**Седьмая стадия анонимности.**

**Пример функционирования вне математических абстракций**

Коваленко Геннадий Александрович

**1. Введение**

Все доказательства, дополнительные пояснения, «подводные камни», развитие анонимности и противоречия безопасности необходимо искать в основной статье «Теория строения скрытых систем» [1]. В данной же статье будет представлено только функционирование седьмой стадии анонимности, то есть абсолютной анонимности, без каких бы то ни было теоретико-математических пояснений. Весь акцент будет уделён примеру реальной работе системы.

**2. Анонимность**

Для понимания седьмой стадии анонимности необходимо в первую очередь выявить само определение анонимности, её основные характеристики и очертания. В общих чертах:

1. Анонимность обязана быть внутренней (относительно анализа со стороны узлов) и внешней (относительно анализа трафика сети). Данный критерий должен обуславливаться разрывом связи между субъектами посредством их объекта (полиморфизмом информации).

* Под полиморфизмом информации понимается множественное шифрование в совокупности с последующей маршрутизацией.

2. Анонимность обязана быть двунаправленной относительно субъектов информации и применяться как к отправителю - инициатору связи, так и к получателю - платформе связи. Данный критерий должен обуславливаться разрывом связи между идентификацией сетевой и криптографической.

* Под идентификацией сетевой подразумеваются IPv4, IPv6 адреса. Под идентификацией криптографической подразумеваются публичные ключи, хеши публичных ключей.

3. Анонимность обязана предотвращать сохранение данных и метаданных в транспарентном состоянии для промежуточных узлов. Данный критерий должен обуславливаться заменой всех платформ связи на пятую стадию анонимности, тем самым уменьшая мощность доверия до теоретически возможного минимума.

* Под пятой стадией анонимности предполагается система, безопасность которой определяется только (или в большей мере) качеством клиентской части.
* Под мощностью доверия понимается количество узлов, участвующих в хранении или передаче информации, представленной дли них в открытом представлении.

На вышеприведённых критериях базируются сети шестой и седьмой стадий анонимности ориентируемые на безопасность. Но отличие седьмой стадии, в сравнении с шестой, сводится к дополнительному критерию, изменяющим первый:

4. Анонимность абсолютная обязана существовать даже в заведомо враждебной, замкнутой и полностью прослушиваемой системе. Данный критерий должен обуславливаться модификацией первого критерия, а именно заменой полиморфизма на вероятностный полиморфизм.

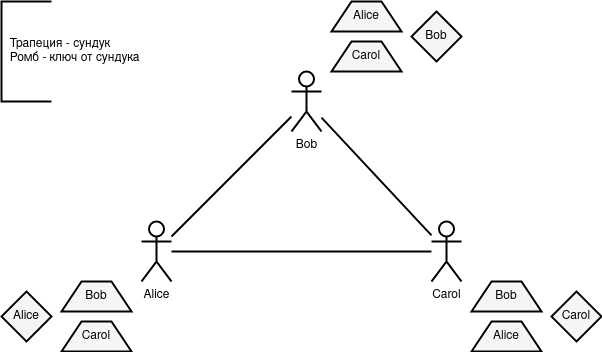
* Под вероятностным полиморфизмом понимается случайно выбранное число из диапазона [*0*;*N*] представленное количеством слоёв шифрования в совокупности с заливочной маршрутизацией.

Третий критерий анонимности в последующих рассуждениях будет опущен, т.к. он предполагает существующую анонимную сеть в базе которой уже располагаются безопасные сервисы, построенные на пятой стадии анонимности. Само же повествование этой статьи рассчитано на анализ анонимной передачи информации, а не её сохранения.

**3. Седьмая стадия анонимности**

Предположим, что существует три участника — Алиса, Боб, Кэрол, где ни один из них не заинтересован в деанонимизации остальных субъектов посредством выдачи себя как единственного маршрутизатора информации. Такое условие необходимо, потому как сеть становится деанонимизированной только при условии *N - 1 = 2*, где *N* - количество участников. Это есть базис системы, её основание, с которого начинается абсолютная анонимность как таковая.

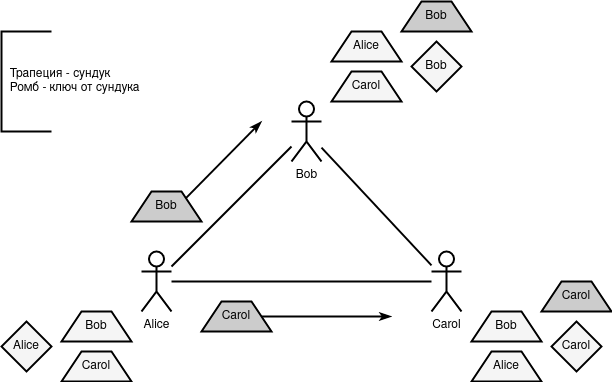
Теперь предположим, что у каждого участника существует безграничное количество сундуков[[1]](#footnote-2) от каждого субъекта в сети (в реальном мире такое условие конечно же невозможно, но примем во внимание, что все описанные действия должны происходить в компьютерной сети, где информация способна дублироваться бесконечное количество раз), при этом каждый способен создавать сообщение, отправлять и получать. Также, каждый участник содержит свои ключи под выданные им сундуки. Связь в такой системе широковещательная, то есть создавая сообщение каждый должен получить свой сундук.



**Рис. 1.** Исходная модель коммуникации субъектов в седьмой стадии анонимности

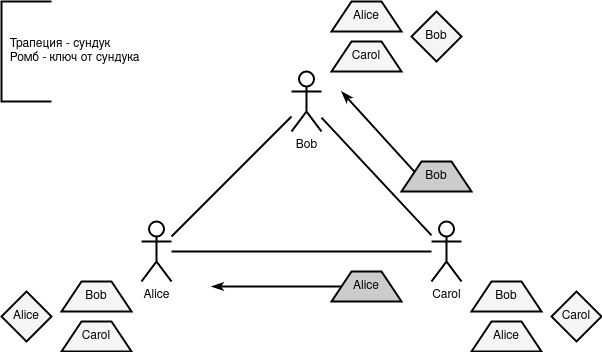
Допустим, Алиса является инициатором связи, иными словами отправителем, при этом получатель информации нам неизвестен. Первоочередной задачей ставится определение получателя информации.

Алиса кладёт своё сообщение в один из сундуков, все их закрывает и отправляет каждому. Получатель же в такой системе должен ответить отправителю, что может его сразу же выдать, но в этом случае стоит учесть момент, в котором, из-за вероятностного полиморфизма, Алиса может в один сундук положить другой. Во вложенном сундуке уже может существовать настоящее сообщение (чисто технически можно выявить сундуки с разными размерами, а следовательно, и получателя сообщения. Данный аспект также распространяется и на компьютерные сети, где информация имеет свой размер. Решение данной проблемы описано в основной статье, в разделе ««Подводные камни» седьмой стадии анонимности». Лучше пока предположить, чисто теоретически, что все сундуки без исключения имеют одинаковые размеры).



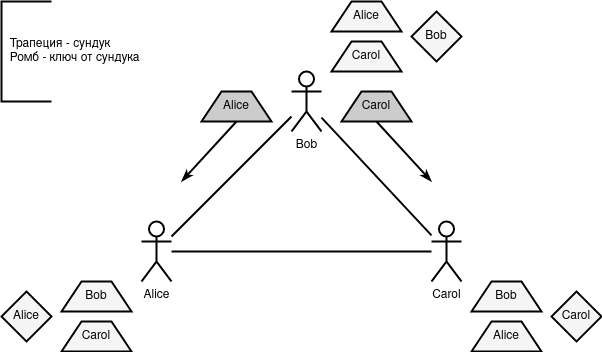
**Рис. 2.** Отправление сундуков в одном из которых находится сообщение от Алисы

Таким образом, в сундуке Боба может оказаться сундук Кэрол и наоборот, либо может оказаться просто сообщение. Вероятность каждого события . В любом случае получатель должен ответить на запрос, равно как и маршрутизатор должен отправить полученный сундук дальше. На данном этапе определить получателя не представляется возможным.



**Рис. 3.** Действия Кэрол - это ответ или маршрутизация?

Кэрол продолжив действия, отправляет одновременно и Алисе, и Бобу их сундук. В одном из сундуков находится также сообщение. Но и данное транспортирование также вызывает неопределённость, а именно является ли Кэрол получателем (сундук Алисе) или она является маршрутизатором (сундук Бобу).



**Рис. 4.** Действия Боба - это ответ или запрос?

Финалом возможной (т.к. Алиса не отвечает на ответ) маршрутизации со стороны Кэрол является последующая неопределённость, а именно является ли Боб получателем (сундук Алисе) или он вовсе является отправителем (сундук Алисе или Кэрол).

В итоге такая цикличность и прирост неопределённостей только суммируется. Это уже можно видеть на данной примере, где в начале связи Алиса была определённым инициатором, а спустя два действия сам факт отправления становится алеаторным (точно ли Боб является отправителем?).

**4. Заключение**

В данной статье была приведена работа седьмой стадии анонимности, где было показано зарождение неопределённости посредством вероятностного полиморфизма. Первоначально известный фактор отправления спустя две итерации становится уже алеаторным.

**Список литературы**

1. Коваленко, Г. Теория строения скрытых систем. [Электронный ресурс]. — Режим доступа: https://github.com/number571/gopeer/blob/master/hiddensystems.pdf (дата обращения: 12.01.2022).

1. Под сундуками понимается криптографическая идентификация, где открытый сундук - это публичный ключ, а ключ от сундука - это закрытый ключ. [↑](#footnote-ref-2)