Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.932.2

Павлюкевич
Сергей Геннадьевич

Алгоритмы обеспечения безопасности клиент-серверных приложений

АВТОРЕФЕРАТ
диссертации на соискание степени магистра технических наук
по специальности 1-40 80 02 «Системный анализ, управление
и обработка информации»

Научный руководитель
Севернёв Александр Михайлович
кандидат технических наук, доцент

Минск 2022

ВВЕДЕНИЕ

Рост значимости веб-сервисов в современном мире очевиден: практически все компании, начиная с самых мелких и заканчивая наиболее крупными, имеют свои приложения или сайты в интернете. Многие сервисы предоставляют возможность управления важными ресурсами по средствам веб приложения. В связи с этим огромное внимание уделяется изучению криптографических методов защиты информации, так как многая информация хранится на серверах в виде хеш-значений, используя различные методы симметричного шифрования, ассиметричные шифры и хеш-функции.

На данный момент существует множество методов авторизации и аутентификации пользователя: от самых простых - как введение логина и пароля, до самых сложных – включающих в себя многоэтапную систему подтверждения подлинности. Все они различаются используемыми протоколами передачи данных, сложностью реализации, стоимостью поддержания работоспособности системы и т.д.

В магистерской диссертации рассматриваются актуальные проблемы обеспечения безопасности клиент-серверных приложений и способы их решения. Рассмотрены методы и разработан новый алгоритм.

Для достижения поставленной цели необходимо решить следующие основные задачи:

– провести анализ предметной области;

– исследовать существующие методы аутентификации в клиент-серверных приложениях;

– исследовать проблемы, сложности и недостатки;

– рассмотреть выбранный метод и предложить новый алгоритм на его основе.

В первой главе приведён обзор требований и уровней гарантий аутентификации в клиент-серверных приложениях.

Во второй главе рассматриваются общение принципы и способы аутентификации в клиент-серверных приложениях.

В третьей главе приведены примеры реализаций современных методов аутентификации крупнейшими ИТ-компаниями.

В четвёртой главе представлен новый алгоритм по безопасному обновлению токена аутентификации.

Магистерская диссертация выполнена самостоятельно, проверена в системе «Антиплагиат». Процент оригинальности соответствует норме, установленной кафедрой.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель исследования. Целью диссертационной работы является исследование существующих и разработка новых алгоритмов обеспечения безопасности клиент-серверных приложений.

Задачи исследования. Достижение поставленной цели включает решение следующих задач:

– обзор существующих методов аутентификации в клиент-серверных приложениях;

– анализ существующих методов аутентификации в клиент-серверных приложениях;

– исследование выбранного метода и разработка алгоритма на его основе.

Объекты исследования. Объектами исследования являются существующие алгоритмы обеспечения безопасности клиент-серверных приложений.

Предметы исследования. Предметами исследования являются выбранные методы и алгоритмы, а также разработка новых на их основе.

Новизна полученных результатов. В ходе проведенного исследования разработано решение обновления токенов доступа, которое не использует дополнительные токены, не уступает в безопасности и проще в разработке.

Личный вклад соискателя. Соискателем выполнены все изложенные в работе разработки и исследования. Постановка задач и обсуждение результатов проводились совместно с научным руководителем и сотрудниками кафедры информационных технологий автоматизированных систем Белорусского государственного университета информатики и радиоэлектроники. Соавторы опубликованных работ принимали участие в обсуждении промежуточных и конечных результатов. Обработка, интерпретация данных, а также выводы сделаны автором самостоятельно.

Апробация результатов диссертации. Основные положения диссертационной работы опубликованы в научно-практическом журнале «Энигма» [2-А.].

Структура и объём диссертации. Диссертация состоит из оглавления, перечня условных обозначений и терминов, общей характеристики работы, введения, четырёх глав, заключения, списка использованных источников, списка публикаций автора. Полный объём диссертации составляет 55 страниц, включая 19 рисунков на 19 страницах и 5 таблиц. Список использованных источников включает 31 наименование, занимает 3 страницы.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, общей характеристики работы, четырёх глав, заключения и списка использованных источников.

В главе 1 «Исследование предметной области» рассмотрены и исследованы основные требования к механизмам безопасности, основные угрозы веб-приложений, а также способ построения уровней строгости аутентификации. На основании исследования были выделены основные уровни гарантии аутентификации и их правила.

В главе 2 «Способы аутентификации в веб-приложениях» выделены и исследованы наиболее популярные способы аутентификации веб приложений. Проведя их подробные анализы, был выделен и рассмотрен наиболее популярный механизм аутентификации, его реализация, основные преимущества и недостатки при работе с ним.

В главе 3 «Исследование реализаций современных систем аутентификации» проанализированы популярные технологии и аутентификаторы от ведущих компаний в области информационных технологий.

В главе 4 «Механизм обновления токена доступа для аутентификации по JWT-токенам» рассмотрены существующие методы и проведен сравнительный анализ с другими методами. На основании полученных знаний предложено альтернативное, более простое решение.

ЗАКЛЮЧЕНИЕ

Целью диссертационной работы является разработка нового алгоритма обеспечения безопасности клиент-серверных приложений на основе токенов, так как существующие решения хоть и считаются наиболее оптимальными для обеспечения безопасности, они имеют ряд недостатков в виду сложности своей структуры и реализации.

Во второй главе рассмотрены существующие методы обновления токена доступа в механизме аутентификации на основе токенов, а также проведен сравнительный анализ с методами обновления срока действия в механизме на основе *cookies*. На основании этого анализа сделан вывод, что методы обновления срока действия аутентификационных *cookies* не могут быть использованы для обновления срока действия токена доступа в механизме аутентификации на основе токенов. Был рассмотрен механизм обновления с использованием дополнительного токена (токена обновления), после чего был сделан вывод, что данный метод добавляет сложности как при работе с ним.

В третьей главе проанализированы существующие технологии и аутентификаторы, разработанные крупными и популярными компаниями индустрии информационных технологий. Была выявлена тенденция использования одноразовых паролей как способа аутентификации, что добавляет дополнительный уровень безопасности веб-приложениям. Аутентификация с использованием одноразовых паролей удовлетворяет третьему уровню гарантии аутентификации. В основе механизма аутентификации с использованием одноразовых паролей обычно лежит механизм аутентификации по токенам.

В последней главе, на основании полученных знаний, предложено альтернативное решение, которое соответствует изначально поставленным целям и задачам: оно является простым в реализации и, в то же время, с точки зрения безопасности не уступает существующим решениям обновления токена доступа без использования дополнительных токенов.

Таким образом, в результате исследования все поставленные задачи были решены.

СПИСОК ПУБЛИКАЦИЙ АВТОРА

[1-А.] Павлюкевич, С.Г. Построение классификатора изображений на основе предобученной нейронной сети / Н.С. Громовой, С.Г. Павлюкевич, В.Ю. Усик. // Научно-практический журнал «Энигма» / Раздел «Технические науки» – Минск, ноябрь 2021 г. – 14 с., [Электронный ресурс]. – Режим доступа: *https://enigma-sci.ru/domains_data/files/ROOT_DIRECTORY/POSTROENIE%20KLASSIFIKATORA%20IZOBRAZhENIY%20NA%20OSNOVE%20PREDOBUChENNOY%20NEYRONNOY%20SETI.pdf*.

[2-А.] Павлюкевич, С.Г. Алгоритмы обеспечения безопасности клиент-серверных приложений / Н.С. Громовой, С.Г. Павлюкевич, В.Ю. Усик. // Научно-практический журнал «Энигма» / Раздел «Технические науки» – Минск, январь 2022 г. – 17 с., [Электронный ресурс]. – Режим доступа: *https://enigma-sci.ru/domains_data/files/ROOT_DIRECTORY/POSTROENIE%20KLASSIFIKATORA%20IZOBRAZhENIY%20NA%20OSNOVE%20PREDOBUChENNOY%20NEYRONNOY%20SETI.pdf*.