УТВЕРЖДАЮ

Заместитель директора по научной работе

ФГУ ФНЦ НИИСИ РАН,

директор МСЦ РАН - филиала

ФГУ ФНЦ НИИСИ РАН

к.т.н., доцент

Шабанов Борис Михайлович

5 декабря 2017 года

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

Межведомственный суперкомпьютерный центр Российской академии наук - филиал Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» (МСЦ РАН - филиал ФГУ ФНЦ НИИСИ РАН)

на диссертацию

Федотова Андрея Николаевича

«Разработка метода оценки эксплуатируемости программных дефектов»,

представленную к защите на соискание учёной степени кандидата технических наук по специальности 05.13.11 — математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Актуальность

Поиск ошибок и уязвимостей является важной задачей для обеспечения безопасности программ. Уязвимости, приводящие к выполнению произвольного кода, являются наиболее опасными. На сегодняшний день существуют методы и программные инструменты, позволяющие получить набор входных данных программы, который позволяет выполнить заданный код нарушителя (эксплойт). Большинство из них недоступно или не пригодно для промышленного применения. Кроме того, они не учитывают защитные механизмы, препятствующие эксплуатации программных дефектов. В диссертационной работе Федотова А.Н. предлагается новый подход к обнаружению эксплуатируемых дефектов, способный учитывать работу современных механизмов защит от эксплуатации уязвимостей. Таким образом, тема диссертационной работы Федотова А.Н. является актуальной.

Общая характеристика диссертационной работы

Диссертация имеет общий объём 98 страниц и состоит из введения, четырех глав, заключения, списка литературы и одного приложения.

Во введении описывается актуальность проблемы, формулируются цель и задачи диссертационной работы, указана научная новизна результатов исследования, раскрыта их практическая значимость и приводятся основные положения, выносимые на защиту.

В первой главе приводится обзор работ по теме диссертации, а также рассматриваются современные защитные механизмы, препятствующие эксплуатации уязвимостей. Основное внимание было уделено существующим методам автоматической генерации эксплойтов и методам фильтрации аварийных завершений программ. Выделены недостатки и ограничения, присущие рассмотренным методам. Проанализированы современные механизмы защит от эксплуатации программных дефектов. На основе проведённого анализа сделан вывод о том, что существующие методы и инструменты не позволяют получать эксплойты, которые остаются работоспособными в условиях работы широко распространенных современных защитных механизмов таких, как: рандомизация адресного пространства (ASLR) и защита от исполнения данных (DEP).

Вторая глава посвящена описанию предложенного автором метода оценки эксплуатируемости программных дефектов, основанного на методе предварительной фильтрации аварийных завершений и методе автоматической генерации эксплойтов по информации об аварийном завершении программы. Метод автоматической генерации эксплойтов позволяет получать работоспособные эксплойты в условиях работы защитных механизмов DEP и ASLR. Фильтрация аварийных завершений обеспечивает отбор таких аварийных завершений, для которых вероятнее всего будет сгенерирован эксплойт, что в целом позволяет быстрее обнаружить эксплуатируемые дефекты.

В третьей главе рассматривается программная реализация предложенных методов. Программный инструмент оценки эксплуатируемости включает в себя систему фильтрации аварийных завершений и систему автоматической генерации эксплойтов. Работоспособность полученных эксплойтов проверяется автоматически посредством запуска исследуемой программы в эмуляторе на сгенерированных входных данных.

В четвёртой главе приводятся результаты применения разработанных методов и инструментов. Разработанный инструмент применялся для оценки эксплуатируемости дефектов, найденных в результате фаззинга. Также проводилась оценка эксплуатируемости дефектов из открытых источников и набора тестовых программ из DARPA Cyber Grand Challenge 2016 года. На основе этих данных сделан вывод о применимости предложенного метода к использованию в промышленных проектах.

В заключении содержатся выводы и сформулированы основные результаты диссертации.

Список литературы содержит 67 наименований.

В работе получены следующие **результаты**:

1. 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 ОС Linux и семейства ОС Windows.
2. Метод оценки эксплуатируемости программных дефектов, использующий автоматическую генерацию эксплойтов и предварительную фильтрацию аварийных завершений.
3. Программный инструмент, реализующий метод оценки эксплуатируемости программных дефектов.

Достоверность полученных результатов подтверждается их апробацией на семинарах, конференциях различного уровня, научными статьями, четыре из которых опубликованы в изданиях, входящих в перечень ВАК РФ. Практическая значимость полученных результатов подтверждается результатами применения разработанных методов и программных инструментов.

К сожалению, в работе имеются отдельные недостатки.

1. В работе отмечается возможность оценки эксплуатируемости дефектов для программ, работающих на различных процессорных архитектурах, но результаты применения методов приведены только для программ, выполняющихся на процессорах с архитектурой x86/64.
2. В разделе 2.4 описан подход к построению предиката пути. К сожалению, вопрос корректности предиката пути в работе не рассматривается.

Отмеченные недостатки не снижают положительной оценки диссертационной работы. Диссертация является законченным научным исследованием, написанным на высоком научном уровне. Результаты диссертации представлены в пяти статьях автора, докладывались на российских и международных научных конференциях. Автореферат диссертации правильно и полно отражает содержание работы и надлежащим образом оформлен.

Результаты диссертации позволят повысить безопасность разрабатываемого программного обеспечения.

Заключение

Диссертационная работа Федотова А.Н. полностью соответствует требованиям ВАК РФ, предъявляемым к диссертациям на соискание учёной степени кандидата технических наук, а Федотов Андрей Николаевич заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.11 — математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Отзыв на диссертацию обсужден на научном семинаре Межведомственного суперкомпьютерного центра Российской академии наук - филиала Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» 4 декабря 2017 года, протокол № 13.

заместитель директора МСЦ РАН - филиала ФГУ ФНЦ НИИСИ РАН
к.т.н., доцент — Антон Викторович Баранов

ведущий научный сотрудник МСЦ РАН - филиала ФГУ ФНЦ НИИСИ РАН
к.ф.-м.н. — Алексей Анатольевич Рыбаков