Reverse engineering: Black-box deobfuscation

Grégoire MENGUY
CEA LIST
gregoire.menguy@cea.fr

Un programme peu contenir de nombreux secrets comme des clés privées ou des algorithmes propriétaires. Un attaquant peu ainsi les voler en rétro-ingéniant le code. L'*obfuscation* propose de protéger les secrets contenus dans le programme en empêchant sa rétro-ingénierie. Elle transforme le programme original en un programme équivalent mais beaucoup plus difficile à comprendre. A l'inverse, la *déobfuscation* tente de simplifier un programme obfusqué pour retrouver une version proche de l'originale. L' évolution des méthodes de déobfuscation a ainsi de nombreuses implications en sécurité. D'un coté, cela permet de mieux estimer la robustesse des protections existantes, améliorant la sécurité des programmes. De l'autre, elle aide à analyser les logiciels malveillants, usuellement obfusqués.

Récemment, les approches en boîte noire, se reposant sur de la synthèse de code se sont révélées très efficaces et ont permis de simplifier drastiquement des programmes obfusqués avec des obfuscateurs complexes comme VMProtect ou Tigress. Ce projet propose d'appliquer Xyntia, le framework de déobfuscation en boîte noire à l'état de l'art, sur des programmes provenant de différents domaines (cryptographe, malware, jeux vidéo etc) pour comprendre les limites actuelles de l'approche et proposer des extensions.

Le projet set déroulera comme suit:

- Étudier et comprendre les méthodes de déobfuscation boîte noire à l'état de l'art;
- L'évaluer sur un jeu de donné de codes réels ou synthétiques pour étudier ses forces et ses limitations dans un contexte donné (*virtualization*, etc);
- Proposer une extension pour pallier à ces limitations et l'implémenter dans Binsec;[1]
- Évaluer cette extension pour prouver son efficacité en pratique.

1 Livrables attendus

Les principaux livrables attendus sont:

- Un résumé des recherches bibliographiques menées;
- Une implémentation documentée de l'extension proposée;
- Le rapport final incluant les deux premiers livrables et le récapitulatif des démarches suivis et des résultats obtenus.

2 Éléments logistiques

Des points réguliers seront organisés avec l'encadrement. Ils pourront être réalisés en visioconférence ou au CEA sur le site Nano-Innov à Saclay.

3 Postuler

Pour postuler, les étudiants doivent contacter l'encadrant par mail.

[1] Framework open source d'analyse de binaire développé au CEA: https://binsec.github.io/