УДК 519.681.3

Неявные предикаты. Обфускация CFG с помощью конечных автоматов. Обфускация с использованием тулчейна LLVM.

Молокович Д.А. (ГБОУ СОШ 31)
Научный руководитель – Сокина Л.А.
(ГБОУ СОШ 31)

Введение. Определение обфускации программ, как математической задачи. Исследование существующих методов ее решения. Написание расширения (pass) для компилятора clang для обфускации программ, написанных на C/C++. Изучение существующих работ по этой теме, определение направления для дальнейшего изучения. Обфускация находит широкое применение: начиная от компаний, которым нужно защитить алгоритм программы, и до разработчиков вирусов, которые применяют обфускацию с целью обхода автоматизированных средств защиты(AV/EDR) и ручного анализа аналитиками ПО.

Основная часть. В работе определяются критерии обфускации и рассматриваются ее методы без строгого доказательства. Строгое определение обфускации пока что неразрешимая проблема криптографии, поэтому в большинстве работ формулируется нестрогое определение [1] [2] того, что можно считать обфусцированной программой. На основе данного определения я рассматриваю следующие методы, применимые на практике:

- Opaque predicates [1] (неявные предикаты)
- Control Flow Flattening (Обфускация графа потока выполнения)

Выводы. В ходе исследования был проведен анализ множества зарубежных и отечественных работ по теме обфускации программ. Изучены наиболее перспективные методы для решения поставленной задачи и частично реализованы, как PoC(Proof of Concept).

Список использованных источников:

1. Zobering L., Galbraith S. D. , Russello G. When are Opaque Predicates Useful? // 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). — 2019. — авг. — с. 168—175.
2. Xu D. , Ming J. , Wu D. Generalized Dynamic Opaque Predicates: A NewControl Flow Obfuscation Method // SpringerLink. — Cham, Switzerland, 2016. — авг. — с. 323—342.