ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.087.01

на базе Федерального государственного бюджетного учреждения науки

Институт системного программирования им. В.П. Иванникова

Российской академии наук

Министерства науки и высшего образования РФ

по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____

решение диссертационного совета от 25 мая 2021 года № 2021/17

О присуждении Нурмухаметову Алексею Раисовичу, гражданину РФ ученой степени кандидата технических наук.

Диссертация «Применение диверсифицирующих преобразований для защиты от эксплуатации уязвимостей» по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» принята к защите 25 марта 2021 г., протокол № 2021/07 диссертационным советом Д 002.087.01 на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ; адрес: 109004, г. Москва, ул. А. Солженицына, дом 25), создан Приказом Минобрнауки России о советах по защите докторских и кандидатских диссертаций от 2 ноября 2012 г. № 714/нк.

Соискатель Нурмухаметов Алексей Раисович, 1990 года рождения, работает младшим научным сотрудником в Федеральном государственном бюджетном учреждении науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ).

В 2013 году соискатель окончил Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Московский физико-технический институт (государственный университет)». В 2016 году соискатель окончил

аспирантуру Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук.

Диссертация выполнена в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Научный руководитель – кандидат физико-математических наук Курмангалеев Шамиль Фаимович, старший научный сотрудник отдела компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук.

Официальные оппоненты:

1. Ильин Вячеслав Анатольевич, доктор физико-математических наук, главный научный сотрудник Курчатовского комплекса НБИКС-природоподобных технологий (КК НБИКС-пт) Федерального государственного бюджетного учреждения "Национальный исследовательский центр "Курчатовский институт",
2. Волконский Владимир Юрьевич, кандидат технических наук, начальник отделения «Системы программирования» ПАО «Институт электронных управляющих машин им. И.С. Брука»

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное учреждение «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук», г. Москва в своем положительном заключении, подписанном кандидатом физико-математических наук и заведующим отделом математического обеспечения ФГУ ФНЦ НИИСИ РАН А. И. Грюнталем, указала, что диссертационная работа является законченным научным исследованием, написанным на высоком научном уровне и полностью соответствует требованиям ВАК, предъявляемым к диссертациям на соискание

ученой степени кандидата технических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и достижениями в данной отрасли науки, наличием публикаций в сфере исследований, соответствующей теме диссертации, и способностью определить научную и практическую ценность диссертации.

Соискатель имеет 13 опубликованных работ, в том числе по теме диссертации 7 работ, в том числе 6 опубликованных в рецензируемых научных изданиях, 2 из которых опубликованы в изданиях, входящих в международную систему цитирования Web of Science и Scopus.

Публикации посвящены разработке диверсифицирующих методов для изменения программного кода во время компиляции и запуска, а также их реализации в рамках операционных систем семейства Linux. Вклад соискателя в совместных публикациях, где он значится первым автором, заключается в разработке методов диверсификации, их реализации, проведению и обработке экспериментальных результатов, подготовке статей.

Наиболее значимые работы по теме диссертации:

1. Нурмухаметов А.Р. [и др.]. Применение компиляторных преобразований для противодействия эксплуатации уязвимостей программного обеспечения // Труды Института системного программирования РАН. — 2014. — Т. 26, № 3. — С. 113—126.
2. Nurmukhametov A.R. [et al.]. Application of Compiler Transformations Against Software Vulnerabilities Exploitation // Programming and Computer Software. — 2015. — July. — Vol. 41, no. 4. — Pp. 231–236.
3. Нурмухаметов А.Р. Применение диверсифицирующих и обфусцирующих преобразований для изменения сигнатуры программного кода // Труды Института системного программирования РАН. — 2016. — Т. 28, № 5. — С. 93—104.

4. Нурмухаметов А.Р. [и др.]. Мелкогранулярная рандомизация адресного пространства программы при запуске // Труды Института системного программирования РАН. — 2017. — Т. 29, № 6. — С. 163—182.
5. Nurmukhametov A.R. [et al.]. Fine-Grained Address Space Layout Randomization on Program Load // Programming and Computer Software. — 2018. — Сент. — Т. 44, № 5. — С. 363—370.

Диссертационный совет отмечает, что соискателем получены новые научные результаты:

- разработан метод диверсификации кода программы на уровне промежуточного представления компилятора, который позволяет генерировать большое количество различных исполняемых образов программы с целью усложнения планирования широкомасштабной атаки на все множество копий программы;
- разработан метод рандомизации адресного пространства программы при запуске, который случайно меняет порядок следования функций в памяти, с целью осложнения эксплуатации уязвимостей;
- разработан метод оценки эффективности механизмов защиты от атак, которые повторно используют имеющийся в памяти процесса код. Метод заключается в оценке количества выживших гаджетов, в оценке вероятности функции остаться на своём месте, в экспериментальной проверке работоспособности различных ROP-цепочек.

Теоретическая значимость исследования состоит в том, что исследована задача случайных перестановок местами функций (с учетом их длины); в результате её решения установлено, что вероятность остаться на своем месте для крайних функций превосходит вероятность остаться на своем месте для функций, расположенных ближе к центру; этот результат указал на недостатки изначальной реализации системы защиты, и,

следовательно, реализация была улучшена (при помощи добавления сдвига

всех функций как целого) с точки зрения эффективности противодействия атакам, которые повторно используют имеющийся в памяти процесса код.

Значение полученных соискателем результатов исследования для практики состоит в том, что:

- на основе разработанных методов реализована дополнительная система защиты для операционных систем семейства Linux, которая внедрена в операционные системы компании ЗАО «МВП «Свемел» на базе дистрибутивов CentOS и Debian;
- разработанный метод оценки эффективности защитных механизмов может быть использован для тестирования других методов защиты от атак, которые повторно используют имеющийся в памяти процесса код.

Достоверность результатов исследования подтверждается тем, что:

- разработанные методы, реализованные в качестве дополнительной системы защиты операционной системы, показывают работоспособность в масштабах всей операционной системы;
- экспериментально показана эффективность реализованной защиты на примере синтетических тестов и на реальных примерах уязвимостей программного обеспечения.

Личный вклад соискателя состоит в разработке метода диверсификации кода программы при компиляции; в разработке алгоритма мелкозернистой рандомизации адресного пространства процесса при запуске программы; в реализации программного инструмента в виде дополнительной системы защиты для операционных систем семейства Linux; в проверке эффективности защиты, предоставляемой реализованной системой, от эксплуатации методами повторного использования кода; в обработке и в интерпретации результатов; в подготовке публикаций по теме исследования.

На заседании 25 мая 2021 г. диссертационный совет принял решение присудить Нурмухаметову А.Р. ученую степень кандидата технических наук.

При проведении голосования диссертационный совет в количестве 17 человек, из них 9 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 22 человек, входящих в состав совета, проголосовали: за – 17, против – 0, воздержались – 0.

Председатель диссертационного совета,
академик РАН Аветисян А. И.

Ученый секретарь диссертационного совета,
кандидат физико-математических наук Зеленов С. В.

25 мая 2021 г.