ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.1.120.01,
созданного 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 17 декабря 2024 года № 2024/18

О присуждении Сигалову Даниилу Алексеевичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Методы выявления поверхности атаки веб-приложений при помощи анализа клиентского JavaScript-кода» по специальности 2.3.5 – «математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» принята к защите 17 октября, протокол № 2024/15 диссертационным советом 24.1.120.01, созданным 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 Сигалов Даниил Алексеевич, 1993 года рождения.

В 2015 году соискатель окончил факультет вычислительной математики и кибернетики Московского государственного университета имени М.В.Ломоносова. В 2023 году окончил аспирантуру Федерального государственного бюджетного образовательного учреждения высшего образования Московский государственный университет имени М.В. Ломоносова.

Работает младшим научным сотрудником в Лаборатории математических проблем компьютерной безопасности Кафедры информационной безопасности факультета ВМК МГУ имени М.В. Ломоносова (ведомственная принадлежность — Министерство науки и высшего образования РФ).

Диссертация выполнена на кафедре информационной безопасности факультета Вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования Московский государственный университет имени М.В. Ломоносова (ведомственная принадлежность — Министерство науки и высшего образования РФ).

Научный руководитель – кандидат физико-математических наук Гамаюнов Денис Юрьевич, заведующий Лабораторией математических проблем компьютерной безопасности Кафедры информационной безопасности факультета ВМК МГУ имени М.В. Ломоносова.

Официальные оппоненты:

1. Мазин Анатолий Викторович, доктор технических наук, заведующий кафедрой защиты информации Калужского филиала федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»,
2. Курмангалеев Шамиль Фаимович, кандидат физико-математических наук, ведущий научный сотрудник отдела компиляторных технологий Федерального государственного бюджетного учреждения науки «Институт системного программирования им. В.П. Иванникова Российской академии наук»

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА - Российский технологический университет», город Москва в своем положительном заключении, подписанном Ивановой Ириной Алексеевной, кандидатом технических наук, доцентом, заведующим кафедры КБ-14 «Цифровые

технологии обработки данных» РТУ МИРЭА, указала, что диссертационная работа представляет собой законченную научно-квалификационную работу, в которой содержится решение научной задачи, имеющей значение для развития соответствующей отрасли знаний — математического и программного обеспечения вычислительных систем, комплексов и компьютерных сетей.

Соискатель имеет 6 опубликованных работ, в том числе по теме диссертации опубликовано 6 работ, из них в рецензируемых научных изданиях опубликовано 6 работ.

Публикации посвящены применению анализа клиентского JavaScript-кода для задач анализа защищённости веб-приложений, определению поверхности атаки сервера с помощью статического анализа клиентского JavaScript-кода. Вклад соискателя заключается в разработке и реализации методов анализа JavaScript-кода, проведении экспериментов с ними как на реальных данных, так и на тестовых наборах данных, в подготовке наборов данных для проведения экспериментов.

Наиболее значимые работы по теме диссертации:

1. Обнаружение серверных точек взаимодействия в веб-приложениях на основе анализа клиентского JavaScript-кода / Д. А. Сигалов, А. А. Хашаев, Д. Ю. Гамаюнов // Прикладная дискретная математика. — 2021. — № 53. — С. 32—54.

2. Поиск информации о принимаемых сервером запросах в закомментированном клиентском коде веб-приложений / Д. И. Назаров, Д. А. Сигалов, Д. Ю. Гамаюнов // Программная инженерия. — 2023. — Т. 14, № 5. — С. 245—253.

3. Finding Server-Side Endpoints with Static Analysis of Client-Side JavaScript / D. Sigalov, D. Gamayunov // Computer Security. ESORICS 2023 International Workshops. — Springer Nature Switzerland, 2024. — P. 442—458.

4. Dead or alive: Discovering server HTTP endpoints in both reachable and dead client-side code / D. Sigalov, D. Gamayunov // Journal of Information Security and Applications. — 2024. — Vol. 82.

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.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- Разработан метод выявления поверхности атаки сервера веб-приложения с помощью статического анализа клиентского JavaScript-кода. В рамках разработанного метода используется новый алгоритм статического анализа, предложенный в диссертационной работе. Проведена экспериментальная оценка эффективности алгоритма, которая показала увеличение числа обнаруживаемых серверных входных точек по сравнению с существующими инструментами.
- Разработана новая методика поиска уязвимостей веб-приложений в модели «чёрного ящика», позволяющая более полно выявлять недостатки. Повышение полноты достигается за счёт применения нового метода статического анализа для выявления поверхности атаки, предложенного в работе, в сочетании с существующими техниками обнаружения серверных входных точек, а также за счёт использования анализа клиентского кода для обнаружения уязвимостей клиентской стороны веб-приложения.
- Предложенный метод был реализован и используется в системах автоматизированного поиска уязвимостей, разрабатываемых ЦХАБД МГУ и ООО «СолидСофт».

Теоретическая значимость исследования обоснована тем, что:

- Изучены особенности реального JavaScript-кода в сети Интернет, влияющие на возможность анализа этого кода с целью выявления серверных входных точек. Выделены наиболее существенные особенности, обладающие широкой распространённостью на веб-сайтах, которые следует учитывать при разработке алгоритмов анализа. Выделенные особенности и результаты эксперимента по анализу их встречаемости описаны в работе.

- Изложена идея применения статического анализа клиентского кода для выявления поверхности атаки сервера. Приведена аргументация в пользу применимости такого подхода – наличие на страницах недостижимого кода, отправляющего запросы на сервер, а также наличие у методов динамического анализа трудностей с покрытием некоторых частей кода в случаях, кода интерфейс приложения устроен сложным образом.
- Разработан метод выявления поверхности атаки веб-приложения, использующий изложенную идею, а также методика поиска уязвимостей, применение которой предполагает использование разработанного метода.

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

- разработанный метод позволяет улучшать результаты анализа веб-приложения на предмет наличия уязвимостей в модели “чёрного ящика” и приводить к обнаружению новых недостатков безопасности приложения;
- разработанный метод применяется как часть системы автоматизированного обнаружения уязвимостей веб-приложений, разработанной ЦХАБД МГУ;
- разработанный метод внедрён как один из компонентов системы автоматизированного поиска уязвимостей SolidPoint, разрабатываемой ООО «СолидСофт»;
- в ходе экспериментов с разработанным в диссертации методом выявления поверхности атаки и с разработанной методикой поиска уязвимостей были обнаружены уязвимости реальных веб-приложений в сети Интернет.

Оценка достоверности результатов исследования выявила:

- Разработанный метод, реализованный в составе инструмента автоматического выявления серверных входных точек посредством статического анализа JavaScript-кода веб-страниц, показывает свою применимость в рамках анализа веб-приложений на предмет наличия уязвимостей.
- Проведено экспериментальное сравнение с несколькими инструментами извлечения информации о поверхности атаки сервера из клиентской части веб-приложения, на большей части тестовых приложений разработанному

средству удалось найти максимальное количество серверных входных точек как среди уязвимых входных точек приложений, так и среди всех известных входных точек.

Личный вклад соискателя состоит в исследовании клиентского кода реальных веб-приложений для выявления его специфики, с учётом которой сформулированы требования к методу статического анализа клиентского JavaScript-кода, в разработке и реализации метода статического анализа клиентского кода для выявления поверхности атаки сервера, в обработке и интерпретации экспериментальных результатов, подготовке статей.

В ходе защиты диссертации были высказаны следующие критические замечания:

- При сравнении результатов работы разработанного метода с аналогами приведено количество найденных каждым из инструментов входных точек, однако отсутствует оценка того, насколько совпадают наборы точек, найденных разными инструментами.
- Помимо JavaScript и HTML, существуют и другие способы реализации клиентов, взаимодействующих с сервером веб-приложения по протоколу HTTP. В работе не упоминаются другие виды клиентских приложений, не раскрыт вопрос применимости разработанного метода к ним, в том числе вопрос возможности и целесообразности анализа мобильных приложений с целью выявления поверхности атаки.
- В автореферате работы не уделяется должного внимания математической, строгой постановке задач, хотя автор использует специализированные нотации и формализованные описания в тексте диссертационной работы.
- Предложенные алгоритмы не содержат оценок сходимости, вычислительной сложности и ресурсной эффективности.
- В работе не рассмотрена проблема попадания в результаты работы метода входных точек, относящихся к сторонним сервисам, фаззинг которых может быть нежелателен, и чей клиентский код может присутствовать на странице.

Соискатель Сигалов Даниил Алексеевич согласился с замечаниями, ответил на задаваемые ему в ходе заседания вопросы.

На заседании 17 декабря 2024 года диссертационный совет принял решение: за решение научной задачи, разработку методов выявления поверхности атаки веб-приложений при помощи статического анализа клиентского JavaScript-кода, что имеет важное значение для развития технологий выявления потенциальных уязвимостей серверных компонентов веб-приложений, присудить Сигалову Д. А. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 15 человек, из них 8 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 20 человек, входящих в состав совета, проголосовали: за – 15, против – 0.

Заместитель председателя диссертационного совета,
доктор физико-математических наук Петренко А. К.

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

17 декабря 2024 года