РЕЦЕНЗІЯ на статтю

«MOBILE APPLICATION SECURITY IN MODERN TECHNOLOGIES: PROTOCOLS AND ALGORITHMS»

Актуальність та новизна. Тема дослідження актуальна. Мобільні застосунки сьогодні працюють з фінансовими, медичними і корпоративними даними і вибір правильного стеку безпеки — не теоретичне питання. Це щоденна інженерна задача.

Більшість публікацій розглядають TLS, OAuth, JWT і FIDO2 окремо. Автор показує їх як єдину архітектуру. Це відрізняє роботу від звичайних оглядів.

Технічна складова. AES-256-GCM для транспортного рівня — обґрунтований вибір. Алгоритм має апаратну підтримку через ARM Crypto Extensions і використовується в TLS 1.3. На пристроях без цього прискорення ChaCha20-Poly1305 показує кращі результати. Висновок автора тут точний.

ECDSA проти RSA: при 256-бітному ключі ECDSA дає рівень безпеки, порівнянний з RSA-3072. Підпис менший, обчислювальне навантаження нижче. Для пристроїв з батарейним живленням це має значення.

PKCE для OAuth 2.0 описаний відповідно до RFC 7636. Зауваження про JWT точне: більшість реальних інцидентів — це не вразливість протоколу, а помилки реалізації на сервері. Прийняття алгоритму «None» — класичний приклад.

FIDO2: приватний ключ зберігається в Secure Enclave на iOS або TEE на Android. Він не покидає пристрій. Навіть при скомпрометованій ОС. Це суттєва перевага над будь-якими схемами з паролями.

Розділ про поточні виклики охоплює п'ять класів загроз, класифікація яких відповідає OWASP Mobile Security Testing Guide.

Позитивна сторона. Протоколи показані як система. Рисунок 1 демонструє їх взаємодію на чотирьох рівнях — це дає читачу цілісну картину, а не набір визначень.

Порівняння FIDO2 з SMS і OTP — технічно чесне. FIDO2 не передає секрет по мережі. Це усуває SIM-swap і MITM одразу. Класичний двофактор від таких атак не захищає.

Розділ про загрози структурований і відповідає OWASP Mobile Security Testing Guide. Фрагментація платформ як окремий клас ризику — деталь, яку часто ігнорують.

Зауваження та пропозиції. 1. Методи дослідження заявляють моделювання взаємодії протоколів та аналіз ефективності алгоритмів в умовах обмежених ресурсів. Результатів цього немає —ні таблиць, ні числових даних. Рекомендується або додати власні результати тестування, або привезти опис методів у відповідність до фактично виконаної роботи.

2. Статистика про понад 40% мобільних застосунків з некоректною валідацією TLS-сертифікатів наведена без посилання на первинне джерело. Вказати конкретне дослідження – питань не буде.

3. TLS 1.3 захищає канал. Але certificate pinning — прив'язка з'єднання до конкретного сертифіката або публічного ключа — у статті не розглядається. Для повноти аналізу мережевої безпеки варто або включити цей механізм, або пояснити його виключення з області дослідження.

4. Загрози локального сховища описані. Але Android Keystore і iOS Keychain — стандартні платформенні рішення для цієї проблеми — не згадані. Їх розгляд підсилив би практичну частину роботи.

Висновок. Робота має практичну цінність. Системний підхід до стеку протоколів – сильна сторона роботи. Технічні твердження щодо вибору

криптографічних алгоритмів в умовах апаратних обмежень в основному коректні.

До публікації рекомендую доопрацювати: привезти опис методів у відповідність до результатів, додати посилання на статистичні дані, розширити технічний аналіз механізмів захисту локального сховища.

Рецензент:

Люшенко Андрій Миколайович

провідний інженер-дослідник,

архітектор мобільних систем,

експерт у проектуванні масштабованих мобільних та розподілених систем,

магістр прикладної математики,

Одеса, Україна