Метод атаки на кольцевые подписи Monero: воспроизведение эффекта транзакций с нулевыми миксинами

Димаз Анка Виджайя (Dimaz Ankaa Wijaya)[1], Джозеф Лиу (Joseph Liu)[1], Рон Стейнфелд (Ron Steinfeld)[1], Донгкси Лиу (Dongxi Liu)[2]

[1] *Факультет информационных технологий, Университет Монаша, Австралия*
{dimaz.wijaya, joseph.liu, ron.steinfeld}@monash.edu

[2] *Группа Data61, Объединение научных и прикладных исследований (CSIRO), Австралия*
dongxi.liu@data61.csiro.au

Аннотация

Monero является одной из тех криптовалют, которые защищают анонимность пользователя, используя протокол CryptoNote. Возможности защиты анонимности Monero обеспечиваются криптографическими методами, которые подразумевают использование связанных кольцевых подписей и одноразовых публичных ключей. Последние исследования продемонстрировали, что большинство входов Monero отслеживались. Это происходило до того момента, пока использование протокола RingCT при проведении транзакций не стало обязательным. После реализации этого протокола проблема исчезла. Нами предлагается новый способ атаки, который снизит анонимность транзакций Monero или позволит полностью деанонимизировать входы. Предлагаемый протокол может запускаться в рамках сценария RingCT, а также обеспечивает взаимодействие множества атакующих, не требуя от них взаимного доверия. Схема атаки может быть подсажена в уже существующие службы Monero без каких-либо дополнительных комиссий и без риска для денег пользователей.

Ключевые слова: *Monero, кольцевая подпись, анонимность, конфиденциальность, отслеживаемость.*

I ВВЕДЕНИЕ

Monero является одной из самых ценных анонимных криптовалют в мире, и она основана на блокчейн технологии. Данные транзакции в блокчейне может увидеть каждый, как в случае с Bitcoin [1]. Однако, в отличие от Bitcoin, где любой желающий может отследить денежный поток между адресами, такое невозможно, когда речь заходит о Monero. Технологии использования кольцевых подписей и одноразовых ключей реализованы в качестве используемых по умолчанию настроек, что повышает анонимность данных транзакций. Реальные отправители скрываются за счёт добавления множества ложных объектов, при этом статус всех возможных отправителей одинаков, и они не отличаются друг от друга. Использование одноразового публичного ключа означает, что для каждого выхода создаётся уникальный адрес, а реальный адрес получателя никогда не будет открыт в блокчейне. При отсутствии какой-либо дополнительной информации невозможно определить, какой из адресов принадлежит определённому пользователю.

Несмотря на то, что эти методы сохранения анонимности уже были реализованы в Monero, уже было разработано, по крайней мере, 4 метода анализа, позволяющие вскрыть информацию, замаскированную таким образом в среде Monero. Эти методы анализа доказали свою успешность благодаря прозрачности данных блокчейна, проблемы ликвидности и идентификации поведения пользователей.

Нами предлагается новая схема атаки, направленной на нейтрализацию свойств Monero, обеспечивающих невозможность отслеживания валюты. Предлагаемый метод атаки может использоваться для вскрытия реальных выходов в транзакциях Monero или, по крайней мере, для снижения уровня анонимности входов. Схема атаки может быть реализована одним человеком или множеством людей, которые будут действовать совместно, но без необходимости во взаимном доверии. Каждый атакующий будет использовать положительные результаты действий другого атакующего. Наша схема атаки будет эффективно работать в среде RingCT, в которой сторонний наблюдатель не может увидеть сумму транзакции. Создание «тёмной» транзакции, описанной в рамках предлагаемой схемы атаки, не будет стоить каких-либо дополнительных комиссий, если схема атаки будет включена в любую уже существующую службу.

II ОБОСНОВАНИЕ

A Monero

Monero является форком существующей криптовалюты под названием Bytecoin. В основе обеих монет лежит протокол CryptoNote, предложенный человеком, скрывающимся под псевдонимом Николас ван Саберхаген (*Nicolas van Saberhagen*), в 2013 году [2]. Основной целью протокола является создание анонимной криптовалюты. В случае с Bitcoin существуют определённые проблемы, связанные именно с анонимностью пользователей. Предыдущие исследования позволили выявить информацию, касающуюся пользователей Bitcoin и их действий, совершаемых с этой криптовалютой [3]. Более того, злоумышленникам, использовавшим анализ графа, удалось открыть паттерны транзакций [4].

Протокол CryptoNote обеспечивает более высокий уровень анонимности, так как подразумевает использование связанных кольцевых подписей, гарантирующих неотслеживаемость, а также использование одноразовых публичных ключей, которые отвечают за невозможность привязки транзакций к определённым пользователям в новой системе. Эти возможности реализованы на уровне протокола, являющемся обязательным для всех пользователей системы.

Основной особенностью Monero является наличие возможности «правдоподобного отрицания». В наборе публичных ключей невозможно определить, какие из них были потрачены при проведении транзакции (на один вход, созданный несколькими ключами, тратится только 1 публичный ключ). Поэтому другие публичные ключи являются ложными (фальшивыми). Несмотря на эту особенность, которая считается основным плюсом Monero, ограничения, связанные с её реализацией, мешают системе продемонстрировать весь свой потенциал. Анализ показал, что значительную часть транзакций Monero можно отследить [5, 6].

Как и в случае с любой другой криптовалютой, для создания среды необходимо, по крайней мере, 2 участников: демонов и кошельков. Демон Monero является сервером, обеспечивающим клиентов информацией. Демон Monero синхронизирует данные блокчейна с одноранговыми узлами и записывает все транзакции на локальном накопителе. Кошелёк Monero является приложением, которое помогает пользователям управлять своими кошельками, обнаруживать, были ли получены на них новые платежи, подводить баланс и создавать новые транзакции. Кошелёк Monero не сохраняет блокчейн на локальном накопителе. Вместо этого он запрашивает у демона Monero любую информацию, необходимую кошельку Monero для обновления данных.

На рынке есть разные кошельки Monero. Первый и, пожалуй, главный кошелёк monero-wallet-cli создан главными разработчиками Monero. Сейчас он дополнен версией GUI. Вторым кошельком является онлайн кошелёк MyMonero[1]. Это сетевой кошелёк, который можно использовать для создания нового кошелька, транзакций и сканирования блокчейна с целью вычисления текущего баланса. OpenMonero[2] является открытой версией MyMonero с похожим интерфейсом, но улучшенной совместимостью с monero-wallet-cli, которую обеспечивает использование одной и той же мнемонической фразы, состоящей из 25 слов. Третий кошелёк разработан для операционной системы Android и называется Monerujo[3], и также является открытым проектом[4].

Для проведения вычислений с Monero кошельки OpenMonero и Monerujo используют ту же кодовую базу, что и monero-wallet-cli. Отличается только их интерфейс. Другой кошелёк Monero, разработанный Freewallet[5], имеет закрытый код, и его использование не рекомендуется сообществом Monero, так как пользователи не владеют собственными приватными ключами.

При создании транзакции кошелёк Monero не может действовать самостоятельно. Ему необходима информация, которую обеспечивает демон Monero. Так происходит, поскольку в случае с Monero каждый реальный выход, который будет потрачен во входе, должен быть скрыт несколькими другими ложными выходами. Эти ложные выходы часто называют миксинами. Ложные выходы вместе с реальным выходом формируют кольцевую подпись. Общее количество ложных выходов вместе с реальным выходом называют размером кольца.

Ложные выходы являются реальными публичными ключами, которые уже появлялись в блокчейне. Другими словами, эти ложные выходы являются выходами других транзакций. Эти

1 https://mymonero.com
2 https://github.com/moneroexamples/openmonero
3 https://monerujo.io
4 https://github.com/m2049r/xmrwallet
5 https://freewallet.org/currency/xmr

публичные ключи группируются в зависимости от суммы монет, содержащихся в публичных ключах, а затем последовательно индексируются в соответствии со временем их появления в блокчейне.

Сначала кошелёк Monero запрашивает «гистограммные данные». Это информация по максимальному индексу для каждой суммы каждого выхода в блокчейне. На основе этих гистограммных данных кошелёк Monero получает множество индексов. Количество индексов превышает размер кольца. В случае с транзакцией, проводимой в соответствии с протоколом RingCT, индексы будут браться из гистограммы с нулевой суммой (так как при использовании протокола RingCT любая информация о сумме транзакции шифруется, и система не может прочитать эту информацию и указывает нулевую сумму, хотя, на самом деле, она может и не быть нулевой).

Рисунок 1. Как создаются транзакции Monero

Start	Начало
Compute required coins + fee, check balance	Вычислить необходимые монеты + комиссию, проверить баланс
Construct a list of unspent outputs	Построить список непотраченных выходов
Request Histogram Data	Запросить гистограммные данные
Pick indexes from Histogram	Взять индексы из гистограммы
Request public key data based on the chosen indexes	Запросить данные публичного ключа на основе выбранных индексов
Finish	Конец
Transaction validated and confirmed, update wallet balance	Транзакция прошла валидацию и подтверждение, обновить баланс кошелька
Send the transaction to the Daemon	Отправить транзакцию Daemon-программе
Construct the inputs by using real inputs + decoys and sign	Создать входы, используя реальные входы + ложные и подписать

B Анонимность Monero

Анонимность Monero состоит из двух частей: несвязываемости и неотслеживаемости [2]. Несвязываемость можно описать на примере двух транзакций — невозможно определить были они отправлены одному и тому же человеку или нет. А неотслеживаемость касается ряда входов и невозможности определения, какой из входов был потрачен в ходе транзакции [5]. Согласно определению, несвязываемость направлена на защиту получателя, в то время как неотслеживаемость сохраняет анонимность отправителя.

Как неотслеживаемость, так и несвязываемость включены в протокол CryptoNote в качестве основного компонента системы. Неотслеживаемость достигается путём использования кольцевых подписей. Несвязываемость обеспечивается применением одноразовых публичных ключей.

1 Кольцевая подпись

Ривест, Шамир и Тауман (*Rivest, Shamir, Tauman*) первыми предложили использовать кольцевые подписи для раскрытия секретных данных общественности [7]. Утечка секретной информации может свидетельствовать о том, что она происходит из авторитетного источника (например, из совета директоров), но лицо, которое обнародует данные, при этом может пожелать скрыть, что именно оно является источником раскрытия секретной информации. Кольцевая подпись позволяет подписать информацию, используя приватный ключ, соответствующий публичному ключу, включённому в набор публичных ключей. Никто не сможет определить, какой из публичных ключей является тем ключом, которым была подписана транзакция.

Конструкция кольцевой подписи CryptoNote была разработана на основе предшествующих исследований связываемой кольцевой подписи [8] и отслеживаемой кольцевой подписи [9]. Структура таких подписей гарантирует, что ключ, которым они подписаны, можно будет определить, если такой публичный ключ будет использован более одного раза. Эта характеристика важна для криптовалюты, так как позволяет избежать двойных трат. Двойной тратой называют случаи, когда монета (или баланс) тратится более одного раза за время своего существования. Если в случае с какой-либо криптовалютой возможна двойная трата, то монеты в такой системе не стоят ничего и не могут использоваться в среде для хранения ценностей [10].

Кольцевая подпись Monero формируется путём объединения нескольких существующих выходов (называемых ложными выходами или миксинами), содержащих одинаковое количество монет, в один вход. Среди этих выходов должен быть один реальный выход, который будет потрачен при транзакции. У транзакции может быть как множество входов, так и множество выходов.

Рисунок 2. Структура транзакции Monero. Множество выходов, содержащихся во входе, сформированном путём смешивания реального выхода с другими выходами.

Output	Выход
Input	Вход
Transaction	Транзакция

Целью кольцевой подписи является снижение вероятности того, что злоумышленник вычислит реальный выход среди *N*-количества других выходов. Вероятность (P) вычисления траты реального выхода во входе обозначается как 1.

2 Одноразовый публичный ключ

Одноразовый публичный ключ, используемый в соответствии с протоколом CryptoNote, некоторым образом похож на скрытый адрес, который был создан в экосистеме Bitcoin [11, 12]. При этом сценарии получатель отправляет «родительский публичный ключ» отправителю. Затем отправитель, используя секретные ключи, генерирует «дочерний публичный ключ», который включается в данные транзакции в зашифрованном формате [13].

Получатель сканирует сеть на наличие новых транзакций и вычисляет секретный ключ каждой транзакции, используя родительский приватный ключ, который есть у него. Если результат соответствует ключу получателя, то транзакция включается в кошелёк в качестве входящей.

Использование одноразового публичного ключа гарантирует, что только отправителю и получателю будет известно об отношении между родительским публичным ключом и дочерним публичным ключом, которые используются при проведении транзакции, в то время как наблюдатель не может проанализировать отношение между ними при отсутствии каких-либо дополнительных данных, даже несмотря на то, что у наблюдателя есть доступ к блокчейну.

3 Кольцевые конфиденциальные транзакции

Кольцевые конфиденциальные транзакции (RingCT) впервые были использованы в Wolfram Warptangent (версия 5) и стали обязательными в Helium Hydra (версия 6). В блокчейне Monero первым блоком, содержащим RingCT транзакцию, является блок под номером 1 220 517. RingCT является методом, объединяющем в себе использование кольцевых подписей и конфиденциальных транзакций [14]. Он был разработан для того, чтобы включить возможность конфиденциальных транзакций в систему Monero, которая уже использовала кольцевые подписи [15].

Целью RingCT является решение проблем ликвидности путём сокрытия суммы монет, которая содержится в публичных ключах. Основным требованием к структуре кольцевой подписи является наличие у каждого члена кольца одинаковой суммы монет, чтобы нельзя было отличить реального члена кольца от ложного.

Есть проблема ликвидности, когда пользователи не могут создать транзакцию с достаточным количеством ложных объектов и используют транзакцию с нулевыми миксинами [16]. Транзакция с нулевыми миксинами предполагает отсутствие ложных объектов. Следовательно, она отслеживаемая, так как в отличие от транзакций с ложными объектами со 100% вероятностью можно определить, какой публичный ключ тратится в транзакции с нулевыми миксинами. Так как выходы в RingCT транзакциях маркируются как выходы с нулевым количеством монет, ложные объекты могут быть выбраны среди огромного количества публичных ключей.

C k-анонимность

Термин k-анонимность используется для моделирования анонимности данных, когда информацию, содержащуюся в пределах набора K, невозможно отличить от других элементов *k*-1 набора K [17]. В кольцевой подписи, содержащей более одного элемента, анонимность каждого элемента зависит от других элементов. Таким образом, если какое-либо количество *n* элементов

можно удалить из набора, обеспечивающего анонимность, каждый остающийся элемент имеет значение анонимности *k*-*n*.

В случае с Monero, *k*-анонимность может быть использована для определения уровня анонимности каждого входа, содержащего множество выходов в качестве ложных объектов. Анонимность реального входа зависит от неотличимости каждого объекта и количества используемых ложных объектов.

D Модель обработки

Нами была определена следующая модель обработки Monero. Любой может видеть всю информацию, содержащуюся в блокчейне Monero. Безопасность подтверждённых транзакций зависит от модели консенсуса Monero. Мы также определяем 2 типа «атакующих»: Атакующий A и Атакующий B. Атакующий A имеет достаточно средств, чтобы создавать стандартные транзакции и изменённые транзакции, но не имеет никакого доступа к программному обеспечению криптовалютных бирж или кошельков.

Существует группа Атакующих A = [A1, A2, A3, …], вступивших в сговор с целью атаки системы, но они не доверяют друг другу. Атакующий B имеет все те же возможности, что и Атакующий A, но также он может изменять программное обеспечение криптовалютных бирж или кошельков. Также существует группа Атакующих B = [B1, B2, B3, …], вступивших в сговор, но не доверяющих друг другу. Атакующий A и Атакующий B также могут сговориться, чтобы их действия возымели наилучший результат. Атакующие реализуют все этапы предлагаемого метода. Также есть наблюдатели, которые не заинтересованы в создании транзакций, но которых привлекают результаты и последствия. Также есть пользователи, которые используют кошельки и создают транзакции, но не заинтересованы в оценке анонимности своей деятельности.

III ИЗВЕСТНЫЕ АТАКИ НА АНОНИМНОСТЬ MONERO

A *Атака «Black Marbles»*

В этой статье мы используем термин «Black Marbles Attack» (*атака чёрными шариками*), чтобы обозначить атаку на анонимность Monero путём контроля максимально возможного количества выходов в блокчейне Monero [16]. Предполагается, что атакующий пытается контролировать большую часть выходов в блокчейне Monero. Если все выходы в блокчейне представить в виде шариков в урне, то чёрными шариками будут те выходы, которые контролируются атакующим, в то время как белыми шариками будут настоящие выходы, созданные пользователями. Урна обозначает совместно используемый леджер (блокчейн), где хранятся чёрные шарики (выходы, контролируемые атакующим) и белые шарики (настоящие выходы), которые видимы для всех наблюдателей.

Чтобы максимально увеличить эффект атаки, атакующему необходимо создать больше выходов (чёрных шариков), чтобы их количество превышало количество выходов других пользователей (белых шариков). Это можно сделать, отправляя монеты назад на собственный адрес [18]. Так как информация, касающаяся того, был потрачен выход или нет, отсутствует, атакующему необходимо постоянно добавлять большее количество чёрных шариков, чтобы повысить вероятность того, что его выходы будут использованы другими транзакциями в качестве ложных объектов.

B Транзакция с нулевыми миксинами и каскадный эффект

В случае с Monero, транзакциями с нулевыми миксинами называются транзакции, в которых, по крайней мере, один вход не использует никаких ложных объектов или миксинов. Транзакции с нулевыми миксинами не обладают возможностями анонимности, которые обеспечивают кольцевые подписи, и поэтому любой наблюдатель может быстро отследить реального отправителя транзакции. Проблема анонимности не является проблемой только транзакций с нулевыми миксинами, но и любой другой транзакции, которая использует те же выходы, которые были потрачены в транзакции с нулевыми миксинами, в качестве своего ложного объекта.

Кольцевая подпись является эффективным способом правдоподобного отрицания для обеспечения неотслеживаемости в оптимальной среде: есть достаточное количество выходов, имеющих идентичные характеристики, такие как возраст и количество монет, содержащихся в выходе. К сожалению, такую среду невозможно было полноценно реализовать для Monero до тех пор, пока использование протокола RingCT не стало обязательным.

Несмотря на то, что пользователям приходилось разбивать свои транзакции в соответствии с определённым правилом деноминации, это правило никогда строго не соблюдалось. В транзакциях всё ещё можно найти уникальные суммы монет, хотя это и создаёт проблему ликвидности, когда пользователь не может найти другие выходы, содержащие точно такую же сумму монет. Для всех тех выходов, для которых пользователи не могут найти соответствие, ими создаются транзакции с нулевыми миксинами: вход содержит только реальный выход без каких-либо миксинов или ложных объектов.

Несмотря на то, что уже говорилось о том, что транзакции с нулевыми миксинами создают каскадный эффект с точки зрения анонимности других транзакций [16, 18], новые исследования показывают, что эффект гораздо значительнее, чем ожидалось. При использовании методов, описанных в предыдущем исследовании, эффект достигает 87% [5] и 62% [6]. Это означает, что в случае, по крайней мере, более чем половины всех проанализированных входов (до введения протокола RingCT) ложные объекты можно отличить от реальных выходов.

C Временной анализ

В результате анализа транзакций с нулевыми миксинами также было выявлено, что в большинстве случаев реальные выходы тратились как последние выходы [6]. Экстраполирование собранных данных показывает, что 80% реальных выходов, которые удалось обнаружить, являются самыми последними. Единообразная выборка миксинов, используемая системой, не смогла скрыть этих характеристик.

Для решения проблемы были предложены новые методы выборки, треугольное распределение. Протокол треугольного распределения подразумевает, что 25% всех ложных объектов должны выбираться из недавно добавленных выходов. При использовании этого метода ожидается, что результаты временного анализа обнуляются, поскольку хотя бы 1 минимум из 5 обязательных миксинов в последней версии Monero (Helium Hydra) существует менее 5 дней.

D Публикация приватных ключей просмотра

Приватный ключ просмотра является особенностью системы Monero, которая позволяет проверять монеты, которыми владеет пользователь. Если пользователь предоставит приватный ключ просмотра от своего кошелька аудитору, то аудитор сможет отследить каждую монету, полученную на соответствующий адрес. Несмотря на то, что приватный ключ просмотра позволяет осуществлять подобные действия. Аудитор не сможет украсть монеты у пользователя, используя такой ключ. Также аудитор не сможет проверить, были потрачены монеты или нет.

Приватный ключ просмотра также может использоваться для организации атаки на функцию несвязываемости Monero. Предполагается, что анонимность пользователя зависит от анонимности других пользователей. Приватные ключи просмотра могут быть использованы для того, чтобы отличить выходы, отправленные владельцу приватных ключей просмотра, от выходов, отправленных обратно отправителю (сдачи). Несмотря на то, что приватный ключ просмотра можно использовать для определения всех выходов, направленных на адрес приватного ключа просмотра, он не позволяет определить, были или нет потрачены выходы при помощи соответствующего приватного ключа траты.

Рисунок 3. Приватный ключ просмотра позволяет определить все входящие выходы (платежи), приватный ключ просмотра также позволяет определить выходы, отправленные на соответствующий адрес, путём сканирования всех транзакций в блокчейне.

Input	Вход
Transaction	Транзакция
Output	Выход
Private Viewkey	Приватный ключ просмотра

Приватный ключ просмотра считается скорее преимуществом, а не недостатком. Он в основном используется в случаях, требующих соблюдения определённых правил, например, при проведении аудита или при работе с благотворительными организациями [19]. Вместе с тем после аудита невозможно восстановить несвязываемость, не создав нового адреса и не переместив всех средств на этот новый адрес.

E Сравнение предлагаемой нами схемы атаки с уже существующими

При проведении атаки Black Marbles предполагается, что атакующий создаёт новые выходы путём создания транзакций, соответствующих количеству выходов, созданных другими пользователями. Чем больше выходов у атакующего, тем выше вероятность того, что он понизит уровень анонимности других пользователей. Этот тип атаки можно реализовать исключительно индивидуально. Или же, если атака координируется несколькими атакующими, каждому из них придётся доверять другому атакующему при определении того, является ли выход результатом атаки или нет. Атаку Black Marbles также можно комбинировать с публикацией приватных ключей просмотра и направлять транзакции на адрес атакующего. Но при этом транзакции не служат какой-либо другой цели, а следовательно, комиссии, выплачиваемые майнерам, тратятся впустую.

А отличие от Black Marbles, предлагаемая нами схема атаки лучше тем, что сценарий атаки несколькими атакующими скоординирован. Каждый атакующий проводит атаку, а её результат также может быть оценён другими атакующими без использования какой-либо другой информации, такой как приватные ключи просмотра. При использовании предлагаемой нами схемы, транзакцию не нужно направлять на свой собственный адрес, а следовательно, её просто реализовать в существующих онлайн сервисах, таких как биржи или кошельки. Биржи и кошельки не требуют каких-либо дополнительных комиссий, так как им придётся просто реализовать метод в системе и преобразовать свои обычные транзакции в «тёмные» транзакции, у которых будет ослаблен только уровень анонимности.

Предлагаемая нами схема атаки не опирается на наличие транзакций с нулевыми миксинами, так как такой метод устарел после обновления Monero, то есть после введения RingCT и обязательного минимального количества миксинов. На этапе настройки воспроизводится подобное воздействие транзакции с нулевыми миксинами, а на этапе атаки воспроизводится каскадный эффект транзакции с нулевыми миксинами.

Предлагаемая нами схема атаки ещё более эффективна, если её использовать с системой, использующей протокол RingCT, так как атакующему не приходится атаковать множество монет с разным достоинством, а можно сосредоточиться на одной. Более того, RingCT позволяет атакующему использовать небольшое количество монет. Система не может обнаружить количество отправленных монет, поэтому атакующий отправляет 0 монет, и система принимает это.

Наша схема атаки демонстрирует более высокий уровень точности, если сравнивать её с временным анализом. При временном анализе атака зависит от того, как выбираются ложные объекты среди всех доступных выходов в системе. Если алгоритм выбора оптимален, временной анализ не позволяет определить был ли во входе потрачен реальный выход. При использовании нашей схемы атаки реальный выход определяется со 100% точностью. Краткое сравнение приводится в таблице I.

ТАБЛИЦА I. СРАВНЕНИЕ МЕТОДОВ АТАКИ

Факторы	M	M	A	PV	Urs
Взаимодействие атакующих					
Отсутствие в необходимости дополнительных меток					
Устойчивость к протоколу RingCT					
Минимальная сопротивляемость миксинам					
Точность при определении реальных выходов					

IV ПРЕДЛАГАЕМАЯ НАМИ СХЕМА АТАКИ

A Обзор

Предлагаемая нами схема атаки использует мягкость daemon-программы Monero в отношении создания транзакций кошельком Monero. Monerod проверяет только действительность транзакции, передаваемой на сервер. При этом транзакции должны иметь правильный баланс и действительные цифровые подписи. Построение кольца во время создания цифровой подписи полностью обрабатывается кошельком. Daemon-программа Monero помогает кошельку, предоставляя информацию публичных ключей, основанную на индексах, взятых кошельком.

На основе данной информации можно построить вредоносную транзакцию и понизить уровень *k*-анонимности или даже деанонимизировать транзакции Monero. Воздействие будет подобным каскадному эффекту, как при использовании транзакций с нулевыми миксинами.

B Предлагаемый метод

Предлагаемая схема атаки делится на три этапа: подготовка, настройка и сама атака. Реализация этапа атаки возможна с применением двух методов: пассивного и активного. Каждый этап более подробно рассмотрен ниже.

1 Этап подготовки

Для проведения каждой атаки атакующему необходимо некоторое количество непотраченных выходов. Количество выходов зависит от минимального размера кольца *r*, соответствующего требованиям системы Monero. Шестая версия (Helium Hydra) предполагает, что минимальный размер кольца *r* равен пяти, поэтому минимальное количество выходов, необходимое атакующему, также равно пяти. Целью этапа подготовки является сбор непотраченных выходов, которые потом будут потрачены на этапе настройки. Если количество выходов, которые есть в наличии у атакующего, превышает минимальный размер кольца, но при этом оно меньше, чем кратные значения *r*, то остающиеся выходы можно будет использовать на этапе атаки.

При работе с протоколом RingCT необходимость в одинаковом количестве монет для каждого выхода отсутствует. Следовательно, атакующий может использовать небольшое количество монет, распределённое среди множества выходов. Это означает, что атакующий может сосредоточиться только на выплате комиссий за транзакции, не имея каких-либо отложенных на всякий случай монет.

Количество тредов, создаваемых атакующим, зависит от типа атаки, который он собирается использовать. Если атакующий намерен использовать пассивный тип атаки, то ему нужно создать максимально возможное количество тредов. Успех атаки зависит от количества тредов, созданных атакующим, в то время как при активной атаке, атакующем достаточно создать всего один тред. Выходы будут использоваться повторно с последующими транзакциями, что не снизит эффективность атаки, но может вызвать подозрения, когда один и тот же выход будет использован множество раз.

2 Этап настройки

На этом этапе необходимо создать точное количество входов *r* для каждого треда атаки. Это означает, что атакующим будет создано *r* кольцевых подписей. Каждая кольцевая подпись будет тратить выход транзакции, который имеется у атакующего. Допустим, что ряд *l* публичных ключей $L = [PK_A, PK_B, PK_C, PK_D, PK_E, \ldots]$, а их пары образов секретных ключей $K = [I_A, I_B, I_C, I_D, I_E, \ldots]$. Количество публичных ключей в L равно *r*. Ложные объекты для каждой кольцевой подписи выбираются из *L*, как показано на рисунке 4.

Входы могут быть включены в транзакцию или во множество транзакций, но с точки зрения затрат выгоднее иметь *r* входов в одну транзакцию. Этап настройки имеет эффект подобный использованию транзакции с нулевыми миксинами, но с одним отличием. При проведении транзакции с нулевыми миксинами любой может точно определить, какой из входов тратит выход. На этом этапе настройки невозможно определить точный вход, который тратит определённый выход. Мы можем только сказать, что все входы на этапе настройки тратят все члены *L*, независимо от того, какой из входов какой выход тратит. Целью этапа настройки является обнуление вероятности того, что другими транзакциями будет потрачен какой-либо из членов *L*.

Рисунок 4. Этап настройки (r = 5)

Ring Signature	Кольцевая подпись
Signer’s Public Key	Публичный ключ подписывающего

Signer’s Hidden Private Key (Key Image)	Скрытый приватный ключ подписывающего (образ ключа)

Если атакующий не создаёт r входов, где все выходы являются членами L, то требование к воссозданию эффекта транзакции с нулевыми миксинами не выполняется. Другие обозреватели не могут определить, были или нет потрачены входы, и поэтому этап атаки не может быть реализован.

3 Этап атаки

Существуют два типа атаки, которые можно использовать: пассивная атака и активная атака. Каждый тип атаки имеет свои цели и различные методы реализации. Оба типа описаны ниже.

Рисунок 5. Пассивная атака

Ring Signature	Кольцевая подпись
A New Transaction TX_F	Новая транзакция TX_F
Spent	Потрачены
Reduced k-anonymity by 2	Сниженный на 2 уровень k-анонимности

Пассивная атака. Цель пассивной атаки состоит в том, чтобы потраченные на этапе настройки выходы (члены *L*) были использованы другими пользователями во множестве транзакций. Если это произойдёт, наблюдатель пропустит публичные ключи, так как они были потрачены в транзакциях на этапе настройки, а публичные ключи не могут быть повторно использованы в каких-либо других транзакциях. Эти транзакции имеют сниженный уровень *k*-анонимности. Степень снижения уровня *k*-анонимности зависит от количества ложных объектов, поступающих из транзакций на этапе настройки. Пример, показанный на рисунке 5, иллюстрирует снижение уровня анонимности на 2 в соответствии с количеством публичных ключей, использованных в качестве ложных объектов.

Активная атака. Допустим, атакующим B была запущена вредоносная служба кошелька Monero. Целью кошелька является не хищение монет пользователей, а обеспечение отслеживаемости транзакций. Кошельку известны публичные ключи *L*, и он использует их в качестве ложных объектов в кольцевой подписи, как показано на рисунке 6.

Активная атака эффективна, если направлена на выходы других пользователей, особенно если протокол атаки реализован в кошельке. Пользователь может не определить вредоносное поведение кошелька, так как транзакции будут по-прежнему создаваться успешно.

Рисунок 6. Активная атака

Existing Transactions: TX_A, TX_B, TX_C, TX_D, TX_E	Существующие транзакции TX_A, TX_B, TX_C, TX_D, TX_E
Ring Signature	Кольцевая подпись
A Malicious Wallet	Вредоносный кошелёк
A New Transaction TX_F	Новая транзакция TX_F
Public Key being spent in the transaction	Публичный ключ, который тратится при транзакции

Разница между пассивной и активной атаками состоит в том, что в случае пассивной атаки атакующий проводит грубую атаку, чтобы снизить уровень анонимности другой транзакции, в то время как при активной атаке атакующий может полностью деанонимизировать входы. При пассивной атаке необходимость в настройке каких-либо сервисов (биржевых или сервисов кошелька) отсутствует, в то время как при проведении активной атаки сервисы используются и атакуются только теми пользователями, которые используют такие сервисы.

V ОЦЕНКА

A Доказательство концепции

Для доказательства концепции предлагаемой нами схемы атаки был реализован этап подготовки, этап настройки и этап пассивной атаки. Нами был изменён исходный код Monero, чтобы создать вредоносный кошелёк, который смог бы создавать транзакции, соответствующие нашей схеме, в частности, simplewallet.cpp и wallet2.cpp. Схема нашего кошелька показана на рисунке 7.

1 Этап подготовки

Вместо нормального использования протокола при сборе индексов из гистограммных данных, мы берём индексы из публичных ключей, сохранённых в нашем собственном кошельке. Следовательно, так как кошелёк также хранит глобальные индексы для каждого выхода, нет никакой необходимости в запросе данных у daemon-программы, так как кошелёк сам выполнит все необходимые требования.

Нами были успешно реализованы этапы подготовки и настройки в основной сети Monero. Этап настройки был выполнен в один тред при $r = 5$. На этапе подготовки использовался следующие идентификатор:

b6781f2a6f5608553546442b84888346fdc3f78dd8995170180ed74081c05362

2 Этап настройки

А в этапе настройки мы использовали следующий идентификатор:

8d4a0c7eccf92542eb5e1f09e72cc0d934b180b768bc95388d33051db83194bb

Рисунок 7. Схема транзакции атаки

Start	Начало
Compute required coins + fee, check balance	Вычислить необходимые монеты + комиссию, проверить баланс
Construct a list of unspent outputs	Построить список непотраченных выходов
Pick indexes from Histogram	Взять индексы из гистограммы
No request to Daemon is required	В запросе Daemon-программы нет необходимости
Finish	Конец
Transaction validated and confirmed, update wallet balance	Транзакция прошла валидацию и подтверждение, обновить баланс кошелька
Send the transaction to the Daemon	Отправить транзакцию Daemon-программе
Construct the inputs by using real inputs + decoys and sign	Создать входы, используя реальные входы + ложные и подписать

3 Этап пассивной атаки

На этапе настройки нами были установлены 5 публичных ключей, которые можно определить как потраченные при проведении транзакции. Эти ключи были взяты 12 другими входами в качестве одного из своих ложных объектов. Это означает, что используя наши 5 публичных ключей, мы можем снизить уровень анонимности других 12 входов на 1. Успешность подтверждения транзакции в блокчейне Monero на этапе настройки доказывает, что система не проверяет структуру кольцевой подписи. Нами не был реализован этап активной атаки, так как создание транзакции на этапе активной атаки не представляет особого интереса. Количество транзакций, на которых будет оказано влияние, в реальности зависит от других пользователей, а потраченные выходы можно по-прежнему брать в качестве ложных объектов гораздо позже того, как вредоносные транзакции будут подтверждены в блокчейне из-за метода произвольной выборки, который используется Monero.

Чтобы увидеть, был ли наш метод использован в системе Monero, нами были взяты данные блокчейна Monero в формате RDBMS из блоков, начиная с 0 и заканчивая 1 470 000. Мы используем хеш-функцию, чтобы хешировать члены выхода каждого входа в блоках и сравниваем значения хеша, чтобы найти дубликаты.

Рисунок 8. Процент дубликатов в зависимости от размера кольца

Hash Count	Количество хеш значений

При минимальном размере кольца равном двум, нами было обнаружено 2947 дубликатов колец, которые были похожи на те, что были у нас на этапе настройки (включая нашу собственную транзакцию). Эти дубликаты состоят из 1244 чётких наборов и включают в себя 855 различных транзакций. Первый дубликат был обнаружен в блоке 47 410, а последний — в блоке 1 401 899. Наша транзакция вошла в блок 1 468 439.

Рисунок 9. Анализ отслеживаемости с использованием анализа пассивной атаки

Traceability Analysis	Анализ отслеживаемости
Number of Inputs	Количество входов
Iteration	Итерация

Схема, показанная на рисунке 8, отображает статистику обнаружения дубликатов в зависимости от размера кольца. Более половины дубликатов были обнаружены при размере кольца равном двум, в то время как в 43% случаев обнаружения размер кольца составлял три. Небольшое количество данных (2%) было обнаружено при размере кольца равном пяти. Все эти транзакции были созданы без использования протокола RingCT.

При использовании схемы пассивной атаки нам удалось обнаружить 595 входов. При реализации схемы пассивной атаки количество итераций достигало пяти. Затем мы подсчитали все входы, которые были определены нами как потраченные, в зависимости от размера кольца, как показано на рисунке 10. Из 595 входов 73% были обнаружены при размере кольца равном трём, а остальные 28% были обнаружены при размере кольца равном двум. Два входа было найдено при размере кольца равном четырём и только 1 вход был обнаружен при размере кольца равном пяти.

Рисунок 10. Процент отслеживаемых входов в зависимости от размера кольца

Traceable Inputs	Отслеживаемые входы

Если выходы, которые были определены нами как потраченные, использовались другими транзакциями, то их можно отбросить при вычислении реальных входов. Нами было обнаружено ещё 66 входов, уровень анонимности которых был снижен на 1.

Рисунок 11. Снижение уровня анонимности в зависимости от размера кольца

Reduced Anonymity	Снижение уровня анонимности

B Анализ затрат

Чтобы использовать 5 публичных ключей в качестве выходов атаки, понадобилось создать две транзакции: первую для этапа подготовки и вторую для этапа настройки. В случае с нашими примерами, на этапе подготовки было потрачено примерно 0,034 XMR, в то время как на этапе настройки потребовалось 0,0135 XMR. При настройках, используемых по умолчанию, общие затраты составили 0,0475 XMR. При текущей рыночной цене Monero, которая составляет US$216,14, майнеру было выплачено US$10,27.

C Сравнение результатов с каскадным эффектом использования транзакций с нулевыми миксинами

Нами были воспроизведены методы, описанные в работах [5, 6]. Процесс выделения был реализован с применением API-интерфейсов Onion Monero Blockchain Explorer[6]. Onion Monero Blockchain Explorer работает как шлюз для присвоения индексов реальным публичным ключам миксинов транзакций, взятых из Monerod, полностью синхронизированного с сетью. Затем мы сравнили результаты применения известных методов с нашими результатами.

Сравнение показало, что ни один из результатов применения нашей схемы не был обнаружен при помощи известных методов. Возможно, использованные выходы имели проблему ликвидности, а владельцы этих выходов комбинировали их с меньшим количеством выходов. Нам не удалось сравнить наши результаты с данными MoneroLink[7] из-за различий в индексировании выходов. Система MoneroLink не обеспечивает какой-либо информации, касающейся каждого из выходов, и поэтому невозможно определить методы индексирования, используемые системой.

VI ОГРАНИЧЕНИЯ, ЗАКЛЮЧЕНИЕ И ДАЛЬНЕЙШАЯ РАБОТА

A Ограничения

6 https://github.com/moneroexamples/onion-monero-blockchain-explorer
7 http://monerolink.com

В случае с Monero невозможно определить владельцев монет, так как публичный ключ может быть потрачен единожды в течение всего жизненного цикла. Следовательно, так же невозможно вычислить количество транзакций, созданных биржами для определения влияния любого правила, которым приходится следовать бирже при создании таких транзакций.

B Заключение

Нами была предложена и продемонстрирована новая схема атаки на неотслеживаемость системы Monero. Мы показали, что анонимность системы зависит от реализации кошелька и структуры каждой транзакции. Наша схема атаки использует слабые места метода кольцевой подписи, который предполагает произвольную выборку миксинов.

Атакованные кошельки могут лишить пользователей анонимности. При этом их деньги украдены не будут. Обнаружение такого воздействия требует сканирования всех существующих и когда-либо существовавших в блокчейне комбинаций структуры кольца, и маловероятно, что пользователи, которым ничего не известно о такой атаке, когда-либо обнаружат воздействие, так как они попросту не будут терять свои деньги.

В том случае, если правительство захочет отслеживать анонимные криптовалюты, использующие кольцевые подписи, то такое правительство принудит компании, занимающиеся обменом монет, а также предоставляющие сервисы, связанные с кошельками, строить транзакции таким образом, как предполагает предлагаемая нами схема атаки. Несмотря на то, что регуляторы не смогут отследить каждую транзакцию в блокчейне, часть транзакций всё-таки удастся отследить. Компаниям, которые последуют установленным правилам, не придётся тратить дополнительных денег на построение таких транзакций. Могут возникнуть только определённые траты, связанные с изменением их кошельков.

В отличие от атаки Black Marbles, наша схема может быть запущена множеством атакующих. Каждый атакующий будет выгодно использовать результат деятельности других атакующих, так как неотслеживаемость выходов транзакций будет ненадёжной, и это сможет использовать любой, имеющий доступ к блокчейну Monero. Нет никакой необходимости во взаимном доверии между атакующими в отношении данных, которыми они обмениваются, поскольку данные подтверждают правильность атаки. Следовательно, этот тип атаки могут свободно использовать биржи и провайдеры услуг, связанных с кошельками. Правительства могут принудить такие компании использовать такую схему.

На основе результатов нашего исследования необходимо усовершенствовать протокол, чтобы защитить анонимность пользователей, независимо от доверия к кошельку, так как кошелёк может построить транзакцию, которая снизит уровень анонимности или вообще уничтожит анонимность. Обнаружение и занесение в чёрный список являются двумя альтернативными методами, которые позволят избежать такой атаки.

C Дальнейшая работа

Предложенный нами метод атаки также может быть реализован в других системах, использующих кольцевые подписи, например, в системе электронного голосования (e-голосования). Такие системы могут быть подвергнуты нашей атаке по следующему сценарию. Предположим, проводятся выборы, в ходе которых кандидаты соревнуются для получения места в правительстве. Кандидат хочет «купить голоса» голосующих, чтобы победить в выборах. Так как при электронном голосовании используются кольцевые подписи, кандидат покупает голоса оптом. Чтобы сделать это, необходим координатор продавцов голосов. Координатор создаёт список всех продавцов голосов и разбивает их на группы в зависимости от размера кольца n, используемого системой e-голосования. Каждая группа состоит из n продавцов голосов. Затем каждый член такой группы сообщает свой публичный ключ, который другие члены группы должны будут использовать в качестве ложного объекта. Каждая группа создаёт n транзакций с идентичными членами кольца, чтобы голоса были отданы определённому кандидату. Структура транзакции напоминает ту, что мы имеем на предлагаемом нами этапе настройки.

ССЫЛКИ

1 S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, Available: http://bitcoin.org/bitcoin.pdf.

2 N. van Saberhagen, "Cryptonote v 2. 0," 2013.

3 S. Meiklejohn *et al.*, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *USENIX ;login:,* 2013.

4 D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Financial Cryptography and Data Security*: Springer, 2013, pp. 6-24.

5 A. Kumar, C. Fischer, S. Tople, and P. Saxena, "A Traceability Analysis of Monero's Blockchain," *IACR Cryptology ePrint Archive,* vol. 2017, p. 338, 2017.

6 A. Miller, M. Möser, K. Lee, and A. Narayanan, "An Empirical Analysis of Linkability in the Monero Blockchain," *arXiv preprint arXiv:1704.04299,* 2017.

7 R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2001, pp. 552-565: Springer.

8 J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Australasian Conference on Information Security and Privacy*, 2004, pp. 325-335: Springer.

9 E. Fujisaki and K. Suzuki, "Traceable ring signature," in *Public Key Cryptography*, 2007, vol. 4450, pp. 181-200: Springer.

10 M. V. Alstyne, "Why Bitcoin has value," *Commun. ACM,* vol. 57, no. 5, pp. 30-32, 2014.

11 P. Todd. (2014, October 8, 2015). *Stealth Addresses*. Available: http://sourceforge.net/p/bitcoin/mailman/message/3 1813471/

12 unSYSTEM Wiki. (2014). *DarkWallet/Stealth*. Available: https://wiki.unsystem.net/en/index.php/DarkWallet /Stealth

13 S. Noether and S. Noether, "Monero is Not That Mysterious," 2014.

14 G. Maxwell, "Confidential Transactions," *URL: https://people.xiph.org/~greg/confidential_values.t xt (Accessed 09/05/2016),* 2015.

15 S. Noether and A. Mackenzie, "Ring confidential transactions," *Ledger,* vol. 1, pp. 1-18, 2016.

16 S. Noether, S. Noether, and A. Mackenzie, "Mrl-0001: A note on chain reactions in traceability in cryptonote 2.0," Technical report2014.

17 L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 10, no. 05, pp. 557-570, 2002.

18 A. Mackenzie, S. Noether, and M. C. Team, "Improving Obfuscation in the CryptoNote Protocol," 2015. Moneroblocks. *Richlist*. Available: https://moneroblocks.info/richlist