МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Двухфакторная аутентификация с использованием технологии Bluetooth Web API

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Волковой Юлии Вячеславовны

Научный руководитель
доцент _____ А. С. Гераськин
23.01.2021 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2021 г.

Саратов 2021

ВВЕДЕНИЕ

На сегодняшний день довольно тяжело представить повседневную жизнь человека без современных передовых технологий. Они с каждым днем все больше внедряются в повседневность и становятся неотъемлемой ее составляющей[1]. Развитие технологий приводит к автоматизации и упрощению различных сфер деятельности. Одним из самых наглядных примеров является реализация программного обеспечения.

Однако прогресс не стоит на месте, и с развитием интернета увеличивается количество программного обеспечения, прошедшего трансформацию от мобильных и настольных приложений в сайт. Данная эволюция произошла в связи с тем, что разработка одного продукта в виде сайта, который доступен на всех устройствах, обходится гораздо дешевле создания нескольких продуктов для различных платформ.

В связи с этими проблема информационной безопасности с каждым днем становится все более и более актуальной[2]. Используется большое количество технологий, которые были созданы с целью обеспечить защиту информации на разных уровнях. Вследствие этого большую популярность обрела технология двухфакторной аутентификации. В качестве второго фактора аутентификации могут использоваться различные виды факторов, например, аппаратный токен или же push-уведомление с одноразовым кодом. Но есть ли более удобная технология для двухфакторной аутентификации?

Параллельно происходило развитие технологии Bluetooth и увеличение возможностей языка JavaScript в рамках браузера. Так в декабре 2009 года была выпущена спецификация ядра Bluetooth − Bluetooth low energy (BLE). Введение

---

[1] Грошева, Е. К. «Информационная безопасность: современные реалии» / Е. К. Грошева, П. И. Невмержицкий; [Электронный ресурс]: // Интернет-портал – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-sovremennye-realii/viewer (дата обращения 05.09.2020) – Загл. с экрана. – Яз. рус.

[2] Иванов, О. «Информационная безопасность в цифрах» / О. Иванов; [Электронный ресурс]: // Интернет-портал – URL: https://www.anti-malware.ru/analytics/Threats_Analysis/2018-cybersecurity-statistics (дата обращения 05.09.2020) – Загл. с экрана. – Яз. рус.

протокола Web-Bluetooth и его реализация многими браузерами привела к возможности взаимодействия браузера и Bluetooth-устройств.

Актуальность темы заключается в активной разработке BLE технологии для удобного применения в браузере персонального компьютера, который имеет Bluetooth-адаптер. Данная реализация позволит разработчикам своих устройств значительно упростить и ускорить создание новых приложений до уровня сложности создания сайта.

Новизна данной работы заключается в возможности передавать данные как с устройства, так и на устройство через Bluetooth, что позволяет использовать смартфон как хранилище токена для двухфакторной аутентификации.

Исходя из выше изложенного, можно сформулировать цель данной дипломной работы − практическая реализация двухфакторной аутентификации с использованием Bluetooth Web API.

А для достижения выше поставленной цели необходимо решить следующие задачи:

- изучить двухфакторную аутентификацию;
- рассмотреть виды факторов аутентификации, их достоинства и недостатки;
- исследовать беспроводную технологию передачи данных Bluetooth;
- рассмотреть основные режимы передачи данных;
- изучить стандарт Bluetooth Web API.

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 50 страниц, из них страниц 37 – основное содержание, включая 25 рисунков и 2 таблицы, список использованных источников из 21 наименования.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы «Двухфакторная аутентификация» содержит описание и объяснение, что такое двухфакторная аутентификация, где она применяется, описание процесса и подхода. В разделе описана практика использования различных типов факторов:

1) Фактор знания: то, что знаете только вы − к данному фактору относятся секретные сведения, которые знает только авторизованный субъект. Например, PIN-код, пароль или секретная комбинация клавиш.

2) Фактор владения: то, чем вы владеете − к данной категории относятся предметы, которыми владеет авторизованный пользователь. Например, ключ от замка, личная печать или вариация аппаратного токена.

3) Фактор свойства: то, что является частью человека − к этому фактору относится все, что подходит под определение биометрических данных − лицо, отпечатки пальцев, радужная оболочка глаз, последовательность ДНК.

Были детально описаны существующие на данный момент виды факторов: аппаратный токен, аудио и текстовые сообщения, программный токен и push-уведомления, представлены их достоинства и недостатки.

Второй раздел «Исследование технологии Bluetooth» был посвящен беспроводной технологии передачи данных Bluetooth − технологии, с помощью которой реализуется возможность беспроводного обмена данными между такими устройствами, как персональные компьютеры (настольные, карманные, ноутбуки), мобильные телефоны, интернет-планшеты, принтеры, цифровые фотоаппараты, мышки, клавиатуры, джойстики, наушники и другие, расстояние между которыми сильно зависит от преград и помех, однако может достигать 100 метров.

Были описаны история технологии, на чем основана ее концепция, какие технологии используются для передачи данных на расстоянии, расписанные по пунктам плюсы и минусы. В первой части данного раздела описывается развитие технологии, этапы совершенствования. Были указаны ключевые спецификации технологии: Bluetooth 3.0, Bluetooth 4.0, Bluetooth 4.2, Bluetooth

5.0. У каждой спецификации были кратко описаны новшества и отличия от их предшественников.

Поскольку устройства поддерживают несколько режимов скоростей передачи данных, то во второй части данного раздела было приведено описание режимов скорости передачи данных:

- базовая (Basic Rate, BR) и улучшенная скорость (Enhanced Data Rate, EDR) передачи данных;
- высокоскоростной режим (High Speed, HS) передачи данных с альтернативным MAC/PHY;
- Энергосберегающий режим (Low Energy).

Как итог данной части раздела – таблица с детальными сравнительными характеристиками стандартов Bluetooth.

Таблица 1 – Основные отличия Bluetooth BR/EDR и LE

Характеристика	Bluetooth BR/EDR	Bluetooth LE
Физические каналы	79 каналов по 1 МГц	40 каналов по 2 МГц
Сканирование/Подключение	Запрос/Ответ	Эдвертайзинг (Advertising)
Количество устройств пиконета	7 активных / 255 всего	Неограничено
Приватность адресов устройств	Нет	Доступно
Максимальная скорость передачи данных	1-3 МБит/с	1 МБит/с при GFSK модуляции
Алгоритм шифрования	E0/SAFER+	AES-CCM
Радиус действия	30 метров	50 метров
Максимальная выходная мощность	100 мВт (20 дБм)	10 мВт (10 дБм)

В третьей части раздела была проанализирована безопасность данной технологии и сделан вывод, что при соблюдении базовых требований к безопасности Bluetooth не несет серьезной угрозы для обычного пользователя данной технологии, также хорошей практикой для достижения максимальной практики являются несколько правил: не устанавливать соединение с неизвестными устройствами Bluetooth; отключать Bluetooth, если в данный момент вы его не используете.

В третьем разделе был сделан обзор на Bluetooth Web API – интерфейс, с помощью которого происходит взаимодействие Bluetooth-устройств с сайтами, примеры существующих API, продемонстрирована поддержка Bluetooth Web API всеми современными браузерами, что показано на рисунках ниже.

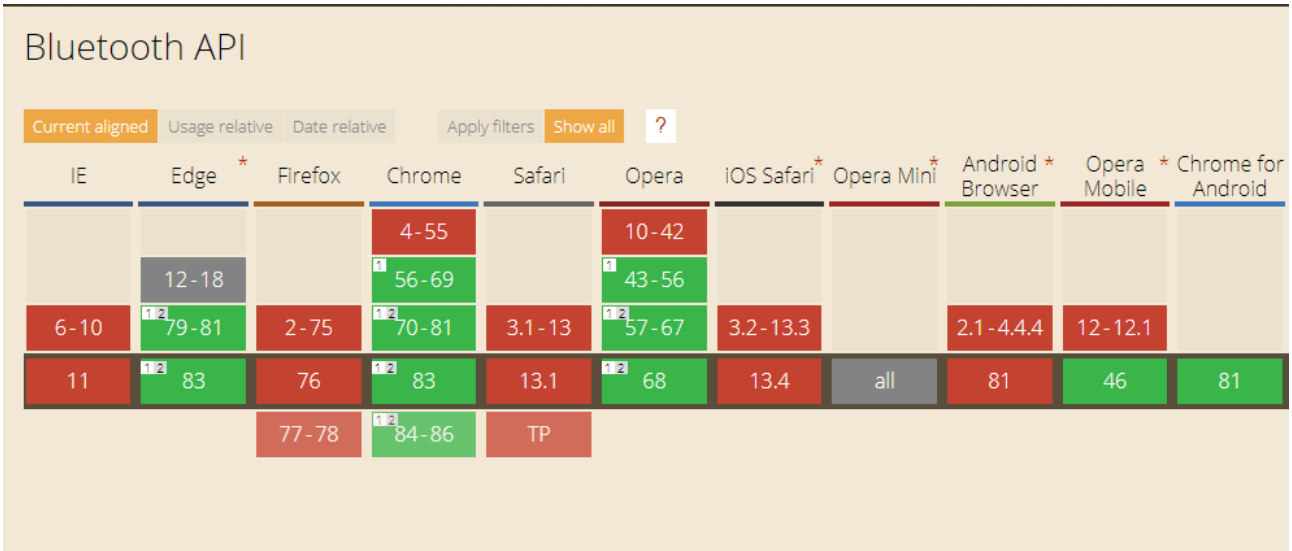

Рисунок 1 – Поддержка Bluetooth Web API

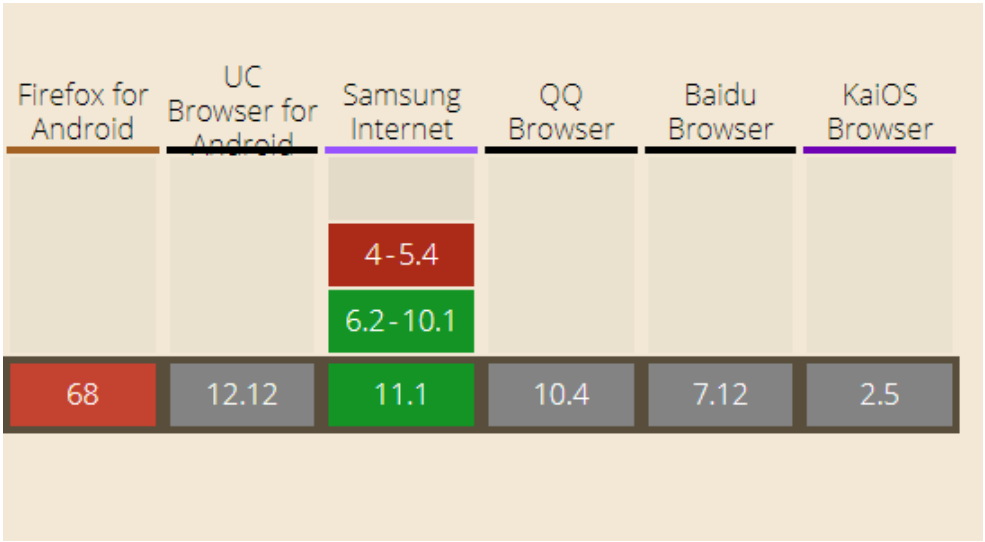

Рисунок 2 – Поддержка Bluetooth Web API

Также была описана текущая версия спецификации Bluetooth Web API, рассмотрены существующие риски безопасности и способы ими воспользоваться злоумышленникам. Во второй части данного раздела по пунктам была расписана защита от уязвимостей со стороны разработчиков вредоносных Web-сайтов:

- уязвимость ближайших Bluetooth-устройств;
- атака близлежащих Bluetooth-устройств;
- ошибки безопасности Bluetooth-устройств.

В третьей части – произведено сравнение вредоносных программ в нативном приложении и на сайте, что продемонстрировано в таблице ниже.

Таблица 2 — Сравнение шагов для получения доступа в нативном приложении и на Web-сайте

Нативное приложение	Web-приложение
Шаг №1. Нажать на рекламное предложение об установки приложения	Шаг №1. Просиходит вызов метод navigator.bluetooth.requestDevice()
Шаг №2. Нажать «Установить приложение»	Шаг №2. Пользователь должен выбрать уязвимое устройство в модальном окне для подтверждения, в котором имеется информация о сопряжении
Шаг №3. Нажать «Открыть приложение»	Шаг №3. Пользователь должен нажать «Сопряжение»
Шаг №4. Разрешить, путем нажатия «Принять» в запросе, использования Bluetooth	

Четвертый раздел – это раздел программной реализации Bluetooth Web API. В данном разделе были представлены алгоритмы регистрации и аутентификации на сайте, что показаны ниже, также были описаны используемые технологии: язык JavaScript и библиотеки React – клиентская часть, NodeJS – интерпретатор для серверной части.

В качестве успешной реализации программы были продемонстрированы все этапы работы приложения.

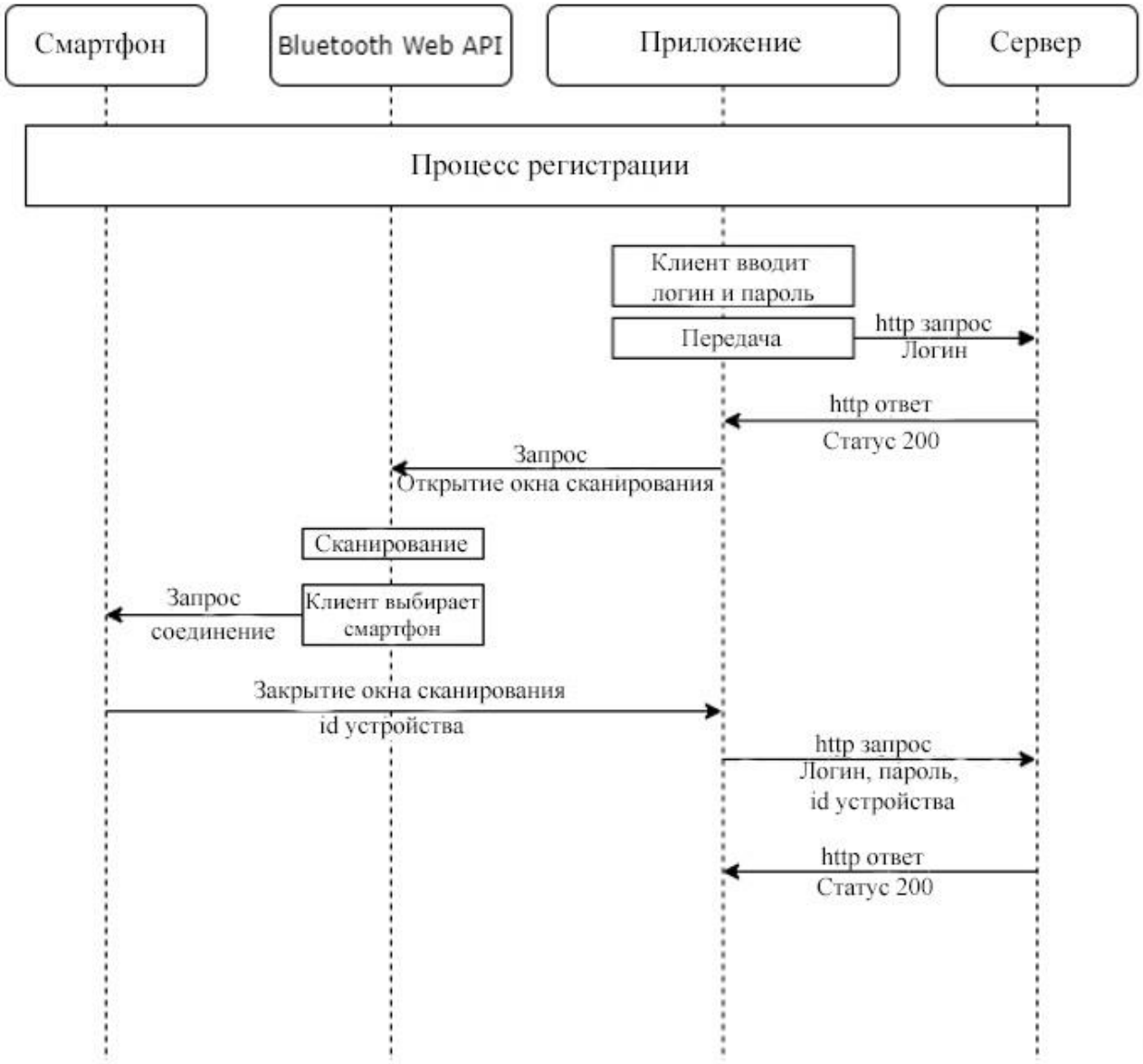

Рисунок 3 – Блок-схема алгоритма регистрации на сайте

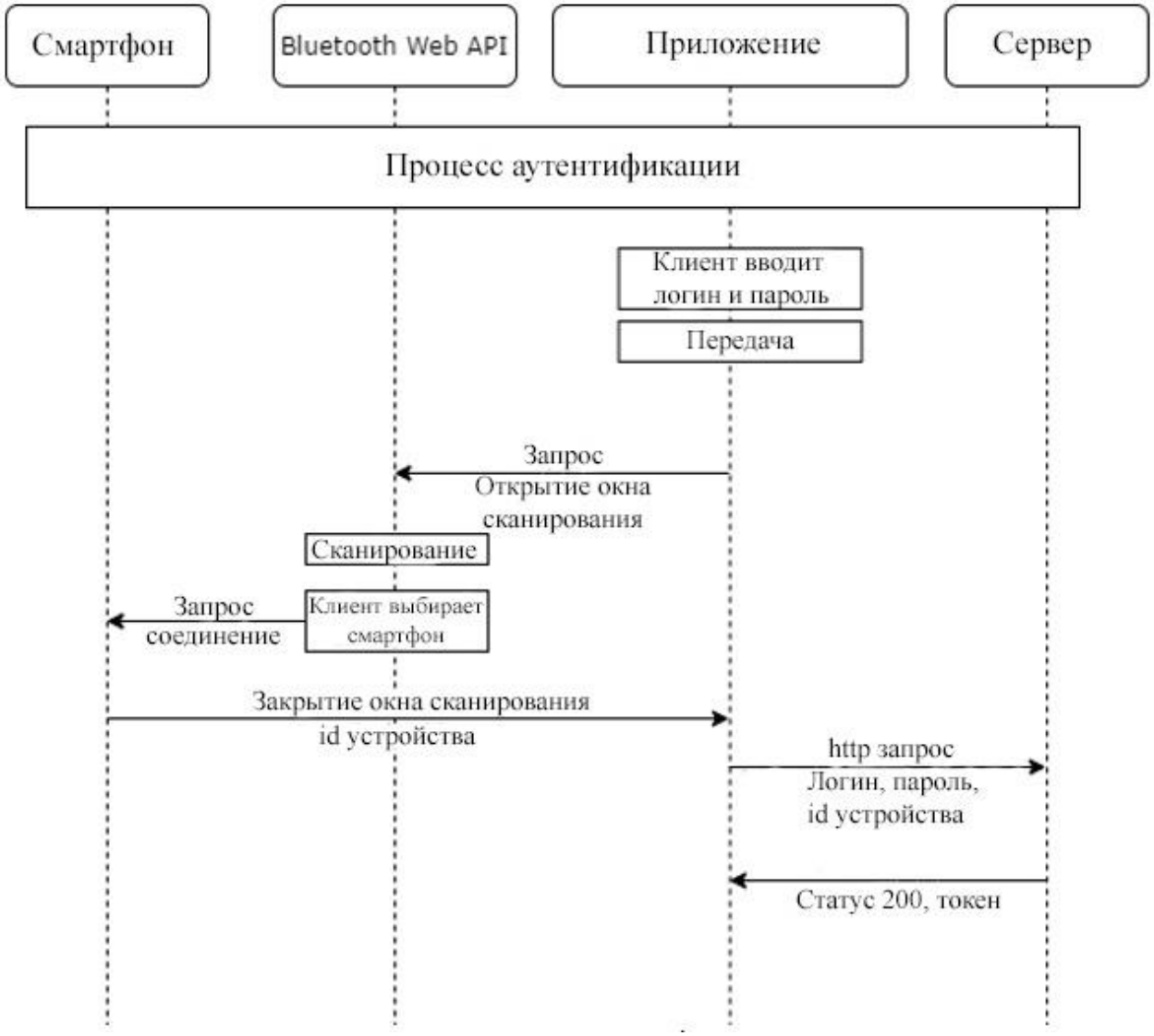

Рисунок 4 – Блок схема алгоритма аутентификации на сайте

В пятом разделе дипломной работы было проведено тестирование для верификации работоспособности разработанной библиотеки. Тестирование показало корректную работу продукта, реализованного в рамках дипломной работы.

ЗАКЛЮЧЕНИЕ

В настоящее время информация является достаточно ценным ресурсом, поэтому защита информации от несанкционированного доступа злоумышленниками является актуальной проблемой. В данной работе была реализована двухфакторная аутентификация, где в качестве второго фактора использовался смартфон с поддержкой Bluetooth.

Таким образом, в дипломной работе была изучена двухфакторная аутентификация, на какие категории можно поделить устройства, которые могут использоваться в качестве второго фактора аутентификации. Были рассмотрены виды факторов, проанализировали, какие достоинства и недостатки существуют у каждого вида фактора.

В следующем разделе был произведено исследование беспроводной технологии передачи данных Bluetooth, концепция технологии, а также принцип работы. После чего изучили развитие Bluetooth, кратко описали все существующие версии, указали новшества, которые приходили с каждой версией, рассмотрели и сравнили режимы передачи данных.

В третьем разделе, после изучения всех базовых технологий, которые необходимы для достижения цели данной дипломной работы, изучили стандарт Bluetooth Web API, рассмотрели поддержку браузерами данного стандарта, произвели анализ потенциала разработчиков вредоносных сайтов, а также сравнение вредоносные программы в нативном приложении и Web-сайте.

Далее в рамках практической части были описаны технологии, с помощью которых был разработан прототип переиспользуемого модуля Web-сайта, алгоритмы создания аккаунта и аутентификации, которые представлены в виде блок-схем.

После чего была протестирована пракически реализуемая часть диплома. Результаты тестирования продемонстрировали корректную работу реализуемой библиотеки.