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

Дещеня
Павел Александрович

АЛГОРИТМЫ БЕЗОПАСНОСТИ В КЛИЕНТ СЕРВЕРНЫХ ПРИЛОЖЕНИЯХ

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1 - 40 80 21 Системный анализ, управление и обработка информации (по отраслям)

Научный руководитель

В.С. Муха,
доктор технических наук,
профессор

Минск 2018

ВВЕДЕНИЕ

В настоящее время огромное внимание уделяется изучению криптографических методов защиты информации: различным видам шифрования, созданию цифровых подписей и цифровых водяных знаков и т.п.

Криптография естественным образом оказывает свое влияние и на сферу интернет приложений: многая информация хранится на серверах в виде хеш-значений, протокол TLS (SSL), получивший широчайшее распространение, использует различные методы симметричного шифрования, ассиметричные шифры и хеш-функции.

Однако, несмотря на обилие методов, позволяющих защитить пользователя от нежелательного воздействие, существует множество способов получения доступа к аккаунтам пользователей: кражи паролей, доступ с устройства пользователя, кражи при помощи социальной инженерии и т.п. Исследование, проведенное в рамках “2015 Cyber Security Survey: Major Australian Businesses”, помогло выявить основное типы угроз, вызывающих наибольшую обеспокоенность различных компаний. Предоставленная статистика отражает высокую актуальность угроз затрагивающих вопросы авторизации и аутентификации.

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. Также выбор методик зависит от степени важности хранимой информации и/или степени ущерба,

который может быть вызван при несанкционированном доступе.

Цель: исследование существующих и разработка новых алгоритмов обеспечения безопасности клиент-серверных веб-приложений.

Объект исследования: методы и алгоритмы аутентификации в клиент-серверных приложениях.

Задачей работы является обзор и анализ существующих методов аутентификации в клиент-серверных веб-приложениях, выбор одного из наиболее популярных механизмов и предложения по его модернизации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальности исследования

Рост значимости различных веб-сервисов в современном мире очевиден: практически все компании, начиная с самых мелких и заканчивая наиболее крупными имеют свои приложения или сайты в интернете. Множество предприятий выпускает продукцию, так или иначе, осуществляющую свою деятельность в глобальной сети. Постоянно растет уровень вовлеченности аудитории в различного рода веб-взаимодействия, ежедневное время, проводимое пользователями в сети увеличивается. Вместе с этим растет и доверие к веб-ресурсам: увеличивается количество пользователей интернет банков и магазинов, пользователи зачастую размещают на соответствующих ресурсах конфиденциальную информацию различной ценности. Многие сервисы предоставляют возможность управления важными ресурсами по средствам веб приложения.

Задачи исследования

1. Обзор существующих методов аутентификации в клиент серверных приложениях;
2. Анализ существующих методов аутентификации в клиент-серверных приложениях;
3. Исследование выбранного метода и разработка алгоритма, на его основе.

Новизна полученных результатов

Научная новизна заключается в том, что был предложен новый алгоритм обновления токена доступа (access token). Данный алгоритм позволяет обновить токен доступа (access token) без использования дополнительного токена обновления (refresh token). Данный алгоритм является более простым в реализации в сравнении с существующим алгоритмом с использованием дополнительного токена обновления (refresh token), при этом алгоритм не является менее безопасным.

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 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.

СОДЕРЖАНИЕ РАБОТЫ

В данной работе рассматриваются современные методы аутентификации в клиент-серверных приложениях.

В первой главе рассмотрены и исследованы основные требования к

механизмам безопасности веб-приложений, также рассмотрены основные угрозы. На основании этого выделены четыре уровня гарантии аутентификации, каждый из которых включает в себя определённые правила.

Во второй главе рассматриваются общение принципы и способы аутентификации в клиент-серверных приложениях. Сделан вывод, что наиболее популярным в настоящее время является алгоритм аутентификации по токену доступа, а наиболее популярная структура токена доступа – JSON Web Token (JWT-токен).

В третьей главе проанализированы технологии и аутентификаторы, разработанные крупными и популярными компаниями индустрии информационных технологий. Этот анализ выявил тенденцию использования одноразовых паролей, как способа аутентификации, что добавляет дополнительный уровень безопасности веб-приложениям.

В четвёртой главе представлен новый алгоритм по безопасному обновлению токена доступа (access token) для механизма аутентификации по токенам. Представленный механизм является более простым в реализации чем существующий в настоящее время механизм, так как не требует дополнительных токенов обновления (refresh token) для обновления токена доступа (access token).