АНАЛИЗ ВЕКТОРОВ АТАК НА СИСТЕМЫ СОЦИАЛЬНОГО ВОССТАНОВЛЕНИЯ КЛЮЧЕЙ В СИСТЕМАХ СУВЕРЕННОЙ ИДЕНТИФИКАЦИИ (SSI) И РОЛЬ ПОРОГОВОЙ КРИПТОГРАФИИ В ИХ МИТИГАЦИИ

Шушкевич Д. В.
Факультет компьютерных систем и сетей,
Кафедра программного обеспечения информационных технологий,
Белорусский Государственный Университет Информатики и Радиоэлектроники
Минск, Республика Беларусь
E-mail: dzmitry.shushkevich@gmail.com

В работе анализируются системы социального восстановления ключей (SKR) в контексте суверенной идентификации (SSI). Систематизированы векторы атак (сговор опекунов, социальная инженерия, атака Сивиллы), показывающие уязвимость наивных реализаций SKR, основанных на социальном доверии. В качестве основного механизма митигации предложено использование пороговых схем подписи (TSS). Сравнительный анализ моделей SKR на смарт-контрактах и с усилением TSS демонстрирует криптографическую устойчивость последних к атакам сговора и краже ключа. Сформулированы направления для дальнейших исследований.

Введение

Парадигма суверенной идентификации (Self-Sovereign Identity, SSI), основанная на децентрализованных идентификаторах (DID) и верифицируемых учетных данных (VC), возвращает пользователям контроль над цифровой личностью.[1, 2, 3] Однако, ключевой проблемой массового внедрения SSI остается управление криптографическими ключами: в децентрализованных системах их утеря равносильна безвозвратной потере личности и активов, что критично для нетехнических пользователей.[4, 5]

Для решения этой проблемы предложены системы социального восстановления ключей (Social Key Recovery, SKR). SKR позволяет пользователю задействовать социальную сеть «опекунов» (guardians) для восстановления доступа, [6, 7] что снижает порог входа. Однако реализации SKR на базе смарт-контрактов вводят новые уязвимости, основанные на социальном доверии.[8]

I. Основы SSI и социального восстановления

Парадигма суверенной идентификации

Концепция SSI возвращает пользователям контроль над идентификационными данными, [1, 2] опираясь на технологические столпы: децентрализованные идентификаторы (DID) – уникальные URI, разрешаемые в JSON-документ с ключами, [3, 7] и верифицируемые учетные данные (VC) – криптографически подписанный эмитентом набор утверждений.[3, 2]

Механизм социального восстановления ключей

Технически, кошелек с социальным восстановлением (SKR) функционирует как смарт-контракт, развернутый в блокчейне. В контракте запрограммированы ключевые роли: Ключ для подписи (Signing Key) для регулярных операций и Опекуны (Guardians) – набор доверенных адресов (друзья, устройства), кворум (например, 3 из 5) которых может коллективно одобрить смену ключа. При утере ключа владелец инициирует процедуру, опекуны подписывают транзакцию, и смарт-контракт заменяет старый ключ на новый, предоставленный владельцем.

II. Анализ векторов атак

Угрозы для SKR можно разделить на атаки социального и технического уровней.

Атаки на социальном уровне

- Сговор опекунов. Кворум опекунов может объединиться для замены ключа владельца на свой собственный, похитив его цифровую личность.[3, 4] Эта уязвимость усугубляется «проблемой рационального актора»: в системе, где сговор максимизирует выгоду участников, он является предсказуемым результатом.
- Социальная инженерия. Злоумышленник может обманом убедить владельца или опекунов инициировать процедуру восстановления на вредоносный ключ.
- Атака Сивиллы (Sybil Attack). Атакующий убеждает пользователя назначить опекунами несколько псевдонимов, контролируемых одним лицом. Получив контроль над кворумом, он может единолично захватить аккаунт.

К этим угрозам добавляются технические уязвимости, такие как ошибки в коде смарт-контракта или компрометация устройств опекунов, что нельзя сбрасывать со счетов.[9]

III. Пороговая криптография как

механизм митигации

В отличие от схем типа SSS, требующих уязвимой реконструкции ключа в одной точке, пороговые схемы подписи (TSS) являются более совершенным решением. TSS — это протокол многосторонних вычислений (MPC), в котором полный секретный ключ никогда не собирается в одном месте. Участники (владелец и опекуны) совместно генерируют единый публичный ключ и индивидуальные доли секрета. Для авторизации операции пороговое число участников совместно создает единую цифровую подпись, не раскрывая свои доли. Таким образом, распределяется сама способность подписывать, а не части ключа, что полностью устраняет единую точку отказа.

IV. Сравнительный анализ моделей

В модели TSS право владения привязано к единому публичному ключу, а управляющие транзакции требуют пороговой подписи. Сравнение моделей SKR на смарт-контрактах и с TSS представлено в таблице 1.

Таблица 1 – Сравнение моделей SKR по устойчивости к атакам

Атака	SKR (смарт-контракт)	SKR + TSS	Эффективность TSS
Сговор опекунов	Уязвима	Устойчива	Сговор позволяет подписать транзакцию, но не украсть ключ. Атака криптографически невозможна.
Социальная инженерия	Уязвима	Частично митигирована	Требуется обмануть пороговое число t опекунов, а не одного владельца. Сложность атаки возрастает.
Атака Сивиллы	Уязвима	Частично митигирована	Атакующий может авторизовать транзакции, но не может украсть долгосрочный ключ.
Уязвимость реконструкции	Уязвима	Устойчива	Приватный ключ никогда не восстанавливается в одном месте, что устраняет единую точку отказа.

Заключение

Проведенный анализ показывает, что системы социального восстановления ключей являются важным шагом к повышению удобства использования SSI для массовой аудитории. Однако их безопасность не может основываться на хрупкой модели социального доверия. Атаки на социальном уровне, в частности сговор опекунов, мотивированный как злым умыслом, так и рациональным эгоизмом, представляют собой критическую уязвимость в наивных реализациях SKR.

Внедрение пороговой криптографии, и в частности пороговых схем подписи, обеспечивает необходимую криптографическую основу для усиления этих систем. Распределяя возможность подписи без централизации или реконструкции ключа, TSS превращает SKR из системы, основанной на отзывном человеческом доверии, в систему с надежной, верифицируемой криптографической безопасностью.

Дальнейшая работа в этой области должна быть сосредоточена на разработке формальных, доказуемо безопасных моделей для кошельков на базе TSS, исследовании механизмов выбора опекунов, устойчивых к атаке Сивиллы (возможно, с использованием анализа социальных графов), и анализе производительности протоколов DKG и распределенной подписи на потребительских устройствах.

Список литературы

1. Allen, C. The Path to Self-Sovereign Identity // Life With Alacrity. – 2016. [Electronic resource]. – Mode of access: `http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html`.
2. Müller, P. A Survey on Essential Components of a Self-Sovereign Identity / P. Müller, C. P. Mainka, S. Kruse, T. Wollnitza, J. Pohlmann // arXiv preprint arXiv:1807.06346. – 2018.[6]
3. Buterin, V. Why we need wide adoption of social recovery wallets [Electronic resource]. – 2021. – Mode of access: `https://vitalik.ca/general/2021/01/11/recovery.html`.
4. Korir, D. Smart Contract-Based Social Recovery Wallet Management Scheme for Digital Assets / D. Korir, H. Kim, A. Yousaf // 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC). – 2023. – P. 0506–0512.[3]
5. Douceur, J. R. The Sybil Attack // Peer-to-Peer Systems. – Springer, 2002. – P. 251–260.
6. Halpern, J. Y. Rational secret sharing and multiparty computation / J. Y. Halpern, V. Teague // Proceedings of the thirty-sixth annual ACM symposium on Theory of computing. – 2004. – P. 623–632.
7. W3C. Decentralized Identifiers (DIDs) v1.0 [Electronic resource] // W3C Recommendation. – 2022. – Mode of access: `https://www.w3.org/TR/did-core/`.
8. Барсукевич, С. Н. Смарт-контракты и их роль в обеспечении доверия в финансовых транзакциях / С. Н. Барсукевич, С. Н. Нестеренков, П. С. Жуковец // BIG DATA и анализ высокого уровня = BIG DATA and Advanced Analytics : сборник научных статей X Международной научно-практической конференции – Минск : БГУИР, 13 марта 2024 г. ; – Ч. 1. – С. 309–315.