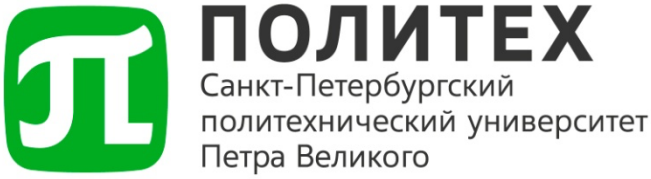
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»
ВШ программной инженерии



КУРСОВАЯ РАБОТА

«Безопасное хранение персональных данных на устройствах IOS»

по дисциплине «Защита информации»

Выполнил
Студент 3530202/80202 группы А.М. Потапова

Руководитель Б.М. Медведев

Санкт-Петербург
2023 г.

СОДЕРЖАНИЕ

Обзор литературы

Каждый год значимость безопасности хранения пользовательских данных в мобильных приложениях возрастает. С ростом осведомленности пользователей об угрозах утечек конфиденциальной информации разработчики приложений должны обеспечивать безопасность хранения данных, используя различные методы защиты.

Современные устройства IOS содержат огромное количество конфиденциальной информации, такой как контакты, сообщения, фотографии, видео, финансовые данные, личные записи и многое другое. К сожалению, это также делает их целью для злоумышленников и киберпреступников, которые могут использовать эту информацию для кражи личных данных, финансовых мошенничеств, взлома устройства и других угроз.

Несмотря на то, что IOS считается одной из самых безопасных платформ для мобильных устройств, она не является абсолютно защищенной от всех видов угроз безопасности. Некоторые из уязвимостей могут быть вызваны некорректной настройкой устройства, ошибками в приложениях, несанкционированным доступом к устройству и другими причинами. Таким образом, приоритетной задачей разработчиков приложений становится обеспечение безопасности хранимых данных.

Виды персональных данных

Для начала, рассмотрим основные виды персональных данных пользователей iOS девайсов:

- Контактная информация: номера телефонов, адреса электронной почты, адреса проживания и рабочие адреса.
- Финансовые данные: информация о банковских счетах, кредитных картах и других финансовых средствах.

- Информация об авторизации: учетные записи, пароли, ключи и сертификаты.
- Личные фотографии и видео.
- Данные о местоположении устройства в определенный момент времени.
- История браузера, посещенные сайты и другая информация о сетевой активности устройства.
- Данные о здоровье и фитнесе, включая данные о сердцебиении, соне, физической активности и др.

Кража таких данных может привести к серьезным последствиям, таким как потеря денежных средств, утечка конфиденциальной информации и т.п.

Оценка рисков реализации угроз

Рассмотрим наиболее распространенные методы кражи перечисленных выше пользовательских данных с оценкой уровня опасности:

- Утеря или кража устройства – *высокий уровень опасности*. Если устройство IOS потеряно или украдено, злоумышленник сможет без особых усилий получить доступ к конфиденциальной информации владельца мобильного устройства.
- Вредоносное ПО – *высокий уровень опасности*. Вредоносное ПО на устройствах IOS может быть установлено через приложения из App Store, веб-сайты или электронную почту. Вредоносное ПО может использоваться для сбора конфиденциальной информации, такой как логины и пароли, и для управления устройством без ведома пользователя.
- Фишинг – *средний уровень опасности*. Фишинг – это мошенническая попытка получить личную информацию, такую как логины и пароли, путем подделки электронных писем, текстовых сообщений и веб-страниц. Несмотря на то, что устройства IOS имеют высокий уровень защиты от

фишинга, пользователи все еще могут быть подвержены этой угрозе, если они не будут осторожны при открытии электронных сообщений или переходе на подозрительные веб-сайты.

- Несанкционированный доступ к данным приложений – *средний уровень опасности*. Если приложение не было разработано с учетом безопасности данных, злоумышленник может получить доступ к конфиденциальной информации, которая хранится в приложении.
- Сетевые атаки – *низкий уровень опасности*. Сетевые атаки могут использоваться для получения доступа к конфиденциальной информации, которая передается между устройством и сервером. Однако, с учетом высокого уровня защиты в IOS, эта угроза не является частой, и пользователи обычно не должны беспокоиться об этом.

Способы устранения угроз

Для устранения перечисленных рисков пользователю можно применять следующие способы:

- Использование паролей и Touch/Face ID для защиты устройства. Это поможет предотвратить несанкционированный доступ к устройству и сохранить персональные данные.
- Использование защищенных соединений. Приложения должны использовать защищенные протоколы, такие как HTTPS, для передачи данных между устройством и сервером.
- Ограничение доступа к персональным данным. Приложения должны иметь минимальный доступ к персональным данным и запросить разрешение у пользователя на доступ к ним.
- Регулярное обновление операционной системы и приложений. Это поможет обеспечить устранение уязвимостей и исправление ошибок в безопасности данных.

- Резервное копирование данных. Пользователи должны регулярно резервировать свои данные, чтобы в случае потери или кражи устройства сохранить доступ к своим персональным данным.
- Тщательный выбор приложений. Пользователи должны скачивать приложения только из официальных источников, чтобы избежать установки вредоносных программ.
- Регулярное удаление ненужных данных. Пользователи должны удалять ненужные данные, такие как старые сообщения или фотографии, чтобы уменьшить риск кражи и потери данных в случае утери или кражи устройства.
- Использование VPN для защиты соединения в общественных сетях Wi-Fi. VPN шифрует соединение и помогает обезопасить передачу данных в общественных сетях Wi-Fi.

Разработчику, в свою очередь, приходится отталкиваться от формата разрабатываемого ПО и используемых технологий. Но, для общих случаев предлагаются следующие решения:

- Хранение паролей и других конфиденциальных данных в безопасном виде с использованием шифрования данных.
- Использование защищенного соединения для передачи данных между приложением и сервером.
- Использование технологии обратимого шифрования для защиты данных в случае утечки устройства.
- Ограничение доступа к базе данных только авторизованным пользователям и разрешение на доступ только необходимой информации.
- Использование механизмов аутентификации для защиты данных от несанкционированного доступа.
- Ограничение доступа к приложению только через защищенный пароль или Touch ID/Face ID.
- Хранение критических данных на сервере в зашифрованном виде.

- Ограничение возможности копирования и экспорта данных из приложения.
- Регулярное обновление приложения для устранения обнаруженных уязвимостей и повышения уровня безопасности.
- Проведение аудита безопасности приложения с целью выявления возможных уязвимостей и проблем в защите данных.

В моем случае приложение использует следующие пользовательские данные: фото/видео контент и текстовые записи. В качестве паттерна проектирования используется MVVM. А в качестве базы данных – фреймворк CoreData. Сторонние сервисы, предоставляющие серверы для хранения данных пользователей было решено не привлекать, с целью устранения рисков кражи и минимизации финансовых затрат на разработку приложения.

Таким образом, защита данных в моем ПО сводится к следующим методам:

- Шифрование данных. Все пользовательские данные, такие как фото/видео и текстовые записи, зашифрованы, используя алгоритм шифрования AES. Это позволит обезопасить данные в случае несанкционированного доступа к устройству.
- Резервное копирование данных. Резервное копирование пользовательских данных на облачный сервис iCloud позволит сохранить копию данных в случае потери устройства или повреждения файлов. iCloud использует сильное шифрование для защиты данных в пути и в покое. Данные хранятся в зашифрованном виде на серверах Apple, а доступ к ним предоставляется только после прохождения проверки подлинности.
- Ограничение доступа к данным. Ограничение доступа к пользовательским данным можно осуществить через различные механизмы, такие как пароли, PIN-коды, Touch ID и Face ID. Несанкционированный

доступ к данным можно также предотвратить путем ограничения доступа к файловой системе iOS и использования системного шифрования данных.

- Обновление приложения. Важно периодически обновлять приложение, чтобы закрыть обнаруженные уязвимости в безопасности. Обновления могут включать исправления ошибок, а также улучшения безопасности.

В данной работе я рассмотрю перечисленные методы и интегрирую их в свое приложение.

Цели работы и решаемые задачи

Цель: обеспечить надежное хранение пользовательских данных в приложении, предназначенном для записи воспоминаний и хранения фото/видео контента, используя механизмы шифрования данных и резервное копирование.

Задачи:

- Реализовать безопасный функционал сохранения и загрузки данных в локальную базу данных фреймворка CoreData используя паттерн MVVM.
- Разработать механизм шифрования для защиты пользовательских данных.
- Реализовать функционал создания резервных копий данных и их восстановления из облачного хранилища iCloud для предотвращения потери данных в случае сбоя приложения или устройства.
- Протестировать приложение на наличие уязвимостей и ошибок в системе безопасности.
- Получить у пользователя доступ необходимым персональным данным.
- Реализовать механизм обновления приложения с целью исправления обнаруженных уязвимостей и ошибок в системе безопасности.