Offensive security: Rop chain synthesis

Grégoire MENGUY
CEA LIST
gregoire.menguy@cea.fr

L'adoption de nouvelles protections au niveau binaire rend l'exploitation de bug de plus en plus difficile. Notamment, en réponse à la protection W ^ X interdisant d'exécuter du code accessible en écriture, les attaques via ROP chains ont été proposés. Celles-ci permettent d'outrepasser la protection W ^ X en utilisant le code déjà présent dans le binaire pour implémenter la charge malveillante. Cependant, trouver de telles ROP chains manuellement est difficile. De nombreux outils ont ainsi été proposés pour les générer automatiquement. Néanmoins, les approches actuelles restent insatisfaisantes et savoir comment générer des ROP chains efficacement reste un problème largement ouvert.

Ce projet propose d'étudier l'efficacité de la synthèse stochastique pour la génération de ROP chain. L'objectif sera d'étendre le framework de synthèse de ROP chain "XyROP" pour l'évaluer sur un jeu de données représentatif et le comparer aux approches de l'état de l'art (Roper, ExRop, AngRop, etc). Si le temps le permet, des extensions à d'autres types d'attaque (ex : JOP) pourront être étudiées

Le projet se déroulera comme suit:

- Comprendre le framework de synthèse de ROP chain "XyROP";
- L'évaluer sur un jeu de donné de codes réels ou synthétiques pour étudier ses forces et ses limitations actuelles, par rapport à l'état de l'art;
- 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/