

Васильцов И.И.

*Научный руководитель: к.т.н., доцент А.А. Быков
 Муромский институт (филиал) федерального государственного образовательного
 учреждения высшего образования «Владимирский государственный университет
 имени Александра Григорьевича и Николая Григорьевича Столетовых»
 602264, г. Муром, Владимирская обл., ул. Орловская, 23
 E-mail: ilya.vasiltsov@mail.ru*

Использование технологии виртуализации для защиты кода программной платформы .NET Framework

.NET Framework — программная платформа, выпущенная компанией Microsoft в 2002 году. Основой платформы является общезыковая среда исполнения Common Language Runtime (CLR), которая подходит для разных языков программирования. Функциональные возможности CLR доступны в любых языках программирования, использующих эту среду.[1]

Использование программной платформы позволяет разработчику облегчить создание и поддержку технически сложных или нагруженных проектов. Библиотека Framework Class Library (FCL), содержащая несколько тысяч объектных классов .NET, предоставляет основные программные модули, на основе которых разработчиками реализуются специфические для проекта компоненты.

Основной идеей при разработке .NET Framework являлось обеспечение свободы разработчика за счёт предоставления ему возможности создавать приложения различных типов, способные выполняться на различных типах устройств и в различных средах.

После выполнения компиляции код .net приложений(сборок) содержит набор метаданных, описывающих сборку, ее типы и члены, а также IL-код (сокр. От CIL - Common Intermediate Language), который реализует все члены типов. Для выполнения программы на машине конечного пользователя должна быть установлена среда CLR (Common Language Runtime (CLR)). Встроенный в CLR JIT-компилятор «на лету» (just in time) преобразует промежуточный байт-код в машинные коды нужного процессора[1]. (Рис.1)

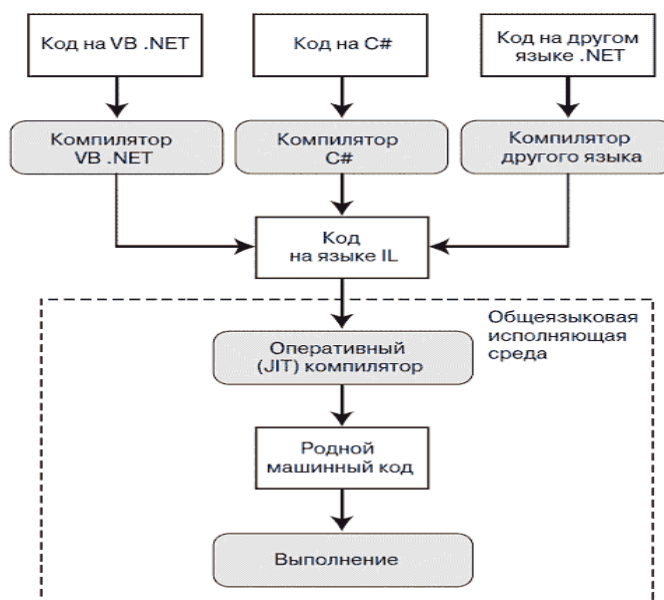


Рис.1. Компиляция и выполнение программ на платформе .Net framework

Скомпилированный код для .NET Framework помещается в логические единицы, называемые сборками (assembly). Компоненты сборки могут находиться в одном или нескольких файлах.

Каждая сборка содержит:

- Манифест
- Метаданные типов
- IL – код
- Ресурсы

Программы, разрабатываемые с помощью .NET Framework, создаются для среды CLR.

Над сборками можно провести операцию декомпиляции – получения исходного кода.

Причины возможности декомпиляции:

- Большое количество информации о сборке в метаданных
- IL – код является абстракцией более высокого уровня, чем машинный код
- Компиляторы языков .net framework выполняют меньше оптимизации кода, чем машинный код компиляторов, преобразующих программу в машинный код.

К настоящему времени разработано множество различных декомпиляторов, позволяющих просматривать исходный код любых .net сборок в виде эквивалентного языка c# или в виде набора IL инструкций. Возникает фундаментальная проблема, а именно: написанная человеком программа может быть человеком же и понята, проанализирована, разобрана. Распространяя свое программное обеспечение, разработчики неизбежно раскрывают свои наработки и алгоритмы, которыми может воспользоваться любой желающий.

Для решения возникшей проблемы необходим алгоритм, который может до неузнаваемости изменить код программы, при этом сохраняя ее функциональность.

В ходе выполнения исследовательской работы было разработано приложение, позволяющее предотвратить возможность декомпиляции.

Виртуализация — предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации, и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе. [2]

Одно из применений виртуализации заключается в симуляции процессора. Это, так называемая, P-code(или pseudo-code) машина. P-code–это машинный язык, который выполняется на виртуальной машине, а не на реальном оборудовании.

Разработанное программное обеспечение использует технику виртуализации кода, позволяя таким образом значительно усложнить анализ защищённых программ. Приложение выполняет трансляцию кода исходной функции, представляющей собой код на языке IL в сформированный случайным образом байт-код виртуальной машины приложения. Исходный код функции удаляется и заменяется вызовом виртуальной машины.

Литература

1. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C#. 4-е изд. — СПб.: Питер, 2013. — 896 с.
2. URL: <https://ru.wikipedia.org/wiki/Виртуализация> [Электронный ресурс] Дата посещения 23.04.18
3. URL: https://ru.wikipedia.org/wiki/.NET_Framework[Электронный ресурс] Дата посещения 23.04.17