3. Методы защиты от mimikatz в домене Windows. — Текст : электронный // Winitpro : [сайт] — 2020. — 16 нояб. — URL: https://winitpro.ru/index.php/2017/08/24/metody-zashhity-ot-mimikatz-v-domene-windows/ (дата обращения: 25.04.2022).
4. Руководство по SQL-инъекциям: изучаем на примерах. — Текст : электронный // tgraph : [сайт] — 2018. — 22 окт. — URL: https://tgraph.io/Rukovodstvo-po-SQL-inekciyam-izuchaem-na-primerah-10-22?tg_rhash=6f689bcee5d75f (дата обращения: 10.04.2022).
5. Positive Technologies. Погружение в AD: разбираем продвинутые атаки на Microsoft Active Directory и способы их детекта / Positive Technologies. — Текст : электронный // Habr : [сайт]. — 2018. — 20 сент. — URL: https://habr.com/ru/company/pt/blog/423903/ (дата обращения: 20.04.2022).
6. Хантер Т. Разбираем атаки на Kerberos с помощью Rubeus / Т. Хантер. — Текст : электронный // Habr : [сайт]. — 2020. — 19 июня. — URL: https://habr.com/ru/company/tomhunter/blog/507140/ (дата обращения: 24.03.2022).
7. Принципы аутентификации по протоколу Kerberos — Текст : электронный // IT band : [сайт]. — 2017. — URL: http://itband.ru/2010/12/kerberos1/ (дата обращения: 14.03.2022).

Н. Н. Халтурин, Д. Д. Сухарев, А. В. Широких
Тюменский государственный университет, г. Тюмень

УДК 004.056

РАЗРАБОТКА ЗАЩИЩЕННОГО МОБИЛЬНОГО ПРИЛОЖЕНИЯ «МОБИЛЬНЫЙ ОХОТИНСПЕКТОР»

Аннотация. *В рассматриваемой работе представлено мобильное приложение, разработанное для отечественных охотников, позволяющее безопасно, комфортно и законодательно заниматься охотой в России. Подробно описаны используемые при разработке технологии, принципы и рекомендации по информационной безопасности.*

Ключевые слова: *мобильная разработка, авторизация, API, Android, Flutter.*

Введение. В настоящее время многие люди стали пользоваться смартфонами повсеместно каждый день. Используя смартфоны,

пользователи могут выполнять различные задачи в любой точке мира. Это повседневные задачи, обустройство дома и использование «умной» бытовой техники, поиск необходимой информации в Интернете, покупки и бронирование различных услуг во время работы или учебы и т. д. Простое в использовании и компактное мобильное устройство для решения многих ежедневных человеческих проблем способствовало невероятно быстрому росту популярности смартфонов среди пользователей по всему миру. Это привело к развитию конкурентного рынка, где компании работают над совершенствованием и развитием собственных уникальных решений, вкладывая все больше ресурсов в исследование тенденций и законов рынка и разработку новых продуктов. Нет никаких сомнений в том, что вышеприведенные аргументы также относятся к рынку охоты в России.

Проблема исследования. В этой работе представлено кроссплатформенное Flutter-приложение, разработанное для компании “Foxcom”, которая занимается созданием клиентских приложений и информационных систем для охотников в России. Разработка приложения должна включать в себя использование современных отечественных методов [1] и рекомендаций по обеспечению безопасности программы [2], которая взаимодействует с серверной частью через сетевые запросы [3]. При помощи созданного мобильного приложения охотники смогут отслеживать свое местоположение на карте, на которой нанесены и выделены специальные зоны — охотугодья, и получать уведомления в случае пересечения их границ. Также, пользователи получат возможность найти всю необходимую информацию об уже полученных ранее разрешениях на охоту.

Материалы и методы

Архитектура приложения

В основе работы мобильного приложения ключевую роль играет «Единая защищенная мобильная платформа: центр мобильных сервисов». Это продукт в реестре отечественного ПО [1]. Обеспечивает

безопасное взаимодействие между мобильным приложением и системой поставщиком данных. В виде схемы это можно изобразить следующим образом (рис. 1):

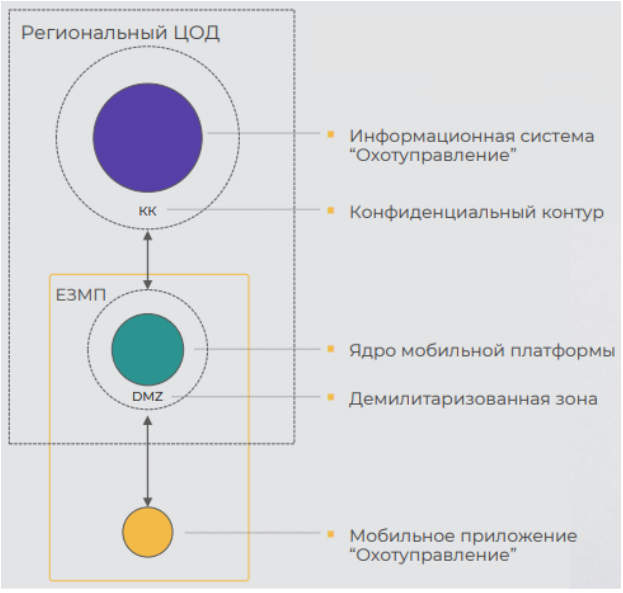

Рис. 1. Архитектура решения

Информационная система представляет собой приложение-агрегатор, который взаимодействующий с базой данных, через которую происходит формирование запросов и отправка данных на Ядро. Конфиденциальный контур — это изолированная сеть, в которую есть доступ с конкретными сетевыми настройками, установленными на стороне ИС и Ядра. Ядро же выступает в роли proxy. Это набор сервисов, обеспечивающих авторизацию в мобильном приложении на основе подписанных сертификатов через CryptoPro.

Защита от угроз

В качестве минимальной версии для Android было принято решение взять именно версию Android 4.4. Во-первых, версия еще поддерживается некоторым количеством разработчиков, позволяя нам охватить большее число потенциальных устройств. Во-вторых,

начиная с версии 4.4, Google начинает делать первые шаги на пути повышения безопасности мобильных приложений. Это выражено более усложненным механизмом, предотвращающим перехват отправляемого и получаемого траффика сервисами Google, что положительно сказывается на общей безопасности приложения.

Главным и основополагающим инструментом работы приложения является протокол Https. Выбор этого протокола обусловлен тем, что он использует SSL и TLS для шифрования соединения между клиентом и сервером, что решают проблему уязвимости http протокола для типа атаки «человек посередине». Так, например, используя библиотеку okhttp, при помощи OkHttpClient.Builder, указывая различные способы шифрования (cipherSuites) и версий TLS (tlsVersions), мы можем благоприятно влиять на безопасность нашего приложения на устройствах с разными версиями от разных производителей. Конфигурации для различных версий устройств и их совместимости с протоколами и шифрами можно найти в официальной документации.

Помимо необходимости использования защищенного сетевого протокола необходимо реализовать логику авторизации пользователей. Аутентификация на стороне сервера и авторизация на клиентском устройстве осуществляется при помощи использования двух типов токенов. Это в первую очередь токен доступа(access) и обновления(refresh). Суть разработанной схемы аутентификации пользователя состоит в использовании этих токенов по следующему алгоритму: если охотник успешно прошел авторизацию через Госуслуги (рис. 2-3), то на стороне серверной части генерируется уникальный токен, при создании которого используется хэш-функция. Хэшированный access токен неотъемлемая часть прохождения аутентификации на сервере, так как только при его валидности клиент получит доступ к своим учетным данным. В целях безопасности токен доступа валиден в течение часа от момента создания и требует своевременного продления. За это отвечает токен обновления. Refresh токен приходит вместе с данными об учетной записи и является обязательным параметром при продлении токена доступа. Весь процесс продления никак не зависит от пользователя, и его реализация

и выполнение полностью сокрыто от охотника. Реализованная схема позволит усилить безопасность приложения даже при несанкционированном перехвате злоумышленниками входящих и исходящих сетевых запросов.

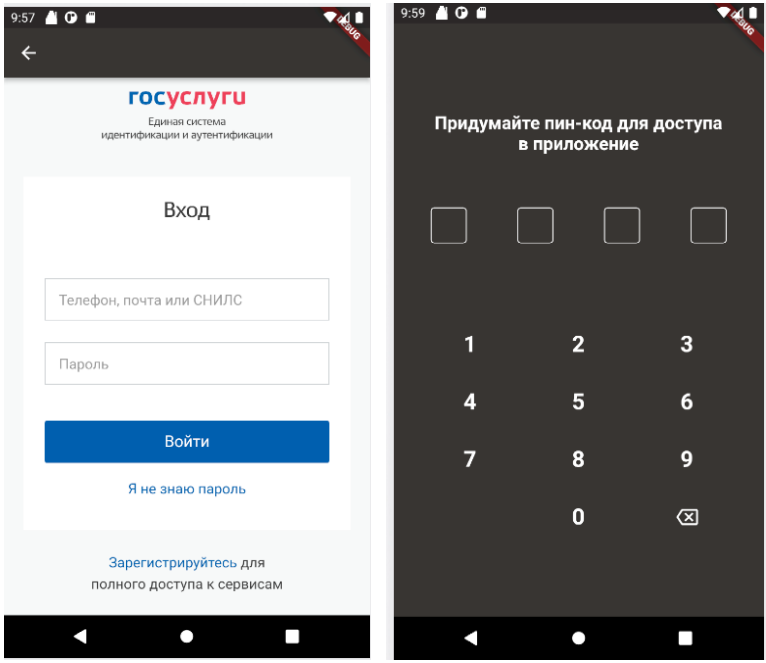

Рис. 2-3. Авторизация в мобильном приложении

Результаты.

Рекомендации ФСТЭК

При создании приложения было очень важно соблюсти рекомендации ФСТЭК для обеспечения безопасности [2]. На данном этапе были решены следующие известные проблемы:

1. Сокрытие логов приложения от рядового пользователя. Это было реализовано при помощи разделения версия на релизную(release) и тестовую(debug). В релизной версии не предусматривалось отображение всплывающих окон с логами ошибок и использование специально подключенного сервиса-помощника Alice,

отслеживающего статусы и ответы при использовании сетевых запросов. В тестовой же сборке эти аспекты упрощали разработку.

2. В приложении был предотвращен переход на неподконтрольные нам веб-ресурсы через встроенный механизм WebView.

Разработка приложения

Разработанный проект является клиентской программой, рассчитанной на использование на платформах Android и iOS. Разработка велась на мобильной кроссплатформенной фреймворке Flutter с использованием преимущественно языка Dart. Этот выбор был обусловлен по нескольким критериям:

1. Возможность использовать один и тот же UI одновременно на двух мобильных платформах (Android и iOS), что позволит сохранить схожий дизайн в обоих случаях.

2. Снижение рисков допущения ошибок в бизнес-логике, так как обе версии мобильного приложения будут иметь одну основу.

3. Перспективная возможность создания desktop-версии программы.

Для реализации механизмов работы с сетевыми запросами был выбран REST, а для его реализации в приложении выбор пал на http-клиент Dio, которые целиком удовлетворяет запросам приложения: возможность вставки заголовков и указания типов контента, поддержка proxy, удобная обработка ошибок и так далее [3].

Помимо взаимодействия с серверной частью, приложение не могло существовать и без локального хранилища данных. При его создании было решено обратиться к концепции базы данных NoSQL формата. Идеальным вариантом стал Hive. Hive — невероятно быстрая, не требующая много ресурсов и простая в реализации база данных, которую мы используем для хранения данных об учетной записи пользователя и сохраненной информации об охотнике, связанной с картой и историей обращений к чат-боту.

Для сокрытия в приложении важных фрагментов исходного кода, например, константные значения публичного токена карты, применялась библиотека flutter_dotenv, позволяющая повысить безопасность приложения.

Заключение. Таким образом, разработанная программа позволит не только избежать частых нарушений законодательства РФ среди охотников, но и позволит облегчить и обезопасить процесс получения и подачи сведений о местоположении и добыче охотничьих ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. Единая защищенная мобильная платформа: Общее описание программного обеспечения. — Текст : электронный // https://platforms.su : портал выбора технологий и поставщиков. — 2016. — URL: https:// platforms.su/platform/2272 (дата обращения: 09.05.2022).
2. Методический документ «Методика оценки угроз безопасности информации. — Текст : электронный // https://fstec.ru : портал федеральной службы по техническому и экспортному контролю. — 2022. — URL: https://fstec.ru/en/component/attachments/download/2919 (дата обращения: 12.05.2022).
3. A powerful Http client for Dart. — 2022. — URL: https://pub.dev/packages/dio (date of the application: 13.05.2022). — Текст : электронный.

Д. Л. Егоров, Н. А. Никишов, Д. И. Токарев, Т. И. Паюсова

Тюменский государственный университет, г. Тюмень

УДК 004.056

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ NFT ДЛЯ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Аннотация. *В статье обсуждаются возможности NFT (non-fungible token, невзаимозаменяемый токен) для защиты интеллектуальной собственности. Представлена реализация NFT с использованием блокчейн-технологий и смарт-контрактов.*

Ключевые слова: *блокчейн, NFT, Non-fungible Token, невзаимозаменяемый токен, смарт-конракт, технология, интеллектуальная собственность, авторское право, Solana.*

Введение. На сегодняшний день проблема защиты интеллектуальной собственности представляется особенно актуальной. «Пиратство» и нарушение авторских прав приводит к демотивации людей, снижению патентования, «утечке мозгов», также происходит