УДК 004.056.5:004.75

УГРОЗЫ И УСИЛЕНИЕ МНОГОФАКТОРНОЙ ФУНКЦИИ ВЫВОДА КЛЮЧА (MFKDF) В ЗАДАЧАХ ВОССТАНОВЛЕНИЯ ДОСТУПА К КРИПТОКОШЕЛЬКУ В СЕТИ SOLANA

Василев В. Н.[1]
Научный руководитель – канд. техн. наук, доцент Пинкевич В. Ю.[1]
[1]Университет ИТМО
vnvassilev@niuitmo.ru

Введение

Некастодиальные криптокошельки дают пользователю полный контроль над средствами, но делают критичным сохранение приватного ключа или seed-фразы: при потере доступ восстановить невозможно, а при компрометации ключа средства могут быть похищены; при этом на практике резервные копии часто хранят небезопасно (фото, облачные заметки, пересылка), что повышает риск утечки. Для снижения этих рисков применяют пороговые схемы, социальное восстановление, мультиподпись и MPC, однако безопасность таких подходов зависит от корректной формализации. Перспективным решением является MFKDF (multi-factor key derivation function) [1], позволяющая выводить ключ из набора факторов по политике m из n, но для использования в сети Solana необходимо учитывать подписи Ed25519, модель аккаунтов и необходимость безопасной ротации ключа после восстановления; поэтому цель работы — построить модель угроз для MFKDF-восстановления доступа к Solana-кошельку [2] и на её основе предложить усиления протокола, снижающие вероятность компрометации и риск отказа в восстановлении.

Основная часть

В MFKDF восстановление доступа строится по пороговой политике m из n: при настройке генерируется случайный ключевой секрет, который делится на n долей так, чтобы для восстановления было достаточно любых m. Для каждого фактора (пароль, секрет на устройстве, биометрия, физический ключ и т. п.) из предъявляемого пользователем материала вычисляется ключ с помощью KDF/HKDF, и этим ключом шифруется соответствующая доля; в хранилище сохраняются только защищённые доли и метаданные политики (m, n, параметры KDF и привязка долей к факторам). При восстановлении пользователь предъявляет любые m доступных факторов, локально получает из них ключи, снимает защиту с m долей, объединяет их в исходный секрет и затем через «тяжёлую» KDF (например, Argon2) детерминированно получает тот же итоговый ключ или seed, что использовался ранее, возвращая контроль даже при потере до n-m факторов.

Модель угроз включает активы: (1) мастер-секрет, определяющий доступ к средствам; (2) материалы факторов и долей; (3) политику восстановления (m-of-n, перечень опекунов, параметры KDF); (4) метаданные хранения и передачи. Рассматриваются нарушители: удаленный атакующий (фишинг, утечки, перебор), вредоносное ПО на устройстве, злонамеренный/скомпрометированный опекун и коалиция опекунов. Ключевые угрозы: компрометация одного или нескольких факторов, подмена политики восстановления и параметров KDF, переносимость долей между кошельками, а также отказ в обслуживании при восстановлении (утрата долей, блокировка доступа,

вымогательство). Для Solana дополнительно значимы риски безопасной ротации ключа и корректного исполнения транзакций при восстановлении/отзыве.

С учётом предполагаемой модели угроз и требований к безопасности предлагается рассмотреть следующие направления усиления протокола для сети Solana: (1) фиксировать правила восстановления и контрольные значения для факторов в отдельном аккаунте программы, чтобы снизить риск незаметной подмены параметров на стороне клиентского приложения; (2) привязать защищённые доли и вычисления к конкретному кошельку и контексту сети (например, учитывать публичный ключ и идентификатор программы), чтобы исключить их использование в другом месте; (3) при необходимости добавить социальный фактор — участие доверенных лиц, которые предоставляют долю только по подтверждённому запросу, с возможностью последующей проверки действий; (4) предусмотреть процедуры смены и отзыва ключа: после восстановления выполнять смену ключевого материала, а при подозрении на компрометацию — быстрый отзыв, сокращающий время возможной атаки. Реализация таких мер может быть выполнена как на стороне кошелька, так и с использованием программы в сети Solana, отвечающей за хранение и проверку правил восстановления и запуск процедур смены/отзыва.

Выводы

Сформирована модель угроз для применения MFKDF в задаче восстановления доступа к Solana-кошельку и предложены усиления, повышающие устойчивость к компрометации факторов, подмене политики и угрозам доступности, а также обеспечивающие безопасную ротацию ключа после восстановления. Результаты применимы при разработке некастодиальных Solana-кошельков с многофакторным восстановлением; дальнейшая работа включает реализацию прототипа и экспериментальную проверку в сценариях потери и компрометации факторов.

Список использованных источников

1. Найр В., Сонг Д. Multi-Factor Key Derivation Function (MFKDF) for Fast, Flexible, Secure, & Practical Key Management [Электронный ресурс] arXiv.org. 2022. Дата обновления: 16.02.2023. URL:https://arxiv.org/abs/2208.05586 (дата обращения: 18.02.2026).
2. Solana Documentation. Solana Foundation. https://solana.com/docs (дата обращения: 18.02.2026).