ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 24.2.415.04, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР), МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____
решение диссертационного совета от 21 декабря 2023 г. № 3

О присуждении Лубкину Ивану Александровичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода» по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность – принята к защите 20 октября 2023 г. (протокол № 2) диссертационным советом Д 24.2.415.04, созданным на базе ТУСУРа (634050, г. Томск, пр. Ленина, 40). Приказ о создании диссертационного совета № 92/нк от 26.01.2023.

Соискатель Лубкин Иван Александрович, 9 марта 1986 года рождения, в 2008 г. окончил Сибирский государственный аэрокосмический университет им. М. Ф. Решетнева (СибГАУ). С 2008 по 2012 г. обучался в аспирантуре СибГАУ. Работает старшим преподавателем на кафедре безопасности информационных технологий (БИТ) Сибирского государственного университета науки и технологий им. М. Ф. Решетнева (СибГУ).

Диссертация выполнена на кафедре БИТ СибГУ.

Научный руководитель – кандидат технических наук доцент Золотарев Вячеслав Владимирович, зав. кафедрой БИТ СибГУ.

Официальные оппоненты: Максимова Елена Александровна, доктор технических наук, профессор кафедры КБ-2 «Информационно-аналитические системы кибербезопасности» МИРЭА – Российский технологический университет

(г. Москва); Абрамов Евгений Сергеевич, кандидат технических наук, зав. кафедрой безопасности информационных технологий им. О.Б. Макаревича Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета (г. Таганрог), дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет» (НГТУ), в своем положительном отзыве, составленном Ивановым А.В., кандидатом технических наук, заведующим кафедрой защиты информации факультета автоматики и вычислительной техники НГТУ, утвержденном Отто А.И., кандидатом технических наук, проректором по научной работе, указала, что диссертация Лубкина И.А. выполнена на высоком научном уровне и представляет собой законченную научно-квалификационную работу в области методов и систем защиты информации, в ходе которой получены новые, оригинальные методы и алгоритмы защиты исполняемого кода программ. Диссертация отвечает требованиям пункта 9 «Положения о порядке присуждения ученых степеней» по актуальности, научной новизне, значимости, объему выполненных исследований, практической и теоретической значимости, 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.

Соискатель имеет 14 опубликованных работ по теме диссертации, в том числе 7 работ, опубликованных в журналах, входящих в список ВАК, и 3 работы, опубликованные в журналах, индексируемых Scopus и/или Web of Science. Общий объем – 6,1 п.л., авторский вклад – 5,2. Получены 2 свидетельства на регистрацию программы для ЭВМ.

Наиболее значимые работы:

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. Lubkin, I. A. Automatic Equivalency Restoration after Software Patching / I. A. Lubkin, V. V. Zolotarev // Proceedings of the 2021 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", T and QM and IS 2021, Yaroslavl, 06–10 сентября 2021 года. – Yaroslavl, 2021. – P. 217-222.

4. Шудрак, М. О. Методика динамического анализа уязвимостей в бинарном коде / М. О. Шудрак, В. В. Золотарев, И. А. Лубкин // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. – 2013. – № 4(50). – С. 84-87.

5. Шудрак, М. О. Методика и программное средство защиты кода от несанкционированного анализа / М. О. Шудрак, И. А. Лубкин // Программные продукты и системы. – 2012. – № 4. – С. 176–180.

На диссертацию и автореферат поступило 7 положительных отзывов из следующих организаций: Отделение «ОКБ Сухого» в г. Таганроге – ОП ПАО «ОАК» (Толоманенко Е. А., к.т.н., инженер-программист второй категории); Казанский национальный исследовательский технологический университет (Садыков А.М, к.т.н, доцент кафедры информационной безопасности); Ростовский государственный экономический университет, г. Ростов-на-Дону (Лапсарь А.П., к.т.н., доцент кафедры информационной безопасности); Иркутский государственный университет путей сообщения (Кириллова Т.К., к.э.н., зав. кафедрой «Информационные системы и защита информации»); Казанский национальный исследовательский технический университет им. А.Н.Туполева (Аникин И.В., д.т.н., зав. кафедрой систем информационной безопасности); Иркутский национальный исследовательский технический университет (Маринов А.А., к.э.н., зам. руководителя центра компетенций по кибербезопасности института информационных технологий и анализа данных); АО «РЕШЕТНЁВ», Красноярский край, г. Железногорск (Потуремский И.В., к. т. н., директор по цифровому развитию).

В отзывах на автореферат указаны следующие основные замечания: в работе не хватает тестирования производительности для более широкого класса аппаратных конфигураций рассматриваемой архитектуры; алгоритм расчета метрики защищенности явно не описывает порядок обработки инструкций процессора с подразумеваемыми, но не указываемыми явно аргументами; в автореферате не указаны результаты полученной метрики защищенности, хотя в диссертации эта информация присутствует; не описана обработка технологической информации из состава заголовков программ, но необходимой для корректного их функционирования; не указан размер затрат времени на проведение анализа защищаемого приложения и на обеспечение его защиты; описание методики защиты эпилогов ошибочно не распространено на точку входа приложения, хотя сам текст методики это подразумевает.

Выбор официальных оппонентов обосновывается тем, что д.т.н. Максимова Е.А. обладает квалификацией анализа системных вопросов безопасности информационных систем в части подверженности действиям злоумышленника; к.т.н. Абрамов Е.С. является признанным специалистом в области информационной безопасности, что подтверждается списками опубликованных работ по теме диссертации.

Выбор ведущей организации обосновывается тем, что НГТУ имеет общепризнанные достижения в области разработки программного обеспечения с учетом требований к безопасности и способен определить и аргументированно обосновать научную и практическую значимость работы Лубкина И.А.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– ***разработан*** 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;

– ***разработана*** модифицированная методика контроля целостности графа

потока управления, *отличающаяся от аналогов* использованием псевдослучайных значений для контроля целостности адресов возврата и защитой фреймов стека вызывающих подпрограмм;

– ***разработан*** 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.

Теоретическая значимость исследования обоснована тем, что:

– *результативно использована* теория множеств и теория вычислимых функций Чёрча для создания модели вычисления выходных данных программ, которая позволила обеспечить встраивание кода средства защиты и обеспечить сохранение логики работы защищаемого приложения без необходимости наличия его исходных текстов.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

– ***разработанная*** программная реализация способа встраивания кода системы защиты с сохранением оригинальной логики ***внедрена*** путем вставки кода системы защиты в сервис *sshd*, используемый на сетевом периметре АО «РТК-Сибирь» с подтверждением корректной работы оригинального клиента с ним. *Разработанная* методика контроля целостности графа потока управления *внедрена* в процесс разработки ПО в СФУ, что обеспечило устранение гаджетов в разрабатываемых приложениях и сделало непригодными для эксплуатации уязвимости, находимые при фаззинге. Результаты внедрения подтверждаются соответствующими актами о внедрении.

Оценка достоверности результатов исследования выявила:

– ***теория*** построена на известных методах теории защиты информации, вычислимых функций Чёрча, компиляции;

– ***идея*** устранения используемых в ходе *RoP*-атак участков и оценки возможности проведения атаки путем анализа их состава *базируется* на анализе выборки уязвимостей и эксплойтов для них;

– ***использовано*** сравнение результатов применения авторских методов с опубликованными ранее методами иных авторов в отечественных и зарубежных публикациях и стандартизующих документах.

Личный вклад соискателя состоит в самостоятельной разработке и реализации метода снижения числа пригодных для проведения *RoP*-атак участков в программах (что обеспечило снижение подверженности приложений к реализации уязвимостей) и метода оценки эффективности систем защиты программ от *RoP*-атак, проведении апробации разработанных методов.

В ходе защиты диссертации были высказаны следующие критические замечания: 1) не рассмотрено применение предлагаемого метода защиты для приложений использующих *just-in-time*-компиляцию (например, написанных на языке *C#*); 2) не приведены затраты оперативной памяти, используемой на этапе применения разработанного средства защиты; 3) в ходе доклада не отражено, существуют ли иные средства, не приведенные в таблице на слайде 20 и выполнялось ли сравнение с ними; 4) второй пункт научной новизны не отражен в перечне поставленных задач.

Соискатель Лубкин И.А. ответил на задаваемые ему в ходе заседания вопросы и сформулированные замечания и привел собственную аргументацию: 1) применение предлагаемого метода защиты для таких приложений потребовало бы интеграции разработанного средства защиты в их компилятор и доказательства корректности этой процедуры, что выходит за рамки работы; 2) для анализа приложения требуется в 10 раз (оценка сверху) больше оперативной памяти, чем его размер; 3) для сравнения на слайде приведены лучшие средства защиты от *RoP*-атак, остальные проанализированы и имеют большее количество недостатков реализуемой защиты; 4) приведенная во втором пункте научной новизны методика разработана в ходе выполнения задачи 4.

На заседании 21 декабря 2023 г. диссертационный совет постановил за решение научной задачи обеспечения защищенности программ от *RoP*-уязвимостей, имеющей значение для развития средств противодействия уязвимостям в части защищенности бинарных приложений присудить Лубкину И.А.

ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 10 человек, из них 5 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 14 человек, входящих в состав совета, проголосовали: за – 10, против – 0, недействительных бюллетеней – 0.

Председатель
диссертационного совета Шелупанов Александр Александрович

Ученый секретарь
диссертационного совета Костюченко Евгений Юрьевич

22.12.2023