УДК 004.056

РАЗРАБОТКА И ВНЕДРЕНИЕ РЕКОМЕНДАЦИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ REACT NATIVE ПРИЛОЖЕНИЯ

Ли Г. (Университет ИТМО)
Научный руководитель – аспирант Шнайдер П.А.
(Университет ИТМО)

Введение. При разработке мобильных приложений одной из важнейших задач является вопрос безопасности. С самой первой стадии разработки необходимо обеспечить безопасность пользовательских данных [1].

В данном докладе формулируются рекомендации, рассматриваются инструменты, методы и технологии по обеспечению информационной безопасности React-Native приложения. Более того, на практике будет рассмотрен процесс внедрения разработанных рекомендаций в мобильное приложение.

Основная часть. React Native мобильное приложение, как и другое программное обеспечение, обладает уязвимостями. К основным вопросам безопасности React-Native мобильных приложений относятся:

- Хранение конфиденциальной информации,
- Выбор локального хранилища для хранения данных,
- Глубинное связывание,
- Специфические проблемы безопасности для IOS, Android,
- Методы аутентификации,
- Пиннинг SSL сертификатов [2].

Подробнее рассмотрим данные уязвимости, а также - какие технологии, инструменты, подходы используются для их устранения.

React Native не позволяет легко и безопасно хранить конфиденциальную информацию на устройстве. Это связано с тем, что в React Native нет модуля, реализующего безопасное хранение конфиденциальной информации. Поэтому все конфиденциальные данные, хранящиеся в устройстве, должны храниться с помощью библиотек, например, iOS Keychain или Android Secure shared storage.

Мобильные приложения обладают уникальной уязвимостью – глубинным связыванием, которая заключается в отправке данных в приложение из другого источника. Информация, переданная с помощью данной технологии, может быть прочитана злоумышленниками, поэтому секретная информация не должна быть передана с помощь данной технологии [3].

Еще одной уязвимостью мобильных приложений является использование конечных точек https. Используя https, клиент доверится серверу только тогда, когда он предоставит действительный сертификат, который подписан доверенным центром сертификации. Злоумышленник может установить на пользовательское устройство вредоносный сертификат корневого центра сертификации, что заставит клиента доверять сертификатам, которые подписаны злоумышленником. Для того чтобы избежать данной атаки используется технология SSL pinning, которая подразумевает встраивание списка доверенных сертификатов к клиенту во время разработки, то есть самоподписанные сертификаты приняты не будут [4].

Для верной авторизации пользователя важно применять многофакторную авторизацию. К методам дополнительной авторизации относят: OTP (one time password), подтверждение по электронной почте, ЭЦП (электронно-цифровая подпись), ответы на дополнительные секретные вопросы, аппаратный токен ключ, биометрическая авторизация [5-6].

Таким образом, были сформулированы следующие рекомендации для обеспечения информационной безопасности мобильного приложения React Native:

- Использование многофакторной авторизации,

- Использование пиннинга SSL сертификата,
- Выбор безопасного хранилища данных для конфиденциальной информации,
- Исключение использования глубинного связывания для передачи конфиденциальной информации.

Выводы. В докладе были предложены рекомендации для обеспечения информационной безопасности мобильного приложения React Native, также были рассмотрены инструменты и методы, которые позволяют применить данные рекомендации. На практике будет выполнено внедрение данных рекомендаций в мобильное приложение React Native.

Список использованных источников:

1. Как обеспечить безопасность приложения [Электронный ресурс]. - 2020. - URL: https://tproger.ru/articles/application-security/.
2. Vachhani H. Security Aspects to consider for a React Native Application [Электронный ресурс]. – 2022. – URL: https://medium.com/simform-engineering/security-aspects-to-consider-for-a-react-native-application-95556f0e4244.
3. Juhola J. Security Testing Process for React Native Applications [Электронный ресурс]. – 2022. URL: https://trepo.tuni.fi/bitstream/handle/10024/138923/JuholaJali.pdf?sequence=2.
4. Security [Электронный ресурс]. – 2023. - URL: https://reactnative.dev/docs/security.
5. Mohan S., Harun N. Jeev Time: Secure Authentication Using Integrated Face Recognition in Social Media Applications // Journal of Soft Computing and Data Mining. – 2022. – Vol. 3 No.2. – С. 19.
6. Султанова Б.К., Щербов А.С. Использование дополнительных методов авторизации пользователей // Scientific Journal of Astana. – 2020. – С. 93.