УТВЕРЖДАЮ

Проректор по научной работе
Новосибирского государственного
технического университета,
кандидат технических наук, доцент
_____ А.И. Отто
«__» ноября 2023 г.

ОТЗЫВ

ведущей организации «Новосибирский государственный технический университет» на диссертацию Лубкина Ивана Александровича «Метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Актуальность работы

Организация процесса разработки программного обеспечения, исключающего появление в нем дефектов, является технически сложной задачей. Вследствие этого программное обеспечение будет подвержено уязвимостям. Рассматриваемая работа направлена на устранение или существенное затруднение использования уязвимостей удаленного исполнения для бинарных приложений, использующих распространенную архитектуру AMD64. Рассмотренный в работе тип RoP-уязвимостей широко используется для проведения атак в настоящее время (примером может служить уязвимость данного класса CVE-2023-30799, которая имеет критический уровень опасности и применима для сотен тысяч устройств). Особенно такие уязвимости опасны при наличии обратной связи у

атакующего (например, при их реализации атаки на уязвимое устройство через Интернет). Предложенный в работе метод не устраняет сами уязвимости, но позволяет устранить используемые при данном классе атак опасные участки программ и проконтролировать качество результата, что обеспечивает актуальность работы. Повышает актуальность то, что защита может быть применена и для приложений, для которых у эксплуатирующей их организации отсутствуют исходные тексты.

Новизна исследования и полученных результатов, выводов и рекомендаций, сформулированных в диссертации

В диссертационной работе впервые:

1. Предложена модель вычислений, позволяющая рассматривать программы как «черный ящик» и определять, будут ли их выходные данные различимы при одинаковых входных данных. На основе данной модели сформулированы условия неразличимости, которые позволили создать алгоритм резервирования в защищаемых программах участков для дальнейшего встраивания кода системы защиты. Это позволило модифицировать существующий метод устранения из программы опасных участков, используемых в RoP-атаках. Суть модификации сводится к устранению опасных участков после компиляции, что обеспечивает отсутствие необрабатываемых участков в приложениях.

2. Предложено «цепочечное» связывание значений, используемых для защиты адресов возврата из подпрограмм, в соседних фреймах стека. Сами используемые для защиты значения являются псевдослучайными и отличаются для каждого экземпляра фрейма стека, что, в отличие от существующих методов, обеспечивает защиту от использования атакующим примитивов чтения. Раскрытие при предлагаемом подходе содержимого стека не снижает защищенность. Данная особенность критически повышает сложность атаки – злоумышленнику необходимо наличие и успешная эксплуатация двух различных типов уязвимостей в рамках вызова одной подпрограммы для успешной атаки.

3. Предложен усовершенствованный метод оценки подверженности приложений к RoP-атакам, который, в отличие от существующих реализаций, оценивает не только количество, но и предоставляемые опасными участками возможностями для атакующего. Это снимает необходимость экспертного анализа состава гаджетов в защищенном приложении и обеспечивает оценку принципиальной возможности проведения атак.

Значимость для науки и практики полученных автором диссертации результатов

Практическая значимость определяется предложенными алгоритмами и их программными реализациями в виде средства защиты программных средств, устраняющего пригодные для атак участки. Кроме того, разработанные решения в части встраивания средств защиты могут использоваться в качестве средства встраивания произвольных алгоритмов в другие приложения. Это позволяет снизить порог сложности для реализации другими разработчиками иных средств защит, так как, используя разработанное решение, они могут фокусироваться на специфичном функционале без необходимости решения проблемы встраивания и обеспечения неразличимости алгоритмов.

Полученные в рамках экспериментального анализа эффективности результаты показали, что разработанное решение позволяет оперативно обеспечивать защиту проприетарных приложений даже в случае отказа их разработчика устранять уязвимости рассматриваемого класса.

Связь темы диссертации с научно-техническими программами

Работа по теме диссертации проводилась в рамках гранта Минобрнауки России № 21/2020 на 2020–2021 гг. «Метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода». Грант выполнялся автором единолично. Работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой

части государственного задания ТУСУРа на 2023–2025 гг. (проект № FEWM-2023-0015).

Рекомендации по использованию результатов диссертационного исследования

Ведущая организация рекомендует основные результаты и выводы исследования для устранения уязвимостей в программных продуктах, для которых, с одной стороны, разработчик либо не устраняет, либо недостаточно оперативно устраняет уязвимости, и, с другой стороны, затруднена замена на аналоги с открытым исходным кодом. Особенно это ценно при наличии возможности доступа к потенциально уязвимому приложению через открытые компьютерные сети, включая Интернет. Кроме того, результаты могут использоваться разработчиками программных продуктов для защиты выпускаемого программного обеспечения (например, как замена средства Stackguard).

Обоснованность и достоверность научных положений, выводов и заключений

Достоверность работы подтверждается результатами, полученными с использованием предлагаемого в работе решения и их сопоставлением с имеющимися современными теоретическими и экспериментальными данными, полученными другими авторами в этой области. В части обеспечения защиты результаты сравнивались с публично доступными средствами G-free и Stackguard. Было показано, что, по сравнению с первым, устраняется большее количество гаджетов, а по сравнению со вторым, – доступность атакующему примитива чтения не приводит к снижению защищенности. В части полноты анализа сопоставление предложенного решения велось с дизассемблером IDA и показало сравнимое качество анализа. Необходимо также отметить, что содержание автореферата диссертации соответствует содержанию диссертации.

Соответствие автореферата основным положениям диссертации

Текст автореферата полностью отражает содержание диссертации и защищаемые научные положения

Подтверждения опубликованных основных результатов диссертации в научной печати

Основные результаты диссертации изложены в 14 печатных изданиях, 7 из которых изданы в российских рецензируемых журналах, в которых должны быть опубликованы основные научные результаты диссертации на соискание учений степени кандидата наук ВАК. Три публикации входят в международную систему цитирования *Scopus*. Результаты были опубликованы в следующих изданиях: Доклады ТУСУР, Информатика и автоматизация, Вестник Сибирского государственного аэрокосмического университета им. М.Ф. Решетнева, Программные продукты и системы, Известия ЮФУ. Технические науки, Безопасность информационных технологий НИЯУ МИФИ, Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», 11th International IEEE scientific and technical conference «Dynamics of systems, mechanisms and machines», Материалы XXV Международной научной конференции «Решетневские чтения».

По теме работы было получено 2 свидетельства на регистрацию программы для ЭВМ.

Результаты работы докладывались в 2021 году на семинаре кафедры БИТ СибГУ им. М.Ф. Решетнева и на семинаре кафедры КИБЭВС Томского государственного университета систем управления, а также на следующих конференциях:

– XXV Международная научная конференция «Решетневские чтения». Красноярск, 10–12 ноября 2021 г.

– 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies» (IT&QM&IS).

– XII International scientific and technical conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), 13–15 November 2018, Omsk, Russia.

– XX Международная научная конференция «Решетневские чтения». Красноярск, 1–13 ноября 2016 г.

– VII Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности SibInfo – 2007. Томск, 17–18 апреля 2007.

Соответствие содержания диссертации указанной специальности

Тема и содержание диссертационной работы соответствует паспорту специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность», в частности, по следующим пунктам:

п.15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

п.5. Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.

п.11. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.

Оценка содержания диссертации, ее завершенность в целом, замечания по оформлению

Представленная работа имеет завершенную логичную структуру и состоит и введения, пяти глав основного текста, заключения, списка литературы, включающего 104 наименования, и 9 приложений. Общий объем работы — 179 страниц, в том числе 13 таблиц и 11 рисунков.

Во введении обосновывается актуальность диссертационного исследования, дана оценка степени разработанности темы диссертационного исследования, сформулирована цель и соответствующие ей задачи

исследования, представлены научная новизна, теоретическая и практическая значимость, методология и методы исследования, изложены положения, выносимые на защиту.

Первая глава посвящена выявлению слабых мест существующих методов защиты и формулированию требований к предлагаемым решениям. Для этого была сформирована и проанализирована выборка публично доступных уязвимостей, выделены конечные состояния, необходимые атакующему, сформирована модель атак. Также даны описание структурных элементов программ для архитектуры AMD64 и рамки рассматриваемой предметной области. Далее сформирована выборка из средств защиты, выделены наиболее эффективные методы защиты, а также их недостатки, устранив которые, можно обеспечить защиту от рассматриваемого вида уязвимостей. Несовершенство существующих методов и их реализаций вкупе с множественным числом RoP-уязвимостей свидетельствует об актуальности модифицированного метода, устраняющего опасные участки. Не менее актуальным является встраивание системы защиты после сборки исполнимого образа программы, т.к. в противном случае невозможно надежно устранить опасные гаджеты и защитить программы при отсутствии для них исходных текстов. Далее в главе рассмотрены существующие подходы по встраиванию средств защиты в программы при отсутствии их исходных текстов, выделены основные проблемы, сделан вывод о необходимости обоснования неизменности алгоритма защищаемого приложения, что не рассматривается обычно авторами.

Во второй главе представлена модель вычислений, описывающая формирование выходных результатов работы программы на основе входных данных. По результатам сопоставления двух запусков одной и той же программы с учетом механизма ASLR и сторонних эффектов формулируется критерий самонеразличимости. Далее при условии выполнения этого условия формулируется критерий неразличимости алгоритмов с учетом семантики. По результатам анализа структуры программ предлагаются условия

выполнения модификации, при соблюдении которых исходная и производная программы будут семантически неразличимы, при этом во второй будут выделены участки для встраивания кода системы защиты. Предложен алгоритм встраивания, обеспечивающий модификацию с выполнением условий семантической неразличимости. Также обоснован выбор средств непосредственно для анализа и контроля корректности.

В третьей главе описывается метод снижения числа пригодных для проведения RoP-атак участков в программах, а также приводятся используемые в рамках него алгоритмы и методики. Для приведения в непригодное для использования атакующим состояние эпилогов подпрограмм применяется методика контроля целостности адреса возврата. Нововведением является использование для защиты значений, непредсказуемых для атакующего. Для устранения участков, которые используются злоумышленником за счет исполнения инструкций со смещением относительно их начала, предложен метод синонимических замен. В результате инструкции оригинальной программы заменяются на синонимичные, но не содержащие значений байт, интерпретируемых как инструкции возврата.

В четвертой главе предложен метод контроля эффективности систем защиты программ, направленных на снижение числа гаджетов. Данный метод учитывает недостатки существующих методов и основан на определении наличия у злоумышленника средств выполнения подпрограмм с ненулевым числом аргументом. При предложенном автором подходе учитывается не изменение числа гаджетов, а снижение их разнообразия и достаточность для проведения атак. Вводятся метрика защищенности и способ её расчета, позволяющие для обрабатываемой программы дать оценку сверху доступных злоумышленнику средств и возможности атаки в принципе.

В пятой главе приводятся результаты апробации и экспериментальной оценки эффективности разработанного средства защиты. Приводится архитектура программной реализации, результаты контроля корректности. Приведены результаты обработки приложений с расчетом метрик защищенности. Далее представлены результаты определения метрик для существующих аналогов, показывающие не только повышение защищенности, но и устранение средств проведения атак при использовании предложенного метода защиты. Также приведены результаты тестирования производительности предложенного решения, показывающие лучшую производительность по сравнению с альтернативными решениями.

В заключении приводятся основные результаты и выводы, полученные автором в ходе работы.

В ходе ознакомления с диссертационной работой возникли следующие вопросы и замечания:

1. В диссертации вводится понятие неразличимости программ. Не ясна цель такого введения, если существует тождественное понятие эквивалентности программ.

2. В работе не приведено, кем были разработаны методы защиты от атак (или предотвращения возможности атак), которые модифицируются и развиваются автором диссертации.

3. В диссертации на стр. 41 в конце пункта 2.1. утверждается: «Выбор следующего ББ зависит от состояния на момент начала ББ, но не на момент его окончания». Это утверждение довольно спорное, поскольку если ББ завершается операцией условного перехода и условие для нее вырабатывается в процессе выполнения ББ, то, очевидно, выбор следующего ББ зависит от состояния на момент окончания текущего.

4. В выводах к главе 2 совершенно неясен смысл вот этой фразы: «Далее формулируются условия неразличимости состояний с учетом

семантики программ, идея которой состоит в одинаковости адресов для ячеек памяти, хранящих семантически одинаковые значения, но не адресной информации».

Указанные замечания не снижают ценности проделанной автором работы и ее положительной оценки. В целом диссертация Лубкина И.А. выполнена на высоком научном уровне и представляет собой законченное научное исследование в области методов и систем защиты информации, в ходе которого получены новые, оригинальные методы и алгоритмы защиты исполняемого кода программ.

Результаты работы полностью и своевременно опубликованы в ведущих рецензируемых изданиях, рекомендуемых ВАК РФ, прошли апробацию в виде докладов на многих конференциях. Автореферат диссертации полно и верно отражает содержание работы.

Заключение

Диссертационная работа Лубкина Ивана Александровича «Метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода» выполнена на актуальную тему, обладает научной новизной и содержит авторское научно обоснованное техническое решение для поиска уязвимостей в исполняемом коде. Полученные в работе практические результаты свидетельствуют о вкладе Лубкина И.А. в совершенствование и развитие выбранного научного направления. Диссертация является завершенной научной квалификационной работой, соответствующей требованиям – пунктам 9 и 10 «Положения о порядке присуждения ученых степеней» ВАК России, предъявляемым к диссертационным работам, а её автор – Лубкин Иван Александрович – заслуживает присуждение ему ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Отзыв на диссертацию Лубкина И.А. «Метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода» обсужден и утвержден на расширенном заседании кафедры Защиты информации АВТФ НГТУ 17 ноября 2023, протокол № 12.

Заведующий кафедрой Защиты информации АВТФ НГТУ
кандидат технических наук, доцент,
Иванов Андрей Валерьевич
E-mail: andrej.ivanov@corp.nstu.ru

Подпись заведующего кафедрой Защиты информации
АВТФ НГТУ,
к.т.н., доцента Иванова А.В.
удостоверяю

вед. специалист по кадрам

24 ноября 2023 года

Сведения об организации:

Федеральное государственное бюджетное образовательное учреждение высшего образования Новосибирский государственный технический университет (НГТУ)

Адрес: 630073, г. Новосибирск,
пр-т К.Маркса, 20, тел. +7 (383) 346 50 01
E-mail: rector@nstu.ru
https://nstu.ru/