УДК 004.056

АНАЛИЗ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ШИФРОВАНИЯ ДАННЫХ В МОБИЛЬНЫХ СИСТЕМАХ

Саросек М.М.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Воробей А.В. – магистр технических наук, ассистент кафедры ИПиЭ

Аннотация. В статье рассматриваются современные методы шифрования данных для *Android*, включая *File-Based Encryption* (*FBE*) для защиты файлов на уровне файловой системы, использование *Android Keystore* для безопасного хранения и управления ключами, а также механизмы передачи данных по сети с использованием *TLS/SSL* протоколов.

Ключевые слова: *Android*, *File-Based Encryption*, *TLS* протокол, *SSL* протокол

Введение. С развитием мобильных технологий и расширением функционала мобильных приложений, обеспечение безопасности данных на устройствах *Android* становится фундаментальным аспектом разработки. Системы *Android* предоставляют широкий спектр инструментов и технологий для шифрования данных, обеспечивая конфиденциальность и целостность информации, сохраненной на устройствах.

В данном контексте становится важным исследование и анализ методов шифрования, применяемых в мобильных системах *Android*. Эта работа посвящена подробному рассмотрению современных технологий шифрования.

Основная часть. Анализируя темы, такие как *File-Based Encryption* (*FBE*), *Android Keystore*, применение *TLS/SSL* протоколов для защиты передаваемых данных, мы стремимся предоставить полное понимание методов, которые обеспечивают надежную защиту конфиденциальности пользовательской информации в мобильных приложениях на платформе *Android*.

File-Based Encryption (*FBE*) представляет собой метод шифрования данных на уровне файловой системы в операционной системе *Android*. Она была введена для обеспечения безопасности данных пользователя в ситуациях, когда устройство находится в заблокированном состоянии. Основная идея FBE заключается в том, что каждый файл на устройстве шифруется отдельным ключом, и доступ к файлу разрешается только после успешного ввода ключа разблокировки [1].

Преимуществами *File-Based Encryption* являются:

1. Изоляция файлов: файл на устройстве шифруется независимо от других файлов. Это обеспечивает высокий уровень изоляции данных и предотвращает распространение конфиденциальной информации, даже если один из файлов был скомпрометирован.
2. Безопасность в состоянии блокировки: *FBE* обеспечивает защиту данных даже в случае утери или кражи устройства. Если злоумышленник получит физический доступ к файлам, они останутся зашифрованными, что снижает риск утечки конфиденциальной информации.
3. Прозрачность для пользователя: пользователи могут управлять своими данными без необходимости беспокоиться о шифровании. Ключи автоматически разблокируются при вводе пользовательского *PIN*-кода или использовании других методов разблокировки.

TLS/SSL представляет собой протоколы шифрования, применяемые для обеспечения безопасного обмена данными между клиентом и сервером через сеть, такую как интернет. Они широко используются для защиты конфиденциальных данных, таких как логины, пароли, и другая чувствительная информация [2].

Преимуществами *TLS/SSL* можно назвать следующие:

1. Шифрование данных: одним из основных преимуществ *TLS/SSL* является шифрование данных, передаваемых между клиентом и сервером. Это обеспечивает конфиденциальность информации и предотвращает ее перехват и прочтение злоумышленниками.

2. Идентификация сервера: *TLS/SSL* обеспечивает аутентификацию сервера, что гарантирует, что клиент подключается к правильному серверу, а не к поддельному. Это предотвращает атаки «*Man-in-the-Middle*».

3. Целостность данных: протоколы *TLS/SSL* гарантируют целостность передаваемых данных. Это означает, что данные не могут быть изменены или повреждены в процессе передачи [3].

Заключение. Совместное использование *File-Based Encryption* и *TLS/SSL* протоколов в мобильных приложениях создает полный уровень защиты, гарантируя, что как данные на устройстве, так и данные, передаваемые по сети, остаются защищенными от несанкционированного доступа.

В современном цифровом мире, где конфиденциальность играет важную роль, эти технологии становятся неотъемлемой частью безопасной разработки программного обеспечения для мобильных устройств.

Список литературы

1. Образовательный онлайн-форум «Хабр» [Электронный ресурс] / Образовательный онлайн-форум «Хабр» – Москва, 2017. – Режим доступа: https://habr.com/ru/articles/340146/ – Дата доступа: 19.01.2024

2. Образовательный онлайн-форум «Артис Медиа» [Электронный ресурс] / Образовательный онлайн-форум «Артис Медиа» – Москва, 2016. – Режим доступа: https://habr.com/ru/articles/340146/ – Дата доступа: 19.01.2024

3. Образовательный онлайн-форум «Хабр» [Электронный ресурс] / Образовательный онлайн-форум «Хабр» – Москва, 2012. – Режим доступа: https://habr.com/ru/articles/143259/ – Дата доступа: 19.01.2024

UDC 004.056

ANALYSIS OF MODERN DATA ENCRYPTION TECHNOLOGIES IN MOBILE SYSTEMS

Sarosek M.M.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vorobey A.V. – master of technical sciences, assistant of the department of EPE

Annotation. The article discusses modern data encryption techniques in Android, including File-Based Encryption for protecting files at the file system level, using Android Keystore for securely storing and managing keys, and mechanisms for transferring data over the network using TLS/SSL protocols.

Keywords: Android, File-Based Encryption , TLS protocol, SSL protocol