ИСП ОБФУСКАТОР

ИСП РАН

ИСП Обфускатор — комплекс технологий по противодействию массовой эксплуатации уязвимостей, возникающих в результате ошибок или закладок. Если злоумышленник смог атаковать одно из устройств с одинаковым ПО, остальные останутся под защитой благодаря изменениям, внесённым в код.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Обфускатор защищает систему от массовой эксплуатации уязвимостей с помощью различных методов диверсификации кода и позволяет собирать код полного дистрибутива ОС.

ОБФУСКАТОР — ЭТО:

- Тонкая настройка баланса между степенью запутывания и уровнем производительности (при применении с целью защиты от обратного анализа). Минимальное замедление работы — в 1,2 раза, максимальное — в 8 раз;
- Полная автоматизация (не требуется специальная подготовка исходного кода программы и дополнительные усилия со стороны билд-инженеров заказчика);
- Использование набора открытых компиляторов GCC, который позволяет корректно собирать код полного дистрибутива ОС;
- Использование оригинального метода обеспечения целостности потока управления (CFI), который успешно противодействует большинству атак с повторным использованием кода (ROP, JOP, ret-to-plt и др.). На базе компилятора GCC реализован прототип CFI, который показал среднее замедление на наборе тестов SPEC CPU2006 около 2%, что заметно ниже, чем у традиционных методов;
- Два метода диверсификации:
  - Динамическая диверсификация кода при запуске программы. Применяется, когда заказчику обязательно нужен один и тот же код на всех устройствах (например, из-за обязательной сертификации). Этот метод позволяет перемещать до 98% кода с небольшим увеличением его объёма и ухудшением производительности примерно на 1,5%. Преимущества Обфускатора по сравнению с аналогичными продуктами:
    - Перемешивание до функции (в отличие от технологий ASLR и Pagerando, которые перемещают только крупные блоки кода);
    - Перемешивание функций во всей системе, кроме ядра, а также отсутствие конфликта с антивирусами (преимущества перед аналогичной технологией Selfrando, разработанной для Tor Browser);
  - Статическая диверсификация кода. Каждый раз при компиляции в зависимости от заданного ключа получается новый исполняемый файл. Преимущества данного метода:
    - не увеличивается объём бинарного кода (в частности, важно для интернета вещей);
    - ухудшение производительности стремится к нулю;
    - благодаря работе внутри компилятора, а не постфактум в компоновщике, можно применять расширенный набор диверсифицирующих преобразований и более гибко его настраивать.
    - Метод обеспечения целостности потока управления (CFI).
- Бесконфликтное совмещение с другими средствами защиты ПО (в том числе с системным механизмом ASLR).

ДЛЯ КОГО ПРЕДНАЗНАЧЕН ОБФУСКАТОР?

- Разработчики специализированных дистрибутивов операционных систем;
- Разработчики прикладного ПО.

ОПЫТ ВНЕДРЕНИЯ

ИСП Обфускатор внедрен в ОС «Циркон», которую используют МИД и Пограничная служба ФСБ России.

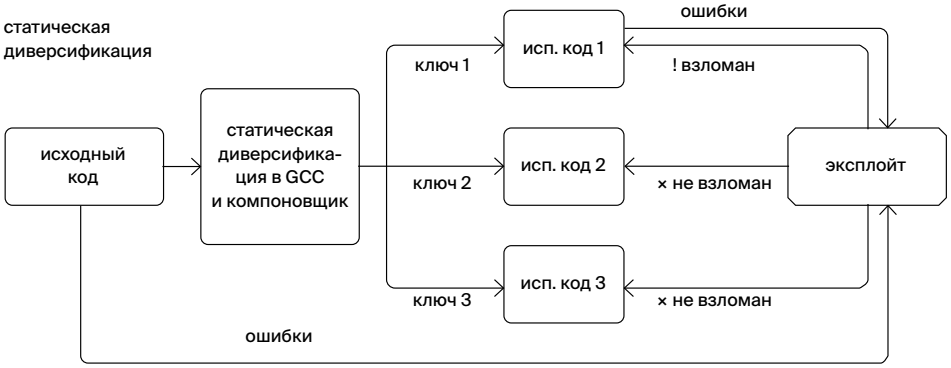
СИСТЕМНЫЕ ТРЕБОВАНИЯ

Обфускатор — универсальный продукт, который можно адаптировать под любые системные требования. В настоящее время основная версия работает в ОС на базе ядра Linux (начиная с версии 2.6) с поддержкой архитектуры Intel x86/x86-64.

СХЕМА РАБОТЫ

обычная сборка

статическая диверсификация



динамическая диверсификация