Reverse engineering: White-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. À 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, le backward-bounded symbolic execution (BBSSE) s'est révélé particulièrement efficace et a permis de simplifier drastiquement des codes hautement obfusqués comme le malware X-Tunnel. L'objectif de ce projet sera donc d'appliquer l'analyse de BBSSE à de nouveaux cas d'usage plus complexes pour comprendre ses limites actuelles et proposer des extensions.

Le projet se déroulera comme suit:

- Étudier les méthodes de déobfuscation à l'état de l'art et notamment le *backward-bounded symbolic execution (BBSSE)*;
- Évaluer le BBSSE sur un jeu de donné de codes réels ou synthétiques pour étudier ses forces et ses limitations dans un contexte donné;
- 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/