ОТЗЫВ
официального оппонента Ильина Вячеслава Анатольевича
на диссертационную работу Нурмухаметова Алексея Раисовича
«Применение диверсифицирующих преобразований
для защиты от эксплуатации уязвимостей»,
представленную на соискание ученой степени
кандидата технических наук по специальности
05.13.11 – «Математическое и программное обеспечение
вычислительных машин, комплексов и компьютерных сетей»

Диссертационная работа Нурмухаметова Алексея Раисовича направлена на решение проблемы предотвращения внешнего (зловредного) воздействия на ПО с помощью уязвимостей, доступ к которым появляется в процессе исполнения этого ПО в конкретных компьютерных средах – в диссертации такое воздействие обозначено, как *эксплуатация уязвимостей, порождённых ошибками, которые не были устранены на этапе разработки и тестирования*. Это проблема стоит в одном ряду с актуальными вызовами современного системного программирования. Несмотря на определенные успехи в этом направлении проблема (внешнего) несанкционированного вмешательства в результате эксплуатации уязвимостей не получила полного решения. Акцент в диссертационной работе поставлен на уязвимостях ПО, написанных на языках, которые характеризуются небезопасной работой с памятью (например, C и C++). Несомненно, тематика диссертационной работы А.Р. Нурмухаметова является **актуальной** с ясными прикладными перспективами.

Как отмечено в диссертации, эксплуатационные уязвимости опасны, прежде всего, потому, что количество компьютеров, на которых одновременно работает идентичное ПО, во многих случаях огромно – что является благодатной почвой для проведения массовых (внешних) атак. В этой связи, в литературе, активно обсуждается такой метод предупреждения атак на основе эксплуатации уязвимостей как *диверсифицирующие преобразования* — преобразования внутренней структуры ПО и/или реализации данного ПО в конкретной вычислительной среде, с целью получить большое количество его копий с различной структурой и/или реализацией в вычислительной среде, но с идентичной (прикладной) функциональностью. Собственно, этот **подход** и принят в диссертационной работе в качестве базового.

Соответственно **цель диссертационного исследования** - развитие систем автоматической защиты от эксплуатации уязвимостей программного обеспечения на всех стадиях его разработки, сборки, распространения и работы. И для достижения этой цели поставлены и решены следующие **задачи**:

- разработка метода запутывания программного кода на уровне промежуточного представления компилятора для генерации диверсифицированной популяции исполняемых файлов;

- разработка метода диверсификации внутренней структуры исполняемого файла при загрузке его в память;
- проведение оценки производительности и эффективности разработанных методов.

Подчеркнем ключевые факторы **новизны** результатов, полученных в диссертации А.Р. Нурмухаметова:
- запутывание программного кода на уровне промежуточного его представления в компиляторе,
- мелкозернистая рандомизация ПО на уровне функций с целью уникального изменения адресного пространства на каждом запуске ПО, п
- оценка эффективности разработанных методов диверсификации по успешности противодействия повторным атакам программного кода, размещенного в памяти.

В части **практической значимости** полученных результатов мы согласны с формулировками, приведенными в диссертации:
- предложенные алгоритмы реализованы в промышленных операционных системах CentOS 7 и Debian 10;
- на эти разработки получены сертификаты о Государственной регистрации программ для ЭВМ.

Полученные в ходе диссертационной работы результаты были опубликованы в 7-ит статьях, две из которых в изданиях, индексируемых в Scopus и Web of Science.

Диссертация содержит 140 страниц текста, который состоит из Введения, шести Глав, Заключения, списка литературы (72 источников), списков Рисунков (25 штук) и Таблиц (6 штук), а также пяти Приложений (А-Д).

Во **Введении** обосновывается актуальность диссертационной работы, формулируются цели и задачи исследования, обосновываются новизна и практическая значимость полученных результатов, формулируются положения, выносимые на защиту.

Первая Глава посвящена обзору предметной области диссертационной работы, включая обзор литературы и программных средств, связанных с тематикой диссертационной работы. Отмечаются недостатки существующих в современных ОС методов защиты. Формулируются основные идеи предлагаемых диверсифицирующих преобразований. Анализируются основные требования к разрабатываемым методам и возможным применениям их в операционных системах, а также совместимость с существующими механизмами защиты.

Во **второй Главе** описывается разработанный в диссертации метод генерации диверсифицированной популяции исполняемых файлов на уровне промежуточного представления компилятора. Для генерации диверсифицированной популяции используются: перестановка функций местами внутри модуля или всей программы, перестановка местами базовых блоков

внутри функции, добавление локальных переменных и перемешивание их на стеке. Приводятся результаты измерений падения производительности.

Третья Глава посвящена описанию разработанного в диссертационной работе метода мелкозернистой рандомизации внутренней структуры программы при запуске. Обсуждается концепция метода, описывается структура и набор дополнительной информации о границах функций и ссылках. Описываются проблемы совместимости с имеющимися средствами защиты ОС Linux. Приводятся результаты измерения производительности, потребления оперативной памяти и места на жёстком диске.

В **четвёртой Главе** приведены результаты оценки эффективности реализованных методов диверсифицирующих преобразований:

- по количеству выживших гаджетов, работоспособности эксплойтов на примере синтетических уязвимостей, внедрённых в реальные программы,
- по работоспособности эксплойтов на реальных примерах уязвимостей.

Приводится статистика по эффективности противодействия атакам повторного использования кода в виде ROP-цепочек.

Пятая Глава обсуждается решение задачи о случайных перестановках функций местами: выводится формула вероятности функции остаться на своём месте, показано, что вероятность крайних функций остаться на своём месте значительно превосходит вероятность функций, расположенных внутри файла.

В **шестой Главе** приводится описание программной реализации дополнительной системы защиты ОС семейства Linux на основе методов, предложенных в Главах 2 и 3. Представлена архитектура реализованной системы. Обсуждаются изменения, внесённые в компилятор GCC, компоновщик ld и загрузчик ld.so.

В **Заключении** приводятся формулировки основных результатов, полученных в ходе диссертационной работы. Также обсуждаются возможные направления дальнейших исследований.

Замечания по представленной диссертационной работе:

1. В разделе 2.2 обсуждается практическая возможность распространения каждому пользователю уникальной копии исполняемого образа прикладного ПО. Однако, оценок реальных затрат в связи с использование дополнительных ресурсов не приведено.
2. В разделе 2.7 приводится результат влияния на производительность диверсифицирующих преобразований над промежуточным представлением компилятора и указывается на ускорение некоторых тестов. Однако, такое улучшение производительности не объяснено.
3. В диссертации не обсуждалось, как можно применять разработанные методы диверсифицирующих преобразований к профилактике возможных атак эксплуатируемых уязвимостей, которые могут иметь место при изменениях в системном ПО в связи с внедрением тех самых разработанных методов диверсифицирующих преобразований.

Эти замечания, однако, не снижают высокую оценку полученных в диссертационной работе результатов.

Заключение

Диссертация А.Р. Нурмухаметова представляет собой завершённое исследование, проведённое на высоком научно-техническом уровне. Основное содержание диссертации отражено в опубликованных диссертантом статьях, доложено на научных конференциях. Полученные результаты работы соответствуют поставленным задачам. Автореферат правильно отражает основные положения диссертации.

Диссертационная работа Нурмухаметова А.Р. соответствует требованиям ВАК РФ, предъявляемых к диссертациям на соискание учёной степени кандидата технических наук, а её автор, Нурмухаметов Алексей Раисович заслуживает присуждения ему учёной 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,
Доктор физико-математических наук,
Главный научный сотрудник
КК НБИКС-природоподобных технологий
НИЦ «Курчатовский институт»

Ильин Вячеслав Анатольевич
27 апреля 2021