МЕТОДЫ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ В УСЛОВИЯХ МИНИМИЗАЦИИ РЕСУРСОВ МОБИЛЬНОГО УСТРОЙСТВА

Аннотация: Мобильные устройства активно используются для хранения и передачи личных данных, что создает угрозу для конфиденциальности пользователей. Однако, с учетом ограниченных вычислительных и энергетических ресурсов мобильных устройств, задачи по обеспечению безопасности требуют специальных подходов. В данной статье рассматриваются методы защиты пользовательских данных, такие как оптимизированное шифрование и оптимизация протоколов безопасности, направленные на минимизацию нагрузки на процессор, память и батарею мобильного устройства.

Ключевые слова: безопасность данных, мобильные устройства, шифрование, легковесные протоколы, минимизация ресурсов, мобильная безопасность.

Автор: курсант Академии МВД Республики Узбекистан, 308-группа Эргашев Мирислом Умид ўғли

Введение: С увеличением использования мобильных устройств для передачи и хранения конфиденциальных данных возросла потребность в эффективных методах их защиты. Тем не менее, ограниченные ресурсы мобильных устройств создают вызовы для реализации методов защиты, особенно таких, как шифрование и сложные протоколы безопасности. Данная статья фокусируется на методах, позволяющих обеспечить безопасность данных без значительного влияния на производительность и энергоэффективность устройства.

1. Основные проблемы защиты данных в мобильных устройствах

Ограниченные ресурсы мобильных устройств

Мобильные устройства ограничены в вычислительной мощности, объеме памяти и емкости батареи, что усложняет использование стандартных методов защиты данных, применяемых для десктопных и серверных систем.

Риски безопасности мобильных данных

Мобильные устройства подвержены множеству угроз, включая кражу данных, перехват сетевого трафика и несанкционированный доступ. Устройства могут подвергаться атакам при подключении к открытым Wi-Fi сетям, при установке вредоносного ПО или при использовании устаревших версий ОС.

2. Методы защиты данных с минимальным использованием ресурсов

Для защиты пользовательских данных на мобильных устройствах применяются различные методы, направленные на минимизацию нагрузки на процессор и оперативную память.

Легковесное шифрование данны

Симметричное шифрование

Симметричное шифрование, использующее один и тот же ключ для шифрования и дешифрования данных, потребляет меньше вычислительных ресурсов по сравнению с асимметричными методами. **Алгоритмы, такие как AES (Advanced Encryption Standard)** с уменьшенной длиной ключа, позволяют достичь высокой скорости шифрования при низком уровне энергопотребления.

Легковесные криптографические алгоритмы

Существует ряд криптографических алгоритмов, специально адаптированных для устройств с ограниченными ресурсами. Например, алгоритмы **LEA (Lightweight Encryption Algorithm)** и **SPECK/SIMON**, разработанные для мобильных устройств, требуют минимальных вычислительных мощностей и энергозатрат, обеспечивая при этом достаточный уровень безопасности для большинства мобильных приложений.

Адаптивное шифрование

Адаптивное шифрование предполагает выбор уровня шифрования в зависимости от контекста использования данных. Например, для передачи менее критичных данных можно использовать алгоритмы с более короткими ключами или упрощенные методы шифрования, а для критичных данных — более сильные и надежные методы.

2.2 Оптимизация протоколов безопасности для мобильной среды

Оптимизация SSL/TLS

Протоколы SSL и TLS широко используются для защиты передаваемых данных, однако их реализация может быть ресурсоемкой. Для мобильной среды возможны следующие оптимизации:

- **Снижение количества рукопожатий**: сокращение числа рукопожатий при использовании SSL/TLS позволяет уменьшить задержку и снизить нагрузку на процессор.
- **Сессии без повторного шифрования**: повторное использование установленных сеансов без нового ключа шифрования снижает энергопотребление и ускоряет передачу данных.

DTLS (Datagram Transport Layer Security)

Протокол DTLS — версия TLS для передачи данных в режиме UDP — обеспечивает низкую задержку и подходит для использования в мобильных сетях, где стабильность соединения может быть ограничена. Он используется, например, в приложениях для видеозвонков, где важно поддерживать баланс между безопасностью и скоростью передачи данных.

Легковесные протоколы для Интернета вещей (IoT)

Для защиты данных в условиях ограниченных ресурсов все большее внимание уделяется легковесным протоколам безопасности, таким как **CoAP (Constrained**

Application Protocol), разработанным специально для устройств с малой вычислительной мощностью и ограниченным объемом памяти.

2.3 Хранение данных в мобильной среде

Шифрование хранилищ

Защищенное шифрование хранилища данных на мобильных устройствах предполагает шифрование данных на уровне файловой системы. На устройствах Android и iOS существуют встроенные механизмы для шифрования хранилища данных, что минимизирует нагрузку на ресурсы устройства.

Защищенные контейнеры для данных

Приложения могут использовать **защищенные контейнеры**, которые изолируют критичные данные и используют сильные механизмы шифрования. Контейнеры защищены отдельным PIN-кодом или биометрическими данными, что предотвращает доступ злоумышленников к данным в случае физического доступа к устройству.

Облачное хранилище с локальным шифрованием

Для оптимизации локального хранения данных используются гибридные модели, при которых конфиденциальные данные шифруются на устройстве и отправляются в облако. Это снижает нагрузку на локальное хранилище, сохраняя при этом высокий уровень защиты данных.

3. Адаптивные подходы к обеспечению безопасности

Управление безопасностью на основе контекста: Контекстные системы безопасности применяют адаптивные методы защиты, изменяя уровень безопасности в зависимости от текущего состояния устройства. Например, при низком уровне заряда батареи можно снизить интенсивность шифрования или временно ограничить использование ресурсоемких протоколов.

Оптимизация использования биометрии

Биометрическая аутентификация (отпечаток пальца, Face ID) позволяет защитить данные без нагрузки на вычислительные ресурсы устройства. Биометрические методы аутентификации предлагают высокий уровень безопасности и удобство для пользователя, так как не требуют постоянного ввода паролей.

Двухфакторная аутентификация

Методы двухфакторной аутентификации (например, код через SMS или одноразовый пароль) повышают уровень безопасности, сохраняя нагрузку на процессор и память устройства на минимальном уровне.

4. Вызовы и перспективы обеспечения безопасности на мобильных устройствах

Вызовы минимизации нагрузки: Основной вызов для мобильной безопасности — это минимизация нагрузки на процессор, память и батарею устройства при сохранении высокого уровня защиты данных. Обфускация данных и уменьшение времени сеанса требуют эффективных алгоритмов и протоколов, способных поддерживать баланс между безопасностью и производительностью.

Перспективы развития легковесных алгоритмов и протоколов

Современные исследования в области легковесных криптографических методов направлены на разработку алгоритмов с минимальными требованиями к ресурсам устройства. С появлением 5G и развитием IoT также будут расширяться возможности для оптимизации протоколов передачи данных.

Заключение: Обеспечение безопасности данных на мобильных устройствах требует разработки методов, способных защитить конфиденциальность пользователей с минимальными требованиями к ресурсам. В статье рассмотрены методы защиты данных, такие как легковесное шифрование, оптимизация протоколов безопасности и адаптивные контекстные подходы. В будущем важно продолжать исследования в области оптимизированных методов защиты для

поддержания высокого уровня безопасности данных при минимальном воздействии на производительность устройства.

Источники:

1. Beaulieu, R., Shors, D., Smith, J., et al. (2015). The SIMON and SPECK lightweight block ciphers. Retrieved from: https://www.researchgate.net/publication/283470225_The_SIMON_and_SPECK_lightweight_block_ciphers

2. Hong, S., Kim, J., Ko, Y., et al. (2013). LEA: A 128-bit block cipher for fast encryption on common processors. Retrieved from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6806263/

3. Bansod, G., Jadhav, S., & Dole, R. (2015). Design and implementation of a lightweight block cipher for resource-constrained devices. Retrieved from: https://arxiv.org/abs/1704.08688

4. Rescorla, E. (2012). Datagram Transport Layer Security Version 1.2 (DTLS). Retrieved from: https://en.wikipedia.org/wiki/Datagram_Transport_Layer_Security

5. Tsoutsos, N. G., Maniatakos, M., et al. (2018). eeDTLS: Energy-efficient datagram transport layer security for the Internet of Things. Retrieved from: https://dspace.mit.edu/bitstream/handle/1721.1/122466/eeDTLS__GlobeCom_%281%29.pdf%3Bsequence%3D1

6. Digital Guardian. (n.d.). What is Context-Aware Security? Retrieved from: https://www.digitalguardian.com/resources/knowledge-base/context-aware-security

7. Pomerium. (2022). Context-Aware Authentication: Meaning, Tools, and Examples. Retrieved from: https://www.pomerium.com/blog/context-aware-authentication-meaning-tools-examples

8. Newman, L. H. (2020). Google's Advanced Protection Program Expands to Android. Wired. Retrieved from: https://www.wired.com/story/google-advanced-protection-vulnerable-users-lockdown-android-16