ОТЗЫВ

официального оппонента,
профессора кафедры КБ-2 «Информационно-аналитические системы кибербезопасности» ФГБОУ ВО "МИРЭА - Российский технологический университет", доцента
Максимовой Елены Александровны
на диссертационную работу

Лубкина Ивана Александровича на тему

«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

1. Актуальность работы

Уязвимости в программном обеспечении сегодня представляют серьезную угрозу для безопасности информационных технологий. В части предотвращения их эксплуатации можно выделить два основных направления: выявление с последующим устранением слабостей программного обеспечения и меры по повышению защищенности уязвимых приложений от атак злоумышленника. Так как невозможно формально доказать корректность алгоритмов в общем случае, то меры по повышению защищенности будут всегда востребованы при разработке и эксплуатации программного обеспечения. В современных защищенных операционных системах применяется ряд механизмов защиты от уязвимостей, таких как ASLR и StackGuard. Из-за компромиссов реализации подобные средства являются уязвимыми при наличии в распоряжении у атакующего примитивов чтения.

Поскольку диссертационная работа Лубкина И.А. направлена на создание средства защиты, избавленного от ряда недостатков существующих средств, выбранная тематика является актуальной.

2.Оценка содержания диссертации, ее завершенность

Диссертационная работа общим объемом в 179 страниц состоит из введения, 5 глав, заключения, списка сокращений, терминов и определений, списка литературы и 9 приложений. Список использованной литературы состоит из 104 наименований.

Во введении (стр. 5-12) дана общая характеристика работы, обоснована актуальность темы исследования, сформулированы цель и задачи,

представлены научная новизна, практическая значимость полученных результатов.

В первом разделе диссертационной работы (стр. 13-32) сформулированы модель атак и требования к разрабатываемому модифицированному методу повышения защищенности. Проведен анализ известных уязвимостей и средств защиты.

Во втором разделе диссертационной работы (стр. 33-62) приведен алгоритм резервирования мест для встраивания кода средств защиты, разработанный на основании модели вычисления выходных данных приложений. Также представлены условия модификации, выполнение которых исключает искажение алгоритма защищаемого приложения вследствие внесения модификаций.

В третьем разделе диссертационной работы (стр. 63-89) предложен метод защиты, обеспечивающий как защиту эпилогов подпрограмм, так и устранение уязвимых участков на безопасные синонимичные.

В четвертом разделе диссертационной работы (стр. 90-99) предложен метод оценки, применимый к классу средств защиты, основанных на снижении числа гаджетов в приложениях. Основу метода, отличающего его от существующих вариантов, составляет определение числа аргументов произвольных подпрограмм, доступных атакующему при проведении атак.

В пятом разделе диссертационной работы (стр. 100-117) содержатся результаты экспериментальной отработки и сравнения с аналогами, показывающие невозможность задавать для атакующего ни одного аргумента при вызове подпрограмм после применения средства защиты (что говорит о снижении числа пригодных для атак участков на 100 %) с накладными расходами, сравнимыми с аналогами. Для аналогов показана возможность проведения атаки при вносимых ими больших накладных расходах, чем предложенное средство.

В заключении диссертационной работы (стр. 118-119) представлены основные результаты и приведены перспективы дальнейшей разработки темы.

В приложениях диссертационной работы (стр.136-179) представлены результаты анализа эффективности предложенного решения, сопоставленные с аналогичным решением, копии актов внедрения результатов диссертационной работы и свидетельств о государственной регистрации программ для ЭВМ.

Результаты диссертационного исследования прошли апробацию на 4 международных и 1 всероссийской конференции. По проблеме диссертационного исследования автором опубликовано 14 научных работы, в том числе 7 статей в рецензируемых научных изданиях, рекомендованных ВАК, 3 - в журналах, входящих в международную систему Scopus, 4 – в материалах конференций; получено 2 свидетельства о государственной регистрации программы для ЭВМ.

Количество личных публикаций в рецензируемых изданиях – 1.

Содержание диссертации в полной мере отражает суть работы и решение поставленных перед автором задач. Диссертация является завершенной научно-квалификационной работой, написанной грамотным научным языком. Диссертация хорошо структурирована, характеризуется логической целостностью и последовательностью изложения материала. Автореферат диссертации полностью отражает содержание диссертации и полученные в ней результаты. По форме, как диссертация, так и автореферат, соответствует требованиям ВАК, предъявляемым к кандидатским диссертациям на соискание ученой степени кандидата технических наук.

3. Новизна полученных результатов

В диссертационной работе были разработаны:

1. Модифицированный метод снижения числа пригодных для проведения *RoP*-атак участков в программах, содержащий *новую* модель вычисления выходных данных программ, *новый* алгоритм резервирования мест для встраивания кода средств защиты и *новый* алгоритм синонимической замены элементов программы, содержащих опасные значения, обеспечивающий защиту программ при отсутствии их исходных текстов.
2. Модифицированная методика контроля целостности графа потока управления, *отличающаяся от аналогов* использованием псевдослучайных значений и устойчивая к атакам переполнения буфера.
3. Модифицированный метод оценки эффективности систем защиты программ от *RoP*-атак, содержащий *новую* модель атак и *новый* алгоритм расчета метрик защищенности программ от *RoP*-атак, позволяющий определить реализуемость построения злоумышленником эксплойта.

Научная новизна полученных соискателем результатов соответствует пунктам 5, 11, 15 паспорта специальности 2.3.6.

Положения, выносимые на защиту, дают достаточно ясное представление о проведенных исследованиях и являются новыми научными результатами.

4. Обоснованность и достоверность научных положений выводов и рекомендаций, сформулированных в диссертации

Научные положения, выводы и рекомендации базируются на общепризнанных и апробированных научных теориях: теории алгоритмов, вычислимых функций Чёрча, теории компиляции, теории графов, методах компьютерной алгебры, статистики, понятиях и методах теории сложности. В работе присутствуют ссылки на все заимствованные положения.

Подходы соискателя к решению поставленной задачи логично и системно взаимосвязаны и обусловливают непротиворечивость результатов исследования. Сказанное позволяет констатировать, что научные результаты диссертационного исследования вполне обоснованы.

Достоверность работы подтверждается результатами, полученными с использованием предлагаемого в работе средства защиты, и их сопоставлением с результатами других авторов, проводящих исследования в этой области, а также использованием для перекрестной проверки корректности инструментов анализа программ и средств повышения защищенности от *RoP*-атак, являющихся стандартами де-факто в отрасли.

Достоверность научных положений, выводов и рекомендаций, сформулированных в диссертации, следует также из фактов успешного практического применения предложенных И.А. Лубкиным подходов, что удостоверено актами о внедрении результатов исследования; подтверждается положительным рецензированием научных работ автора при их опубликовании в журналах, рекомендованных ВАК, а также обсуждением результатов работы на всероссийских и международных научных конференциях.

Таким образом, анализ содержания работы позволяет сделать вывод о достаточно высокой степени обоснованности и достоверности основных научных положений, выводов и практических рекомендаций, приведенных в диссертации.

5.Практическая значимость работы

Практическая значимость результатов диссертационного исследования заключается в том, что их применение позволяет как устранить уязвимые участки в эксплуатируемых приложениях, так и проконтролировать эффективность используемой защиты.

Практическая значимость результатов диссертационного исследования подтверждена тем, что полученные в ходе исследования результаты были внедрены в процесс разработки ПО в СФУ, производственный процесс АО «РТК-Сибирь» а также в образовательный процесс СибГУ, что подтверждается соответствующими актами внедрения.

Теоретическая и практическая значимость результатов диссертационной работы подтверждается также тем, что работа выполнялась 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) и при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой части государственного задания ТУСУРа на 2023–2025 гг. (проект № FEWM-2023-0015).

Полученные в работе результаты могут использоваться для повышения безопасности программного обеспечения как на этапе его разработки, так и на этапе его эксплуатации. Кроме того, результаты работы могут использоваться для встраивания других средств защиты в приложения даже при отсутствии их исходных текстов.

6.Замечания

1. В работе дана качественная оценка вероятности угадывания атакующим значения, используемого для защиты адресов возврата. При этом в литературе описан ряд атак (например, из семейства *blind ROP*), в которых множественные попытки обеспечивают угадывание или косвенное определение злоумышленником используемых для защиты значений. Таким образом, недостаточно дать только качественную оценку вероятности успешной атаки.
2. Не рассмотрено применение предложенного в рамках модели вычислений описания сторонних эффектов для спроецированных на виртуальную память диапазонов ввода-вывода, что позволило бы расширить область применения предложенных решений.
3. Основной акцент работы направлен на уязвимости удаленного исполнения кода. При этом не рассмотрен вопрос уязвимостей отказа в обслуживании защищаемых приложений и повышения их подверженности к таким уязвимостям после применения предложенного метода защиты.
4. В положении 1, выносимом на защиту (стр. 8 автореферата, стр. 10 диссертации), а также в выводах по главе 3 диссертации (стр. 89 текста диссертации) обозначены результаты количественной оценки снижения числа уникальных гаджетов и гаджетов, пригодных для атак, соответственно на 98-100% и 100%. Из текста диссертации не понятно, каким образом были получены данные значения.
5. В тексте диссертационной работы идет не обоснованное использование категорий «метод», «методика», «средство». Например, на стр. 4 автореферата говорится о требованиях, в одном случае, к предлагаемому методу, в другом – к предлагаемой методике, на стр. 6 – к разрабатываемому средству. Аналогичная ситуация по не совсем корректному использованию автором категорий «RoP-уязвимости» и «RoP-атаки». Например, при описании таблицы 1.1 (стр. 22 диссертации), а также при обозначении разрабатываемого средства: на стр. 11, 20, 63, 90, 93, 99 диссертации – речь идет о разработке средства «противодействия RoP-атакам», на стр. 5, 12, 23, 24, 107, 118 диссертации – о средстве «противодействия RoP-уязвимостям».
6. В научной новизне (стр. 7 автореферата, стр. 9-10 диссертации) диссертант обозначает предложенные им: модифицированный метод снижения числа пригодных для проведения *RoP*-атак участков в программах, модифицированную методику контроля целостности графа потока управления и модифицированный метод оценки эффективности систем защиты программ от *RoP*-атак. В Положениях, выносимых на защиту обозначены средства защиты, разработанные на их основе. При этом, в теме диссертации заявлен метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода, по тексту диссертации не идентифицируемый и не обозначенный.

7. В тексте диссертации не представлены программа и методика испытаний в рамках экспериментальной оценки корректности средства встраивания (п.5.2), что не позволяет в полной мере оценить их результаты (стр. 104 текста диссертации, таблица 5.2).

8. В тексте автореферата и диссертации отсутствует нумерация формул, что не позволяет проследить логическую связь между ними; используются сокращения без расшифровки (таблица 1 на стр. 21 автореферата и таблица 5.6 на стр. 110 диссертации), что затрудняет понимание их сути.

9. В заключении диссертации (стр. 118-119) в качестве одного из полученных результатов обозначен «алгоритм определения свободных ресурсов процессора с учетом бинарного интерфейса приложений», не обозначенный в основных выводах и результатах работы в автореферате (стр. 21-22). Кроме того, в тексте диссертации (стр.118) показано падение производительности на 13%, в тексте автореферата (стр. 22) – на 12,9%.

Необходимо отметить, что приведенные замечания не влияют на общую положительную оценку диссертации.

Работа соискателя обладает внутренним единством, содержит новые научные результаты и положения, выдвигаемые для публичной защиты и свидетельствующие о личном вкладе автора в науку.

7.Заключение

Диссертация Лубкина Ивана Александровича, представленная на соискание ученной степени кандидата технических наук, является завершенной научно-квалификационной работой, в которой решена важная научно-техническая задача автоматизированного поиска уязвимостей в исполняемом коде, что имеет существенное значение для построения эффективных программных средств защиты.

Диссертация выполнена на высоком научно-техническом уровне и основана на методах теории алгоритмов, теории сложности, вычислимых функций Чѐрча, теории компиляции, теории графов, методы компьютерной алгебры, статистики.

Оформление и стиль изложения соответствуют требованиям Положения ВАК. Автореферат полностью отражает содержание диссертации. Все основные научные результаты опубликованы в отечественной и зарубежной печати.

Поставленные в диссертации задачи соответствуют современному уровню научных исследований и представляют собой заметный вклад в развитие методов и систем защиты информации, информационную безопасность в части решения вопросов обеспечения защищенности эксплуатируемых программ.

Учитывая полученные в ходе диссертационного исследования результаты, считаю, что работа удовлетворяет критериям, изложенным в

«Положении о порядке присуждения ученых степеней» ВАК России, утвержденном постановлением Правительства РФ №842 от 24.09.2013, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор Лубкин Иван Александрович заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
доктор технических наук, доцент,
профессор кафедры КБ-2
«Информационно-аналитические системы
кибербезопасности» ФГБОУ ВО «МИРЭА
– Российский технологический
университет»

27.11.23 Максимова Елена Александровна

Тел.: +79616982279

Докторская диссертация защищена по специальности:
2.3.6 – Методы и системы защиты информации, информационная безопасность

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет» ФГБОУ ВО «РТУ МИРЭА», Проспект Вернадского, д.78, г.Москва, ЦФО, 119454, тел. +7 (499) 600-80-80 доб.20563, факс: +7 495 434-92-87, e-mail: mirea@mirea.ru, сайт: https://www.mirea.ru/

Подпись Максимовой Елены Александровны, профессора кафедры КБ-2 «Информационно-аналитические системы кибербезопасности» Федерального государственного бюджетного образовательного учреждения высшего образования "МИРЭА - Российский технологический университет", доктора технических наук, доцента заверяю: ученый секретарь Ученого совета РТУ МИРЭА Н.В. Кононова