Реализация симплексных каналов в распределенных системах на основе схемы предварительного распределения ключей Блома

С.В. Белим
belimsv@omsu.ru

С.Ю. Белим
sbelim@mail.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация

В статье рассмотрена возможность использования схемы предварительного распределения ключей Блома для реализации симплексных каналов в распределенных системах. Модификация схемы Блома состоит в использовании асимметричной функции от трех переменных для формирования ключевых материалов. Предложенная схема не приводит к увеличению объема ключевых материалов. Трудоемкость вычисления парных ключей возрастает.

Введение

Схемы предварительного распределения ключей используются для организации взаимодействия пользователей сети по защищенным каналам связи. Основная идея состоит в том, что каждый пользователь получает набор ключевых материалов, на основании которых он может вычислить общий ключ шифрования с любым другим пользователем системы, используя открытую информацию.

Схема предварительного распределения ключей Блома основана на модели взаимодействия «каждый с каждым». Однако такой подход оправдан только в сетях с доверенными пользователями. В современных глобальных сетях все большее распространение получает подход, в котором вводится ограничение на полномочия отдельно взятых пользователей. Причем ограничения могут быть связаны как с действиями пользователя в сети в целом, так и с ограничением его доступа к ресурсам. Решение данных задач возможно несколькими способами. Один из подходов получил название ID-based криптографии [1].

На сегодняшний день задачи ID-based криптографии решаются с помощью ассиметричных алгоритмов шифрования. Основная идея состоит в выработке ключевой информации на основе идентификаторов [1] или атрибутов пользователя [2, 3, 4]. Основное направление развития ID-based криптографии состоит в развитии подхода, позволяющего связываться с любым абонентом сети только на основе открытой информации. При этом каждый пользователь сети должен получить некоторый сертификат от удостоверяющего центра. Во всех работах, опубликованных к настоящему времени решаются задачи отправки зашифрованных сообщений и электронной цифровой подписи с помощью криптографических алгоритмов с открытым ключом. Основным недостатком данного подхода является общая проблема использования ассиметричной криптографии - трудоемкость вычислений, приводящая к временным задержкам. В связи с чем актуальной является проблема разработки алгоритмов ID-based криптографии, основанной на использовании многочленов.

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2017 (DMS-2017), Omsk, Russia, October 2017, published at http://ceur-ws.org

Следует также учесть критерии, которым должна удовлетворять криптосистема на основе атрибутов, сформулированные в работе [5]:

K1: *Конфиденциальность данных.*

Данные должны быть зашифрованы владельцем перед отправкой их в облако. Неавторизованный участник, включая облако не могут узнать о данных, которые были зашифрованы.

K2: *Детальный контроля доступа.*

В группе пользователей система предоставляет различные правила доступа для каждого отдельного участника группы. Таким образом, пользователи, которые находятся в одной группе могут иметь различные правила доступа к данным.

K3: *Масштабируемость.*

Число зарегистрированных пользователей не должно влиять на производительность системы.

K4: *Контроль действий.*

Недопустима передача атрибутов секретного ключа авторизованного пользователя другим лицам.

K5: *Отзыв прав пользователя.*

Если пользователь выходит из системы, то система может отозвать права данного пользователя. Пользователь, чьи права были отозваны, уже не сможет получить доступ к данным.

K6: *Невозможность сговора.*

Пользователи не могут объединять свои атрибуты, чтобы расшифровать данные, поскольку каждый атрибут связан с многочленом или случайным числом. Таким образом, пользователи не могут вступать в сговор друг с другом.

Также распределение ключей с ограничением на взаимодействие может быть реализовано с помощью хэш-функций [6].

Другой подход основан на модификации схем предварительного распределения ключей. В работе [7] предложена модификация схемы Блома, позволяющая реализовать запрет на отдельные каналы обмена информацией между пользователями. В статьях [8, 9] аналогичная задача решена на основе KDP-схемы предварительного распределения ключей. Однако в обоих случаях запрещен или разрешен полный обмен информацией между двумя пользователями. Тогда как в реальных системах актуальна проблема разграничения доступа к ресурсам исходя из его типа. Таким образом, актуальной является задача модификации схем предварительного распределения ключей, учитывающая направление информационных потоков.

Целью данной статьи является разработка схемы предварительного распределения ключей для системы с учетом типов доступов.

1 Постановка задачи

Рассмотрим систему с двумя базовыми типами доступа: чтения (r) и записи (w). При инициализации канала обмена информацией необходимо следить в каком направлении будут передаваться данные. Таким образом все каналы должны быть симплексными. Введем переменную p, показывающую направление передачи данных. Если пользователь u отправляет запрос на открытие канала по чтению, то есть получению информации, то $s = -1$. Если пользователь открывает канал по записи, то есть передаче информации, то $s = 1$.

В схеме предварительного распределения ключей каждому пользователю по защищенному каналу выдаются некоторые ключевые материалы, на основании которых с использованием открытой информации может быть сформирован общий ключ. В нашем случае симплексных каналов для пары пользователей u_i и u_j должны формироваться два ключа: k_{ij} – ключ для передачи информации от пользователя u_i пользователю u_j, k_{ji} – ключ для передачи информации от пользователя u_j пользователю u_i. В случае обращения пользователя u_i для чтения информации к пользователю u_j или обращения пользователя u_j к пользователю u_i для записи используется ключ k_{ji}. В случае обращения пользователя u_j для чтения информации к пользователю u_i или обращения пользователя u_i к пользователю u_j для записи используется ключ k_{ij}. Потребуем, чтобы запрещенные каналы передачи информации имели нулевой парный ключ, а разрешенные – ненулевой. Схему предварительного распределения ключей, удовлетворяющую данным условиям, будем называть симплексной.

2 Алгоритм предварительного распределения ключей

Реализуем мандатную схему предварительного распределения ключей на базе хорошо известной схемы Блома, проведя ее модификацию.

В схеме предварительного распределения ключей Блома на сервере генерируется симметрический многочлен от двух переменных $f(x,y)$ над полем по модулю p. Каждому пользователю u_i сопоставляется некоторое число r_i. Далее для каждого пользователя формируются многочлены от одного переменного $g_i(x) = f(x, r_i)$. Данные многочлены передаются по защищенным каналам пользователям и хранятся в секрете. При необходимости выработать общий ключ с пользователем u_j пользователь u_i извлекает из открытой базы элемент r_j и вычисляет значение $k_{ij} = g_i(r_j)$. Аналогичным образом поступает пользователь u_j, вычисляя $k_{ji} = g_j(r_i)$. Симметричность многочлена $f(x,y)$ обеспечивает выполнение равенства $k_{ij} = k_{ji}$.

Для реализации симплексной схемы предварительного распределения ключей необходимо учесть направления информационных потоков. Для учета направления потоков будем генерировать на сервере многочлен от трех переменных $F(x,y,s)$ над полем по модулю p, в котором переменная s может принимать два значения (+1 или -1) и определяет направление потока информации. Каждому пользователю u_i как и в обычной схеме Блома сопоставим некоторое число r_i, которое хранится в открытом виде и защищено от изменений. Для каждого пользователя сервер распределения ключей формирует многочлен $G_i(x,s) = F(x, r_i, s)$ и передает его по защищенному каналу. Многочлен $F(x,y,s)$ должен иметь такой вид, чтобы на основе функции $G_i(x,s)$ и чисел r_i для разрешенного обмена информации генерировался ключ $k_{ij} \neq 0$, а для запрещенных каналов $k_{ij} = 0$. При этом оба участника обмена должны вырабатывать одинаковый ключ на основе собственных секретных ключевых материалов и открытой информации друг о друге.

Рассмотрим два вида взаимодействия пользователей при передаче информации. Во-первых, остановимся на случае, в котором пользователь u_i инициирует получение информации от пользователя u_j , то есть обращается к нему с запросом на чтение. Пользователь u_j отправляет информацию предварительно зашифровав ее ключом

$$k_{ji} = G_j(r_i, 1) = F(r_i, r_j, 1).$$

Параметр $s = 1$, так как для u_j информационный поток исходящий. Пользователь u_i получает сообщение и расшифровывает его тем же ключом, вычисляемым на основе своих ключевых материалов:

$$k_{ji} = G_i(r_j, -1) = F(r_j, r_i, -1).$$

Параметр $s = -1$, так как для u_i информационный поток входящий.

Второй случай состоит в том, что пользователь u_i инициирует отправку информации пользователю u_j , то есть обращается к нему с запросом на запись. Пользователь u_i отправляет информацию предварительно зашифровав ее ключом

$$k_{ij} = G_i(r_j, 1) = F(r_j, r_i, 1).$$

Параметр $s = 1$, так как для u_i информационный поток исходящий. Пользователь u_j получает сообщение и расшифровывает его тем же ключом, вычисляемым на основе своих ключевых материалов:

$$k_{ij} = G_j(r_i, -1) = F(r_j, r_i, -1).$$

Параметр $s = -1$, так как для u_j информационный поток входящий.

Из рассмотрения этих двух случаев вытекает три требования, накладываемых на функцию $F(x,y,s)$:

1. $F(x,y,1) \neq F(y,x,1)$,
2. $F(x,y,-1) \neq F(y,x,-1)$,
3. $F(x,y,1) = F(y,x,-1)$.

Первые два требования сводятся к несимметричности функции $F(x,y,s)$ к перестановке первых двух аргументов при любом значении третьего аргумента. Для криптографической стойкости также необходимо потребовать, чтобы вычисление $F(x,y,s)$ было невозможно на основании известного значения $F(y,x,s)$.

Будем задавать $F(y,x,s)$ в следующем виде:

$$F(x,y,s) = \begin{cases} x^{h(y)}, \ if \ s = 1, \\ y^{h(x)}, \ if \ s = -1. \end{cases}$$

Здесь $h(x)$ некоторый многочлен от одной переменной. Очевидно, что данная функция удовлетворяет всем трем требованиям, перечисленным выше. Криптографическая стойкость данной функции обеспечивается трудоемкостью задач линейного логарифмирования и вычисления корня в конечных полях.

Рассмотрим схему распределения ключей на основе данной функции. Каждому пользователю передаются ключевые материалы, необходимые для вычисления функции от двух переменных:

$$G_i(x,s) = F(x,r_i,s) = \begin{cases} x^{h(r_i)}, \ if \ s=1, \\ r_i^{h(x)}, \ if \ s=-1. \end{cases}$$

Для вычисления значений функции $G_i(x,1)$ пользователю u_i необходимо знать одно число $h_i = h(r_i)$, которое сервер передает ему по защищенному каналу.

Рассмотрим более сложный случай вычисления $G_i(x,-1)$. Пусть $h(x)$ представляет собой многочлен степени m:

$$h(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0.$$

Тогда значение функции:

$$\begin{aligned} G_i(x,-1) &= r_i^{a_m x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0} = \\ &= (r_i^{a_m})^{x^m} \left(r_i^{a_{m-1}}\right)^{x^{m-1}} ... \left(r_i^{a_1}\right)^{x} \left(r_i^{a_0}\right) = \\ &= \left(b_m^{(i)}\right)^{x^m} \cdot \left(b_{m-1}^{(i)}\right)^{x^{m-1}} \cdot ... \cdot \left(b_1^{(i)}\right)^{x} \cdot b_0^{(i)}, \end{aligned}$$

где $b_k^{(i)} = r_i^{a_k}$ $(k = 1, ..., m)$.

Таким образом сервер в качестве ключевых материалов высылает пользователю u_i по защищенному каналу вектор:

$$g_i = \left(h_i, b_m^{(i)}, b_{m-1}^{(i)}, ..., b_1^{(i)}, b_0^{(i)}\right).$$

Этих данных достаточно для вычисления значений функции. При этом, задача определения коэффициентов многочлена $h(x)$ по координатам вектора g_i сводится к дискретному логарифмированию.

Следует отметить, что данная схема незначительно увеличивает объем ключевых материалов, хранящихся у пользователя в сравнении с традиционной схемой Блома – добавляется одно число. Однако процедура нахождения парного ключа значительно более трудоемкая, так как требует возведения в степень больших чисел.

Заключение

Таким образом, модификация схемы Блома позволяет организовать обмен сообщениями по симплексным каналам. При этом приходится отказаться от идеи использования симметрических многочленов. Такой отказ обусловлен тем, что сам обмен информацией становится несимметричным.

Список литературы

[1] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. *Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science*, 7:47–53, 1984.

[2] A. Sahai, B. Waters. Fuzzy Identity-Based Encryption. *Cryptology ePrint Archive*, Report 2004/086, 2004.

[3] D. Boneh, M. Franklin. Identity-based encryption from the weil pairing. *In CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, 213–229, 2001.

[4] C. Cocks. An identity based encryption scheme based on quadratic residues. *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, 360–363, 2001.

[5] C.-C. Lee, P.-S. Chung, M.-S. Hwang. A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments. *International Journal of Network Security*, 15(4):231–240, 2013.

[6] S.V. Belim, N.F. Bogachenko. Distribution of Cryptographic Keys in Systems with a Hierarchy of Objects. *Automatic Control and Computer Sciences*, 50(8):773–776, 2016.

[7] S.V. Belim, S.Yu. Belim, S.Yu. Polyakov. The implementanion of discretionary access separation using a modified Blom's scheme of key distribution. *Information Security Problems. Computer Systems*, 3:72–76, 2015.

[8] S.V. Belim, S.Yu. Belim. KDP Scheme of Preliminary Key Distribution in Discretionary Security Policy. *Automatic Control and Computer Sciences*, 50(8):777–786, 2016.

[9] S.V. Belim, S.Yu. Belim. The VPN Implementation on Base of the KDP-Scheme. *CEUR Workshop Proceedings*, 1732, 2016. URL: `http://ceur-ws.org/Vol-1732/paper3.pdf`.

Realization of Simplex Channels in the Distributed Systems on the Basis of the Blom's Preliminary Distribution of Keys Scheme

Sergey V. Belim, Svetlana Yu. Belim

In article the possibility of use of the Blom's keys preliminary distribution scheme for simplex channels realization in the distributed systems is considered. The Blom's schem modification includes use asymmetrical function of three variables for key materials calculation. The suggested scheme doesn't increase the key materials volume. The calculation's difficulty for pair keys increases.