КИБЕРБЕЗОПАСНОСТЬ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

Тилебалдыева Буайша Шералиевна
Студент Ошский государственный университет Институт Математики, физики, техники и информационных технологий

Аннотация: *Современные мобильные приложения прочно интегрированы в нашу повседневную жизнь, храня огромное количество персональных данных. Однако, с ростом популярности мобильных устройств, увеличивается и количество кибератак, направленных на них. Данная статья посвящена исследованию актуальных проблем кибербезопасности в мобильных приложениях. В работе рассматриваются основные виды уязвимостей, методы их обнаружения и предотвращения, а также анализируются современные подходы к обеспечению безопасности мобильных приложений.*

Ключевые слова: *Кибербезопасность, мобильные приложения, уязвимости, безопасность данных, разработка мобильных приложений, DevSecOps*

Введение: Мобильные приложения стали неотъемлемой частью нашей жизни, предоставляя широкий спектр услуг от коммуникации до финансовых операций. Однако, вместе с удобством, мобильные приложения несут в себе и определенные риски, связанные с кибербезопасностью. Уязвимости в мобильных приложениях могут привести к утечке конфиденциальных данных, финансовым потерям, а также к нарушению работы устройств. От банковских операций до социальных сетей, от онлайн-шопинга до систем здравоохранения – практически все сферы нашей жизни так или иначе связаны с мобильными приложениями. Однако, с ростом популярности мобильных устройств, увеличивается и количество кибератак, направленных на них.

Кибербезопасность мобильных приложений – это комплекс мер, направленных на защиту мобильных устройств и приложений от несанкционированного доступа, утечки данных, вредоносных программ и других киберугроз. Обеспечение безопасности мобильных приложений – это сложная задача, требующая комплексного подхода, включающего в себя как технические, так и организационные меры.

Структура работы:

Во введении обосновывается актуальность темы исследования и формулируются цели и задачи работы. В следующем разделе рассматриваются основные виды уязвимостей в мобильных приложениях. Затем анализируются методы обнаружения уязвимостей и современные подходы к обеспечению безопасности. В заключении подводятся итоги исследования и формулируются основные выводы.

Данная работа будет полезна для разработчиков мобильных приложений, специалистов по информационной безопасности, а также для всех, кто интересуется вопросами кибербезопасности в современном цифровом мире.

Актуальность проблемы обусловлена следующими факторами:

Уязвимости мобильных платформ: Операционные системы мобильных устройств, такие как iOS и Android, не лишены уязвимостей, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к данным устройства.

Уязвимости в коде приложений: Ошибки в коде мобильных приложений могут привести к утечке конфиденциальных данных, удаленному управлению устройством и другим негативным последствиям.

Социальная инженерия: Мошеннические действия, направленные на обман пользователей с целью получения конфиденциальной информации, остаются одной из самых распространенных угроз.

*Рост числа мобильных устройств и приложений***:** Постоянный рост числа мобильных устройств и приложений создает благоприятную среду для киберпреступников.

Основные виды уязвимостей в мобильных приложениях

Мобильные приложения, несомненно, упростили нашу жизнь, но одновременно стали лакомым кусочком для злоумышленников. Уязвимости в мобильных приложениях могут привести к утечке конфиденциальных данных, финансовым потерям, а также к нарушению работы устройства. Рассмотрим наиболее распространенные виды таких уязвимостей.

Уязвимости на уровне кода

SQL-инъекции: Вводятся вредоносные SQL-команды в поля ввода приложения, что позволяет злоумышленнику получить доступ к базе данных.

Межсайтовый скриптинг (XSS): Внедрение вредоносного кода в веб-страницы приложения, который выполняется на стороне клиента, позволяя злоумышленнику похищать куки, перенаправлять пользователей на фишинговые сайты и т.д.

Уязвимости к инъекциям: Внедрение произвольного кода в приложение, позволяющее злоумышленнику выполнять произвольные команды на устройстве пользователя.

Небезопасное управление сессиями: Отсутствие или неправильная реализация механизмов управления сессиями, что может привести к угону сессии и несанкционированному доступу к учетной записи пользователя.

Небезопасное хранение данных: Хранение чувствительных данных (пароли, платежная информация) в незашифрованном виде или в легкодоступных местах.

Уязвимости на уровне платформы

Ошибки в использовании API: Некорректное использование API операционной системы может привести к уязвимостям, связанным с доступом к файловой системе, камере, микрофону и другим ресурсам устройства.

Уязвимости в библиотеках: Использование устаревших или небезопасных библиотек может привести к эксплуатации известных уязвимостей.

Уязвимости на уровне сети

Отсутствие или неправильная реализация SSL/TLS: Отсутствие шифрования данных при передаче по сети может привести к перехвату данных злоумышленниками.

Незащищенные каналы связи: Использование незащищенных каналов связи для передачи конфиденциальной информации.

Уязвимости к перехвату данных: Отсутствие аутентификации и целостности данных при передаче по сети.

Социальная инженерия

Фишинг: Мошеннические действия, направленные на обман пользователей с целью получения конфиденциальной информации.

Злоупотребление доверием: Использование социальных связей для получения доступа к устройствам или информации.

Другие виды уязвимостей

Обратный инжиниринг: Разборка приложения для изучения его внутреннего устройства и поиска уязвимостей.

Side-channel атаки: Получение конфиденциальной информации путем анализа побочных каналов (например, времени выполнения операций).

Хранение данных

Шифрование: Шифруйте все чувствительные данные, как во время хранения, так и при передаче.

Безопасное хранилище: Используйте защищенные хранилища для хранения ключей шифрования и другой конфиденциальной информации.

Минимизация данных: Храните только необходимые данные и удаляйте их после того, как они больше не нужны.

Заключение: Данная статья является базовым каркасом для более глубокого исследования. Для написания полноценной научной статьи необходимо провести детальный анализ существующих исследований, собрать статистические данные, провести собственные эксперименты и сформулировать оригинальные выводы.

СПИСОК ЛИТЕРАТУРЫ И ИСТОЧНИКОВ:

1. Михайлов Д.М., Жуков И.Ю «Защита мобильных телефонов от атак»
2. David Kleidermacher "Android Security and Privacy: An Engineering Approach"

3. https://udcs.ru/company/news/zachem-nuzhna-informatsionnaya-bezopasnost
4. https://www.ptsecurity.com/ru-ru/research/analytics/kak-dejstvuyut-apt-gruppirovki-v-yugo-vostochnoj-azii/
5. https://cqr.company/ru/web-vulnerabilities/business-logic-flow-2