ОТЗЫВ
ОФИЦИАЛЬНОГО ОППОНЕНТА
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»

Диссертационная работа А.Н. Федотова посвящена проблеме автоматического выявления дефектов в программном обеспечении, приводящих к уязвимости по отношению к использованию обнаруженного дефекта для внешнего воздействия. При этом не все программные дефекты могут быть использованы для такого воздействия – в диссертации используется такая терминология, как *эксплуатируемость дефекта.* Эта проблема возникла довольно давно в связи с бурным развитием программирования как технологии, используемой для разработки массового ПО, в том числе, промышленного. Ключевой аспект здесь - резкое увеличение количества ошибок при массовом программировании, или неполной проверки всех возможных в реальной эксплуатации разрабатываемого ПО «закоулков» его исполнения или других слабых мест, которые открывают окна для внешнего вредоносного внедрения. Для решения этой проблемы разработаны различные методы выявления слабых мест в эксплуатируемом ПО. Однако полного решения проблемы не получено, да и, с очевидностью, не может быть достигнуто. Это связано с тем, что программирование, как технология, осваивает принципиально новые направления в связи с новыми научными достижениями в области компьютерных наук. Соответственно, стал развиваться подход с возможно максимальным абстрагированием от конкретностей, например, от конкретностей операционной системы, архитектуры используемого компьютера (процессора, …), используемых при создании ПО программных средств и т.д. Разработанные в этом направлении методы, в частности автоматическая генерация тестовых наборов входных данных (эксплойтов) и символьная интерпретация процесса преобразования входных данных в исследуемом ПО в виде вычислений над символьными переменными и константами, позволяет проводить анализ уязвимостей в достаточно общем виде. А.Н. Федотов в своей диссертационной работе использовал такой подход с анализом потока аварийных завершений исследуемого ПО в качестве стартового этапа. При этом в центре внимания был поиск набора входных данных, при котором уязвимость приводит к характерным особенностям исполнения исследуемого ПО, которые можно

интерпретировать как вредоносное внедрение - выполнение постороннего кода или вызов внешней функции (библиотечной) с контролируемыми извне параметрами.

Научно-технологическая новизна результатов, полученных А.Н. Федотовым в диссертационной работе связана, прежде всего, с тем, что имеющиеся в настоящее время инструментальные средства выявления программных дефектов не учитывают работу защитных механизмов от внешних внедрений, которые все в большей степени имплементируются в среды выполнения программ, например, в операционные системы. Наряду с новизной мы видим в этом и подтверждение актуальности диссертационной работы. Несомненно, дальнейшие разработки по данной тематике все в большей степени должны будут отслеживать новейшие достижения во взаимном противоборстве хакерского «искусства» и противодействующих им защитных технологий.

Актуальность разработок, выполненных в диссертационной работе А.Н. Федотовым, также связано с тем, что для достижения требуемой в настоящее время эффективности метода автоматического выявления программных дефектов необходимо привести его программно-техническую реализацию в соответствие с современным уровнем развития компьютерных технологий. С этой целью в диссертации проведен state-of-the-art анализ в этой области и был выполнен ряд важных разработок. Среди них отметим разработку архитектурно независимого метода генерации эксплойтов (наборов входных данных), метода предварительной фильтрации аварийных завершений с классификацией по возможности эксплуатируемости соответствующих программных дефектов, а также метода оценки эксплуатируемости выявленных программных дефектов.

Отметим, что результаты, полученные в диссертационной работе А.Н. Федотова, являются научно обоснованными, как в части четкости постановки решаемых задач, так и в отношении используемых математических и ИТ методов. Положения, которые вынесены диссертантом на защиту, представляют значимый интерес для дальнейших прикладных разработок в области автоматического выявления программных дефектов, предоставляющих возможности для внешнего вредоносного внедрения.

Диссертация состоит из 98 страниц, она включает Введение, четыре главы, Заключение, список литературы (67 источников), список рисунков (17 рисунков), списка таблиц (5 таблиц) и Приложения.

Во введении формулируется цель диссертационной работы, обосновывается ее актуальность, приводятся основные научные результаты, полученные в ходе диссертационной работы.

В Первой главе приводится обзор работ по теме диссертации. Рассматриваются подходы на основе анализа аварийных завершений программы и методы автоматической генерации эксплойтов. Отмечается, что автоматическая генерация эксплойтов весьма требовательна к вычислительным ресурсам. Указывается, что в существующих подходах не учитываются в правильной степени защитные механизмы. Приводится обзор защитных механизмов, присутствующих в современных операционных системах.

Вторая глава посвящена методу оценки эксплуатируемости программных дефектов, развиваемому в диссертации. Метод основан на применении метода фильтрации аварийных завершений и метода автоматической генерации эксплойтов. Фильтрация аварийных завершений позволяет определять наиболее пригодные для дальнейшей внешней эксплуатации аварийные завершения, а также отфильтровывать аварийные завершения, эксплуатация которых менее вероятна. Показано, что разработанный метод автоматической генерации эксплойтов позволяет получить работоспособный эксплойт в условиях работы защитных механизмов, таких как: рандомизация адресного пространства (ASLR) и защита от исполнения данных (DEP). Последовательное применение этих методов при оценке эксплуатируемости программных дефектов позволяет добиться приемлемой эффективности их выделения. Подчеркнем, что это делает возможным прикладное применение разработанного метода оценки эксплуатируемости программных дефектов в процессе разработки массового и промышленного программного обеспечения.

В третьей главе представлено описание программной реализизации метода оценки эксплуатируемости программных дефектов. Соответствующее решение состоит из системы фильтрации аварийных завершений, системы автоматической генерации эксплойтов и эмулятора Qemu. Подтверждение работоспособности получаемых эксплойтов получается при запуске исследуемой программы в эмуляторе.

В четвёртой главе продемонстрированы результаты практического применения разработанных методов и программных инструментов. Тестирование метода оценки эксплуатируемости проводилось для аварийных завершений, полученных в результате автоматической генерации тестовых наборов входных данных, а также на примерах, найденных в открытых источниках. Отметим, что одним из таких источников был тестовый набор

DARPA Cyber Grand Challenge. Приведены оценки эксплуатируемости модельных примеров, листинги которых приведены в Приложении.

В Заключении даются выводы и обозначаются направления дальнейшего развития разработанных методов и их программных реализаций.

Приведем краткие формулировки результатов диссертационной работы А.Н. Федотова, вынесенных на защиту:

- разработан новый метод автоматической генерации эксплойтов по результатам анализа потока аварийных завершений на основе символьной интерпретации трассы машинных команд с учетом работы механизмов защиты DEP и ASLR для ПО, работающего под управлением ОС Linux и Windows;
- разработан метод оценки эксплуатируемости программных дефектов, использующий предварительную фильтрацию аварийных завершений.

Результаты, выносимые диссертантом на защиту, опубликованы в четырех публикациях в рецензируемых журналах, рекомендованных ВАК, один из которых индексируется Scopus, а также в одной публикации в трудах научной конференции.

Достоверность научных положений и выводов диссертационной работы А.Н. Федотова обоснована корректностью постановки задач, использованием современных математических и ИТ методов, и валидацией разработанного метода на значимых в прикладном отношении тестовых примерах и моделях.

Диссертация А.Н. Федотова выполнена на высоком научно-техническом уровне. При этом необходимо сделать следующее замечание. Диссертационная работа имеет явную прикладную направленность – несомненна научно-техническая значимость полученных результатов для усиления защищенности продукции массового производства ПО. Однако в диссертации недостаточно четко показан прикладной вес предлагаемых разработок. Например, насколько весомую долю в общем потоке хакерских атак занимают именно вредоносные внедрения на основе программных дефектов. А также, насколько значимо в прикладном отношении выделение эксплуатируемых программных дефектов.

Это замечание, однако, не снижает научно-технологической значимости, проведенного А.Н. Федотовым диссертационного исследования и разработок, и не изменяют общую положительную оценку.

В заключение отметим, что представленная диссертация А.Н. Федотова представляет собой завершенное исследование, проведенное на высоком научно-техническом уровне. Основное содержание диссертации отражено в опубликованных диссертантом статьях, доложено на научных конференциях.

Полученные результаты работы соответствуют поставленным задачам. Автореферат отражает основные положения диссертации.

Приходим к заключению, что диссертационная работа Федотова Андрея Николаевича по теме «Разработка метода оценки эксплуатируемости программных дефектов» соответствует всем требованиям ВАК РФ, предъявляемых к диссертациям на соискание учёной степени кандидата технических наук, а её 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:

Доктор физико-математических наук,
начальник Отдела информационных технологий
и математического моделирования
Курчатовского комплекса НБИКС-технологий
НИЦ «Курчатовский институт»
123182 Россия, Москва,
пл. Академика Курчатова, д. 1
тел. +7 915 016-00-48
e-mail: ilyin0048@gmail.com

В.А. Ильин
04.12.2017

Подпись сотрудника НИЦ «Курчатовский институт» В.А. Ильина заверяю

Директор департамента
по общим кадровым и социальным вопросам
НИЦ «Курчатовский институт» С.В. Андрущук