre <karl.tombre@loria.fr>

Lien : <http://lhs.loria.fr/> (avec d'autres sujets)

Contexte du stage

Ce stage s'inscrit dans la mise en œuvre du laboratoire de haute sécurité (LHS) en informatique du LORIA. Les objectifs du LHS sont de conduire certaines expérimentations liées à la sécurité informatique, et plus particulièrement à la virologie. Cette plateforme de recherche est unique dans le monde académique et offre de nombreuses opportunités. Ce stage pourra déboucher sur une thèse. Un financement de thèse est déjà assuré.

Description du domaine

Le packing est une méthode de protection des programmes procédant par chiffrement du code. Lors de l'exécution le code est déchiffré dynamiquement afin de retrouver la fonctionnalité initiale du programme packé. Ce procédé est souvent utilisé par les auteurs de programmes malicieux afin de complexifier l'analyse antivirus, afin d'analyser un programme packé un anti-virus doit au préalable déchiffrer le code. Dans l'industrie antivirus, les procédures d'inversion du packing sont écrites manuellement. Cette tâche fastidieuse retarde la mise à jour d'un antivirus lors d'une nouvelle attaque virale.

Objectifs du stage

Le sujet du stage consiste à établir une méthode générique d'inversion du packing. Toutes les informations nécessaires au déchiffrement sont présentes dans le programme packé puisque ce dernier doit être capable de se déchiffrer lors de son exécution. Ainsi, une analyse statique couplée à des méthodes d'exécution symbolique devrait permettre de générer à la volée des procédures d'inversion. Même si ce thème de recherche a souvent été évoqué par la communauté, à l'heure actuelle aucune solution robuste n'existe. Ce stage vise à concevoir un cadre formel pour le déchiffrement automatique de programmes packés. Le stagiaire devra non seulement définir un modèle théorique solide pour modéliser ce processus mais aussi fournir une preuve de concept fonctionnelle sur un échantillon de programmes malicieux réels. La partie expérimentale sera réalisée dans au sein du laboratoire de haute sécurité au Loria.

Compétences

Le stagiaire devra manipuler des concepts théoriques et les mettre en œuvre par l'expérience. Par conséquent, il devra posséder un bagage théorique solide mais aussi faire preuve d'aisance en programmation. A titre indicatif le sujet met en jeu les compétences suivantes. Elles ne sont pas requises, le stagiaire pourra les acquérir au cours du séjour : Cryptographie, analyse statique, analyse dynamique, ingénierie inverse, techniques antivirales.

Bibliographies

- Server-Side Dynamic Code Analysis, W. Guizani, JY Marion et D. Reynaud, Malware 2009, Montréal.
- Architecture of a morphological malware detector, . G. Bonfante, M. Kaczmarek, and JY Marion. Journal in Computer Virology 5(3): 263-270 (2009).
- Dynamic Binary Instrumentation for Deobfuscation and Unpacking, D. Reynaud and JY Marion, DeepSec 2009, Vienne.