Экз. № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

Козачка Александра Васильевича

на диссертационную работу Федотова Андрея Николаевича

«Разработка метода оценки эксплуатируемости программных дефектов»,

представленную к защите на соискание ученой степени кандидата технических наук по специальности 05.13.11 - «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Актуальность темы исследования

В современном мире обнаружение ошибок и уязвимостей является неотъемлемой частью при обеспечении безопасности программ. Получившие широкое распространение средства динамического анализа (фаззинга), позволяют находить большое количество аварийных завершений. Разработчикам крайне тяжело при таком количестве в сжатые сроки исправить найденные фаззингом дефекты. Целесообразно в первую очередь исправлять наиболее опасные дефекты, которые позволяют нарушителю выполнить произвольный код. Оценка дефектов на возможность их эксплуатации злоумышленником должна быть точной и иметь приемлемую скорость работы, что позволит ее применять при промышленной разработке программного обеспечения. Кроме того, при оценке необходимо учитывать распространенные защитные механизмы, препятствующие эксплуатации дефектов. В противном случае, существует возможность получить неработоспособный эксплойт в современных операционных системах.

В диссертационной работе Федотова А. Н. представлен метод оценки эксплуатируемости программных дефектов, отвечающий перечисленным требованиям, что подтверждает ее актуальность.

Диссертационная работа содержит 98 страниц и состоит из введения, четырех глав, заключения, списка литературы и одного приложения. Список литературы содержит 67 наименований.

Во введении обосновывается актуальность, определяется цель работы, формируются основные научные результаты.

В первой главе приводится обзор методов и подходов, относящихся к теме диссертационной работы. Рассмотренные существующие походы на основе анализа аварийных завершений и автоматической генерации эксплойтов имеют ряд недостатков. Анализ аварийных завершений не позволяет получить точную оценку эксплуатируемости для найденных дефектов. Известные подходы к автоматической генерации эксплойтов требовательны к вычислительным ресурсам, а также не учитывают работу современных защитных механизмов. В главе также проанализированы механизмы, препятствующие эксплуатации программных дефектов. Исходя из проведенного анализа наиболее распространенными механизмами защиты в современных операционных системах являются: рандомизация адресного пространства (ASLR) и защита от исполнения данных (DEP).

Вторая глава посвящена предложенному методу оценки эксплуатируемости программных дефектов. Описанный метод состоит из метода предварительной фильтрации аварийных завершений и метода автоматической генерации эксплойтов. Легковесная фильтрация аварийных завершений позволяет отбирать такие аварийные завершения, эксплуатация которых наиболее вероятна. Для этих аварийных завершений будет произведена попытка сгенерировать эксплойт методом автоматической генерации эксплойтов. Метод автоматической генерации эксплойтов позволяет получить работоспособный эксплойт, в рамках работы таких защитных механизмов, как: DEP и ASLR. Таким образом, применяя предложенный метод можно оценивать эксплуатируемость программных дефектов с учетом заявленных требований.

В третьей главе представлено описание программного инструмента, реализующего метод оценки эксплуатируемости программных дефектов. Инструмент состоит из нескольких программных компонентов: система предварительной фильтрации аварийных завершений, система автоматической генерации эксплойтов и эмулятор QEMU. В эмуляторе работает система предварительной фильтрации аварийных завершений. Также он используется для получения трассы выполнения программы, которая необходима для генерации эксплойта. Проверка работоспособности полученного эксплойта происходит в эмуляторе.

В пятой главе продемонстрированы результаты практического применения разработанных методов и программного инструмента. Проводилась оценка эксплуатируемости дефектов, найденных в результате фаззинга, а также известных дефектов из открытых источников. По результатам тестирования делается вывод, о выполнении выдвинутых требований.

В заключении приводятся основные результаты работы, которые выносятся на защиту:

1. Разработан метод автоматической генерации эксплойтов по информации об аварийном завершении программы на основе символьной интерпретации трассы машинных команд с применением промежуточного представления Pivot. Метод учитывает работу механизмов защиты от эксплуатации уязвимостей DEP и ASLR, а также применим к программам, работающим под управлением операционных систем семейств Linux и Windows.
2. Разработан метод оценки эксплуатируемости программных дефектов, использующий автоматическую генерацию эксплойтов и предварительную фильтрацию аварийных завершений.
3. На основе предложенных автором методов разработана и реализована система оценки эксплуатируемости программных дефектов.

Научной новизной обладают следующие выносимые на защиту результаты, полученные лично автором в ходе диссертационного исследования:

1. Разработанный метод автоматической генерации эксплойтов позволяет проводить формирование эксплойтов с учетом механизма защиты от выполнения данных и рандомизации адресного пространства процесса.

2. Разработанный метод предварительной фильтрации базируется на предложенной в работе классификации аварийных завершений и позволяет вырабатывать начальную оценку эксплуатируемости, учитывая влияние встроенных компилятором механизмов защиты от переполнения буферов.

К сожалению, в работе присутствует ряд **недостатков**:

1. Необоснованное использование жаргонизмов в тексте работы. Пример – "канарейка", а не "защитная последовательность байт".

2. Без должных пояснений термин "помеченный" применяется к символьным данным. Пример в тексте диссертации на с. 57: "В случае, когда помечено значение указателя стека, его необходимо исправить на корректное значение".

3. Ошибка в записи алгоритма 2 (с. 59 диссертации). Строка "$Sp = Sp \wedge (stackPointer == svalue)$; " должна быть перенесена в конец алгоритма.

4. На схеме рис. 2.5 (с. 39 диссертации) или (рис. 3 с. 12 автореферата) не отражено преобразование в Pivot, а из него в символьные формулы.

Отмеченные недостатки не влияют на общую положительную оценку работы.

Диссертационная работа Федотова А. Н. является законченным научным исследованием. Практическая ценность работы подтверждается результатами применения разработанных методов и инструментов. Полученные автором результаты прошли апробацию на нескольких конференциях и отражены в опубликованных им работах.

Автореферат полно и корректно отражает содержание диссертационной работы.

Выводы

Диссертационная работа Федотова Андрея Николаевича соответствует всем требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор, Федотов Андрей Николаевич, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.11 - «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Официальный оппонент:
кандидат технических наук,
сотрудник Федерального государственного казенного военного образовательного учреждения высшего образования
«Академия Федеральной службы охраны Российской Федерации»

Козачок А. В.

"1" декабря 2017 г.

Подпись кандидата технических наук Козачка Александра Васильевича заверяю.

Руководитель кадрового

Дёшин А. И.

"07" декабря 2017 г.