УТ
Д
ФГУ ФН
доктор т

С.Е. Власов
«21» 04 2021 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ
Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук»
(ФГУ ФНЦ НИИСИ РАН)

на диссертационную работу
Нурмухаметова Алексея Раисовича

«Применение диверсифицирующих преобразований для защиты от эксплуатации уязвимостей»,

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.

Диссертационная работа Нурмухаметова А.Р. посвящена исследованию и разработке диверсифицирующих преобразований и их применения для защиты от эксплуатации уязвимостей. Разработанные методы, для того чтобы быть практически применимыми, должны иметь приемлемые показатели производительности, препятствовать эксплуатации методами повторного использования кода, обладать совместимостью с текущими средствами защиты для достижения взаимно-усиливающего эффекта, быть применимыми в рамках целой операционной системы (ОС).

Актуальность

Информатизация многих сфер человеческой деятельности, включая критическую инфраструктуру, делает актуальной вопросы её безопасного и бесперебойного функционирования. Ошибки в программном обеспечении могут нести ощутимый экономический ущерб, который может достигать неприемлемых размеров в случае злонамеренной эксплуатации этих ошибок.

Особенно опасны уязвимости, которые приводят к выполнению произвольного кода на уязвимой системе. Развитие технологий программирования, а также средств статического и динамического анализа не приводит к полному устранению возможности эксплуатации уязвимостей. По этой причине возникает и является актуальной задача воспрепятствования эксплуатации уязвимостей. В связи с этим, тема диссертационной работы Нурмухаметова А.Р. является актуальной.

Общая характеристика диссертационной работы

Диссертация имеет общий объём 140 страниц и состоит из введения, шести глав, заключения, списков литературы, рисунков, таблиц и пяти приложений. Список литературы включает 72 наименования.

Во введении обосновывается актуальность диссертационной работы, формулируется её цель и задачи, излагается научная новизна, теоретическая и практическая значимость полученных результатов, формулируются основные положения, выносимые на защиту.

В первой главе рассматриваются основные понятия: уязвимость, эксплуатация, диверсификация кода, эксплойт, код нагрузки. Глава содержит обзор известных методов эксплуатации уязвимостей, а также имеющихся методов защиты от них. Рассматриваются недостатки имеющихся методов защиты и рассматриваются возможные подходы к их устранению на материале научных статей и доступных инструментов защиты. Делается вывод о перспективности применения методов диверсификации программного кода для защиты от эксплуатации.

Во второй главе описывается метод изменения промежуточного представления компилятора с помощью диверсифицирующих преобразований. Описывается подход к генерации диверсифицированной популяции исполняемых образов приложений, которая позволяет усложнить масштабную эксплуатацию. Приводятся описания диверсифицирующих преобразований.

В третьей главе приводится описание предлагаемого метода мелкозернистой рандомизации внутренней структуры программы при запуске. Описывается метод сохранения информации о границах функций и ссылках в специальной секции файла формата ELF на этапе компиляции и статической компоновки, а также способ использования этой информации для перестановки

функций местами и исправления ссылок на этапе загрузки и динамической компоновки. Приводятся результаты измерений производительности.

В четвёртой главе предлагается метод оценки эффективности реализованных методов защиты, состоящий из оценки количества выживших примитивов эксплойтов, а также из экспериментальной проверки работоспособности эксплойтов для синтетических и реальных примеров уязвимостей. На синтетических примерах показывается статистика по эффективности противодействия атакам повторного использования кода в виде ROP-цепочек. Кроме того, показывается как убывает процент успешно сработавших эксплойтов в зависимости от их сложности и для нетривиальных эксплойтов стремится к нулю.

В пятой главе приводится оценка вероятности функции остаться на своём месте при перестановке. Обнаруживается, что вероятность функции расположенной в начале или в конце файла существенно больше, чем для функции, расположенной где-то в середине. Данный вывод учитывается при реализации мелкозернистой рандомизации для улучшения её эффективности.

В шестой главе приводится описание программной реализации дополнительной системы защиты для ОС семейства Linux на основе методов, предложенных в главах два и три. Данная система встроена в одну из ОС семейства Linux и обладает приемлемыми характеристиками по ухудшению производительности программы, совместима с текущими средствами защиты, а также применима в рамках целой ОС. Реализованная система обеспечивает дополнительную защиту от атак повторного использования кода.

Основные результаты диссертационной работы

В диссертационной работе Нурмухаметова А.Р. получены следующие результаты:

1. Разработан метод изменения промежуточного представления компилятора при помощи диверсифицирующих преобразований с целью генерации большого количества различных бинарных образов программы.

2. Разработан метод мелкозернистой рандомизации программы при запуске.

3. Разработан метод оценки качества защиты от эксплуатации уязвимостей, который был применён к мелкозернистой рандомизации.

4. Предложенные методы диверсификации реализованы в рамках дополнительной системы защиты для ОС Linux.

Достоверность полученных результатов

Достоверность полученных результатов подтверждается экспериментальной и теоретической проверкой работоспособности предложенного подхода, а также апробацией на семинарах, конференциях различного уровня, и научными статьями, шесть из которых опубликованы в изданиях, входящих в перечень ВАК РФ, а две статьи в изданиях, индексируемых международной системой цитирования Scopus. Кроме этого, получено два свидетельства о государственной регистрации программы для ЭВМ.

Научная ценность и новизна

В рамках диссертационной работы получены следующие результаты, обладающие обладающие научной новизной и ценностью:

1. Метод диверсификации промежуточного представления программы в процессе её трансляции в машинный код, позволяющий создавать большое количество исполняемых файлов приложения.

2. Метод мелкозернистой рандомизации программы при запуске, который позволяет при каждом запуске программы уникально изменять адресное пространство процесса.

3. Метод оценки эффективности реализованных методов с точки зрения успешности противодействия атакам, которые повторно используют имеющийся в памяти процесса код.

Практическая значимость

Практическая значимость полученных результатов состоит в том, что предложенные соискателем методы могут применяться для защиты от эксплуатации уязвимостей. Разработанные методы и программные инструменты применяются в качестве дополнительной системы защиты ОС семейства Linux. Метод оценки эффективности механизмов защиты от эксплуатации может применяться для других методов и реализаций диверсифицирующих преобразований.

Замечания

В работе имеются следующие недостатки:

1. В разделе 1.8.1 отмечается, что обычная рандомизация малоэффективна для 32 битных приложений и платформ из-за небольшого пространства перебора, и что мелкозернистая рандомизация могла бы существенно его увеличить. Однако из содержания глав 3, 4, 6 нельзя сделать однозначный вывод о том, поддерживаются ли 32 битные приложения.

2. В главе 3 недостаточно полно описываются возможные проблемы совместимости с системами сборки проектов, например в случае использования нестандартных скриптов компоновки, или в случае изменения бинарного кода приложения после его окончательной компоновки, например, с целью оптимизации.

Заключение

Отзыв на диссертацию обсуждён на научном семинаре отдела математического обеспечения ФГУ ФНЦ НИИСИ РАН 20 апреля 2021 г. (протокол № 1 от 20.04.2021 г.)

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

Диссертационная работа Нурмухаметова А.Р. полностью соответствует требованиям ВАК, предъявляемым к диссертациям на соискание учёной степени кандидата технических наук по специальности 05.13.11 — «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей». Нурмухаметов Алексей Раисович заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.11 — «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Заведующий отделом
математического обеспечения
ФГУ ФНЦ НИИСИ РАН,
кандидат физ.- мат. наук А.И. Грюнталь