ПЕРЕДАЧА И ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 004.056

ЗАЩИТА ОТ ДЕАНОНИМИЗАЦИИ В КИБЕРСРЕДАХ, ИСПОЛЬЗУЮЩИХ РАСПРЕДЕЛЕННЫЕ РЕЕСТРЫ ДАННЫХ

Н.М. Охлопков, М.О. Калинин
Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург

Ключевые слова: анонимизация, распределенный реестр, одноразовый ключ.

Анонимность в системах распределенного реестра данных (СРР) не является фундаментальным криптографическим свойством, поскольку она ослабевает по мере накопления нарушителями безопасности транзакций, метаданных о топологии, анализа графа транзакций. Существующие методы анонимизации СРР (миксинг [1, 2], анонимные криптовалюты на базе zk-SNARK (Zerocash/Zcash)[3], CryptoNote/ Monero (кольцевые подписи)[4], stealth-адресация и одноразовые ключи[5]) обеспечивают различные уровни приватности, однако не отвечают одновременно всем требованиям практического внедрения (например, в сети «умного города»), в т.ч. масштабируемости, детерминированности задержек и возможности контролируемого раскрытия информации. Основной причиной угрозы деанонимизации СРР является статичность адреса получателя. Для устранения этой уязвимости авторами разработан новый метод анонимизации СРР, основанный на генерации одноразовых ключей и адресов и обеспечивающий разрыв долгосрочных корреляций. Метод направлен на снижение мультивходовости и ослабление эвристики общего входа.

В используемой двухключевой модели получатель публикует ID_B=(A_B, B_B), A_B=$a_B G$, B_B=$b_B G$, где a_B – просмотровый секрет (для распознавания), b_B – тратежный секрет (для расходования). В СРР не публикуются повторяющиеся адреса вида (A_B, B_B). В каждой транзакции создается новый одноразовый открытый ключ выхода P, который для нарушителя выглядит как случайный открытый ключ. Для масштабируемого управления ключами применяется детерминированная генерация из мастер-секрета [6].

Инициализация субъекта и публикация идентификатора выполняется следующим образом (вход: мастер-секрет $seed \in \{0,1\}^k$, выход: секреты (a, b) и публичный идентификатор ID=(A, B)):

1. Определение секретов:
$a=H2S(HMAC(seed,"view"))$, $b=H2S(HMAC(seed,"spend"))$.
2. Вычисление открытых ключей: $A=aG, B=bG$.
3. Опубликование $ID=(A,B)$.
4. Локальное сохранение секретов (a,b).

Формирование одноразового адреса выхода выполняется следующим образом (вход: идентификатор получателя $ID_B=(A_B,B_B)$, выход: пара (P,R), включаемая в транзакцию):

1. Генерация скаляра $r \leftarrow Z_q, R=rG$.
2. Вычисление и приведение к скаляру общего секрета $s=H2S(rA_B)$.
3. Формирование одноразового ключа выхода $P=sG+B_B$.
4. Включение P в транзакцию как условия владения выходом и R как вспомогательного открытого поля, не раскрывающего владельца.

Получатель не хранит таблицу одноразовых ключей. x восстанавливается из (a_B,b_B) и R. Отправитель собирает транзакцию в UTXO-модели: $tx=(I;\{(P_1,R_1,val_1),\dots,(P_m,R_m,val_m)\};\sigma)$, где I – входы, (P_j,R_j) – одноразовые выходы, val_j – значения, σ – подписи владельцев входов. После рассылки tx попадает в очередь транзакций и фиксируется в блоке. Для расходования UTXO, заблокированного на $P=xG$, получатель формирует подпись $\sigma_{sp}=Sign_x(m_{sp})$, $Verify_P(m_{sp},\sigma_{sp})=1$, где m_{sp} – контекст траты (например, хеш тела транзакции). Одноразовый секрет x после траты подлежит уничтожению, чтобы исключить накопление материала и его повторное использование. Жизненный цикл одноразовых ключей задается как управляемый процесс состояний (рис. 1).

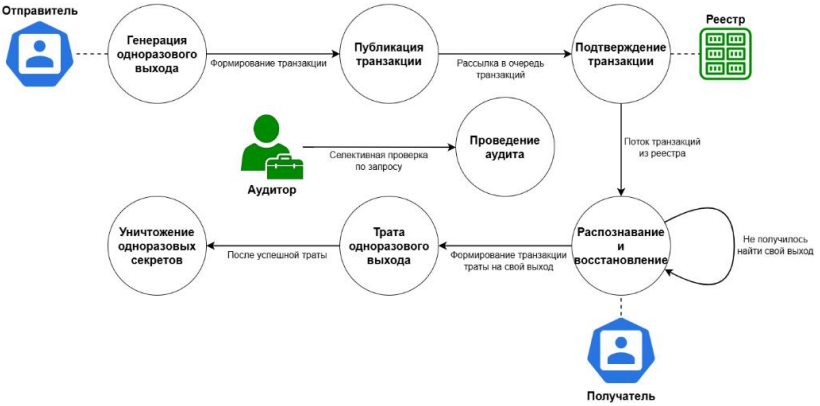

Рисунок 1 – Жизненный цикл одноразовых ключей

Экспериментальная оценка метода выполнена в имитационной СРР. Предполагается, что нарушитель имеет доступ ко всей истории и применяет эвристики общего входа и траты. Метрика F1-мера используется как

показатель успеха деанонимизации: чем выше F1, тем лучше нарушитель восстанавливает структуру CPP. Проверки выполнены для сценариев: «без анонимизации» (F1=1,0), ротация адресов (F1=0,23), метод CoinJoin (F1=0,22), stealth-выходы (F1=0,21). Разработанный метод достигает значения F1=0,17 благодаря сочетанию криптографической несвязываемости выходов и снижению мультивходовости через UTXO shaping, ослабляющему эвристику общего входа. При этом средний размер транзакции (369 байт) ниже, чем у stealth-выходов за счет уменьшения числа входов.

Исследование выполнено за счет гранта Российского научного фонда №24-11-20005, https://rscf.ru/project/24-11-20005/, гранта Санкт-Петербургского научного фонда (договор №24-11-20005 о предоставлении регионального гранта).

Список использованных источников

1.Stütz R. Adoption and actual privacy of decentralized coinjoin implementations in bitcoin // Proceedings of the 4th ACM Conference on Advances in Financial Technologies. – 2022. – P. 254-267.

2.Ruffing T., Moreno-Sanchez P., Kate A. Coinshuffle: Practical decentralized coin mixing for bitcoin //European symposium on research in computer security. – Springer, 2014. – P. 345-364.

3.Sasson E.B. Zerocash: Decentralized anonymous payments from bitcoin //IEEE symposium on security and privacy. – 2014. – P. 459-474.

4.Van Saberhagen N. CryptoNote v.2.0. – 2013.

5.Herskind L., Katsikouli P., Dragoni N. Privacy and cryptocurrencies. A systematic literature review // IEEE Access. – 2020. – Т. 8. – P. 54044-54059.

6. Nguyen-Dinh T. A hierarchical deterministic wallet using Ed25519 digital signature scheme // International Conference on Future Data and Security Engineering. – 2022. – P. 240-257.

Охлопков Никита Михайлович, студ., техник Высшей школы кибербезопасности ИКНК, СПбПУ, ohlopkov_nm@spbstu.ru.
Калинин Максим Олегович, д.т.н., профессор Высшей школы кибербезопасности ИКНК, СПбПУ, max@ibks.spbstu.ru.

УДК 004.056 ; 621.391

ОЦЕНКА НАРУШЕНИЯ СЕКРЕТНОСТИ ПЕРЕДАЧИ ДАННЫХ В РЭЛЕЕВСКОМ КАНАЛЕ

А.А. Тарасенко[1], Е.В. Прокопенко[2]
[1]филиал КузГТУ, г. Новокузнецк,
[2]Кузбасский государственный технический университет имени Т.Ф. Горбачева,г.Кемерово

Ключевые слова: передача данных; пассивный перехват; рэлеевское замирание; вероятность нарушения секретности; нейронная сеть.