УДК 004.738.2

студентка О.И. Авчинникова, д.т.н., проф. Т.В. Бабенко
ГВУЗ «Национальный горный университет»

ОБМЕН СООБЩЕНИЯМИ В МИКС-СЕТЯХ

Рассмотрена идея Д.Чаума организации анонимной микс-сети с пересылкой сообщений через каскад миксов (передаточных узлов) и последовательным шифрованием всех промежуточных результатов. Описаны задачи, решаемые миксами в ходе обеспечения анонимности связи, обговариваются проблемы ее безопасности.

Анонимные сети – это компьютерные сети, созданные для достижения анонимности в сети Интернет и работающие поверх глобальной сети. Среди их многочисленных представителей можно выделить Freenet, TOR, Invisible Internet Project, Mixminion и др.

Наибольшее влияние на развитие анонимных коммуникаций оказала идея известного голландского криптографа Дэвида Чаума о микс-сетях, разработанная еще в 1981 году [1,2]. В предложенном им способе организации сети анонимность достигается путем пересылки сообщения через каскад передаточных узлов, называемых микс-узлами (миксам). Каждый микс-узел решает две основные задачи. Первая – это обеспечение побитовой неразличимости сообщений, чтобы на выходе из узла нападающий не смог идентифицировать отслеживаемое им сообщение по его содержимому. Для этого все входящие сообщения приводятся к одному размеру (короткие сообщения дополняются случайными данными) и шифруются с помощью какой-либо асимметричной криптосистемы, например RSA. Вторая задача – перемешать поток сообщений, чтобы нападающий не мог сопоставить время входа сообщения в узел и время выхода из него и на основе этой информации понять, какое именно сообщение соответствует искомому. Для этого узел некоторое время накапливает входящие сообщения, перемешивает их и отправляет далее в лексикографическом порядке.

Чтобы передать сообщение M абоненту сети с адресом A через n миксов, отправитель должен:

1) с помощью асимметричной криптосистемы, используя открытый ключ получателя K_A, зашифровать сообщение, соединенное со строкой случайных битов R_0, т.е. вычислить $K_A(R_0, M)$;

2) соединив случайную последовательность R_1, значение $K_A(R_0, M)$ и адрес получателя, зашифровать все на открытом ключе K_1 первого микса: $K_1(R_1, K_A(R_0, M), A)$;

3) последовательно зашифровать результат, полученный на шаге 2, с помощью ключей последующих миксов, участвующих в передаче сообщения:

$$K_n(R_n, K_{n-1}(R_{n-1}, \cdots K_2(R_2, K_1(R_1, K_A(R_0, M), A))\cdots)).$$

В таком виде сообщение готово к передаче по сети.

Когда шифротекст поступает на вход микса, он дешифрует его с помощью своего закрытого ключа, отбрасывает случайную последовательность R_1 и передает оставшуюся часть следующему узлу. Чтобы гарантировать, что никакое сообщение не будет обработано повторно, и не сохранять информацию о прежде обработанных узлом сообщениях, предлагается в каждую случайную последовательность R_i вводить уникальный маркер, наподобие метки времени, действительной только для определенного сообщения.

Метод, описанный выше, позволяет абоненту сети X посылать сообщения абоненту Y, причем даже при неотслеживаемом адресе, абонент Y может ответить на это сообщение. Для этого к отправляемому сообщению добавляется обратный адрес отправителя X. Подготовленный к передаче обратный адрес абонента X должен иметь вид $K_1(R_1, A_x), K_x$, где A_X – его реальный адрес; K_x – выбранный для данного случая открытый ключ; R_1 – случайная последовательность; K_1 – открытый ключ микс-узла.

Пример использования участником Y обратного адреса X:

1) на вход первого микса подается

$$K_1\ R_1, K_2\ R_2, \ldots K_{n-1}\ R_{n-1}, K_n\ R_n, A_x\ \ldots\ , K_x\ R_0, M\ ;$$

2) микс дешифрует сообщение и обнаруженную последовательность R_1 использует как ключ, чтобы повторно зашифровать часть сообщения

$$K_x \; R_0, M \; : K_2 \; R_2, \ldots K_{n-1} \; R_{n-1}, K_n \; R_n, A_x \; \ldots, R_1 \; K_x \; R_0, M \; ;$$

3) на выходе последнего $(n-1)$ микса появится

$$A_x, R_n \; R_{n-1} \ldots R_2 \; R_1 \; K_x \; R_0, M \; \ldots .$$

Только адресат X может расшифровать окончательный результат, поскольку именно им были созданы случайные последовательности $R_1 - R_n$ и ключ K_x.

Непрослеживаемые обратные адреса позволяют реализовать передачу заказных писем, так как отправителю анонимного письма может быть предоставлена квитанция, свидетельствующая о том, что письмо появилось на выходе заключительного микс-узла неповрежденным. Для этого вложенный в сообщение адрес получателя расширяется непрослеживаемым обратным адресом отправителя. Когда этот адрес появляется на выходе заключительного микс-узла, он используется им, чтобы передать отправителю подписанную квитанцию, содержащую посланное им сообщение.

Хотя данная система и предоставляет довольно сильную степень анонимности, она не обеспечивает идеальную защиту абонентов от всех возможных атак, например, атаки маркировки, атаки по времени и др.

Перечень литературы:

1. David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 4(2), February 1982.

2. Mix network. http://ru.wikipedia.org/wiki/Анонимные_сети