УТВЕРЖДАЮ:

Проректор по научной и инновационной деятельности ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», доктор физико-математических наук, профессор

Логинов Ю. Ю.

_____ / «26» 09 2023 г.

м.п.

ЗАКЛЮЧЕНИЕ
федерального государственного бюджетного образовательного учреждения высшего образования
«Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева»

Диссертация «Метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода» выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева».

В период подготовки диссертации соискатель Лубкин Иван Александрович работал в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева» на кафедре безопасности информационных технологий в должности старшего преподавателя.

В 2008 г. окончил Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный аэрокосмический университет имени академика М.Ф. Решетнева по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».

Удостоверение о сдаче кандидатских экзаменов выдано в 2023 г. в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева».

Научный руководитель – Золотарев Вячеслав Владимирович, кандидат технических наук, доцент кафедры безопасности информационных технологий Федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева».

По итогам обсуждения принято следующее заключение:

Оценка выполненной соискателем работы.

Диссертация И.А. Лубкина является научно-квалификационной работой, в которой содержится решение важной и актуальной задачи разработки новой модели и оригинальных алгоритмов для повышения защищенности за счет снижения количества пригодных для реализации *RoP*-уязвимостей участков программ.

Актуальность темы и направленность исследования.

История развития информационных технологий и их современное состояние позволяют сделать вывод о том, что разработка программного обеспечения в общем случае не может исключать появление в нем ошибок. Отражением такого состояния дел являются работы по оценке нормального количества ошибок на определенное количество строк кода.

Ошибки программного обеспечения являются основой для реализации угроз. Объективно не может быть создана методика разработки программ, не содержащих ошибок. Устранение ошибок как разработчиками, так и специалистами по информационной безопасности также объективно не может быть выполнено полностью. Поэтому должны применяться меры, препятствующие использованию ошибок в качестве уязвимостей. Для этого выполняются мероприятия по устранению условий, специфичных для определенных классов уязвимостей. В работе рассматривается класс *RoP*-уязвимостей. Уязвимости такого типа основаны на передаче в программу вызывающих сбой данных. Некорректная их обработка нарушает граф потока управления и приводит к реализации уязвимостей удаленного исполнения кода.

Предлагаемый подход к защите ставит своей целью устранение фрагментов программ, используемых для реализации уязвимостей *RoP*-класса. Защита актуальна для программ, с которыми может взаимодействовать атакующий (например, сетевые сервисы, доступные через Интернет). Актуальность защиты от уязвимостей исполняемого кода программного обеспечения во многом обусловлена высоким уровнем распространения проприетарного ПО, исходный код которого представляет собой интеллектуальную собственность той или иной компании, которые, как правило, не заинтересованы в публикации или передаче своих разработок третьим лицам.

Личное участие автора в получении результатов.

Все достигнутые в диссертации результаты получены автором лично. Постановка задач работы осуществлена совместно с научным руководителем Золотаревым В.В. Разработанная модель, алгоритмы и её программная реализация, а также проведение эксперимента и интерпретация результатов выполнены автором лично под руководством Золотарева В.В.

Научная новизна диссертации.

В диссертационной работе были разработаны:

1. Модифицированный метод снижения числа пригодных для проведения *RoP*-атак участков в программах, отличающийся от аналогов встраиванием кода системы защиты в программные модули без требования наличия исходных текстов и с обеспечением неразличимости алгоритма защищенной и оригинальной программы.
2. Модифицированная методика контроля целостности графа потока управления, отличающаяся от аналогов использованием псевдослучайных значений для контроля целостности адресов возврата и защитой фреймов стека вызывающих подпрограмм.
3. Модифицированный метод оценки эффективности систем защиты программ от *RoP*-атак, отличающийся от аналогов определением достижимости конечного состояния системы, необходимого атакующему, путем анализа номенклатуры содержащихся в программе гаджетов.

Практическая значимость диссертации.

Разработанная в ходе работы модель, алгоритмы и программный комплекс могут быть использованы в автоматизированных системах с требованиями устойчивости к уязвимостям для защиты от атак, требующих для реализации стабильности размещения набора участков программного кода относительно друг друга.

Результаты работы по повышению защищенности от *RoP*-уязвимостей были внедрены в рабочий процесс АО «РТК-Сибирь», ФГАОУ ВО «Сибирский федеральный университет», а также в образовательный процесс ФГБОУ ВО СибГУ им. М.Ф. Решетнева для студентов кафедры безопасности информационных технологий.

Ценность научных работ соискателя, полнота изложения материалов диссертации в опубликованных работах.

По материалам диссертации И.А. Лубкина опубликовано 14 работ, из них 7 статей в журналах, входящих в перечень рецензируемых научных журналов и изданий, рекомендованных ВАК, и 3 зарубежные статьи, индексируемые в международной базе Scopus. В том числе получено одно свидетельство о государственной регистрации программ для ЭВМ.

Статьи, опубликованные в журналах, входящих в перечень рецензируемых научных журналов и изданий, рекомендованных ВАК:

1. Лубкин И.А. Метрики защищенности приложений при использовании средств противодействия уязвимостям, основанным на возвратно-ориентированном программировании / Лубкин И.А. // Доклады ТУСУР. – 2021. – Т. 24. – № 4. – С. 46–51.
2. Лубкин И.А. Комплексная система защиты от уязвимостей, основанных на возвратно-ориентированном программировании / И.А. Лубкин, В.В. Золотарев // Информатика и автоматизация. – 2022. – № 2(21). – С. 275–310.
3. Лубкин И.А. Методика динамического анализа уязвимостей в бинарном коде / Шудрак М.О., Золотарев В.В., Лубкин И.А // Вестник Сибирского государственного аэрокосмического университета им М.Ф. Решетнева. – Красноярск, 2013. – № 4(50). – С. 84–87.
4. Лубкин И.А. Методика и программное средство защиты кода от несанкционированного анализа / Шудрак М.О., Лубкин И.А. // Программные продукты и системы. – Тверь, 2012. – № 4. – С. 176–180.
5. Лубкин И.А. Статический анализ бинарного кода в сфере информационной безопасности / Шудрак М.О., Лубкин И.А., Золотарев В.В. // Известия ЮФУ. Технические науки. – Таганрог, 2012. – № 12. – С. 54–60.
6. Лубкин И.А. Методика декомпиляции бинарного кода и её применение в сфере информационной безопасности / Шудрак М.О., Лубкин И.А., Золотарев В.В. // Безопасность информационных технологий НИЯУ МИФИ. – М., 2012. – № 3 – С. 75–80.
7. Лубкин И.А. Методика защиты программного кода от несанкционированной модификации и исследования посредством его хеширования / Кукарцев А.М., Лубкин И.А. // Вестник сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнева. – Красноярск, 2008. – № 1 (18) – С. 56–60.

Статьи, индексируемые в международной базе Scopus:

8. Lubkin I.A. Automatic equivalency restoration after software patching / Lubkin I. A., Zolotarev V. V. // Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies» (IT&QM&IS). – Yaroslavl, 2021. – С. 217–222.
9. Lubkin I.A. Methodology of software code decomposition analysis / Lubkin I. A., Bazhenov I. O. // Dynamics of systems, mechanisms and machines. – Omsk, 2018. – С. 1–5.
10. Lubkin I.A. Technique of verified program module modification with algorithm preservation / Subboton N.A., Lubkin I.A. // 11th International IEEE scientific and technical conference "Dynamics of systems, mechanisms and machines". – Omsk, 2017. – С. 1–5.

Прочие публикации:

11. Лубкин И.А. Исследование генераторов псевдослучайных чисел, используемых для защиты от атак переполнения буфера / Лубкин И.А. // Материалы XXV Международной научной конференции «Решетневские чтения». – Красноярск, 2021. – С. 199–200.

12. Шудрак М.О. Методика декомпиляции бинарного кода и её применение в сфере информационной безопасности / Шудрак М.О., Лубкин И.А. // Материалы II Всероссийской молодежной конференции «Перспектива – 2012». – Таганрог, 2012. – С. 197–202.

13. Шудрак М.О. Методика декомпиляции бинарного кода и её применения в сфере информационной безопасности / Шудрак М.О., Лубкин И.А. // Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых ТУСУР. – Томск, 2012. – С. 245–250.

14. Шудрак М.О. Защита программного обеспечения методом полиморфной генерации кода / Шудрак М.О., Лубкин И.А. // Материалы XIV Международной научной конференции «Решетневские чтения». – Красноярск, 2010. – С. 199–200.

Свидетельства о государственной регистрации программы для ЭВМ и БД:

1. Библиотека защиты программного кода (libzpk). Свидетельство о регистрации программы для ЭВМ. ФИПС №2021666279 от 04.10.2021.

Соответствие содержания диссертации избранной специальности.

Диссертационная работа И.А. Лубкина по своему содержанию соответствует профилю специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», в частности, по следующим пунктам:

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

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

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

Диссертация «Метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода» Лубкина Ивана Александровича рекомендуется к защите на соискание учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Заключение принято на расширенном заседании научно-технического семинара кафедры безопасности информационных технологий Федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева»

Присутствовало на заседании 17 чел. Результаты голосования: «за» – 17 чел., «против» – 0 чел., «воздержалось» – 0 чел., протокол № 1 от «31» августа 2023 г.

Председатель семинара
к.т.н., доцент, зав. кафедры безопасности информационных технологий / В.В. Золотарев