Модификация схемы предварительного распределения ключей Блома с учетом запрещенных каналов

С.В. Белим
belimsv@omsu.ru

С.Ю. Белим
sbelim@mail.ru

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

Аннотация

В статье рассмотрены распределенные системы с запрещенными каналами обмена информацией. Предложена модификация схемы Блома, позволяющая реализовать запрет на обмен информацией между заданными пользователями. Запрет реализуется с помощью обнуления парных ключей шифрования для запрещенных каналов. Многочлен схемы Блома строится на основе элементарных симметрических многочленов. Предложена реализация разработанной схемы для построения VPN.

Введение

Под попарной ключевой схемой предварительного распределения ключей принято понимать схему, в которой один ключ ассоциирован ровно с двумя узлами. В примитивной схеме каждый узел хранит $(n-1)$ ключ для каждого узла сети. Эта схема устойчива к атакам злоумышленника, но обладает плохой масштабируемостью и требует больших ресурсов памяти для хранения ключевых материалов.

Все схемы предварительного распределения ключей подразумевают возможность связи каждого абонента сети с каждым. Тогда как в реальных системах существуют политики безопасности, ограничивающие возможности взаимодействия отдельных пар пользователей. Базовой политикой безопасности является дискреционное разделение доступа, заданное в виде матрицы доступов, определяющих разрешенные каналы передачи информации.

В работе [1] предложена схема предварительного распределения ключей (так называемая схема Блома), которая позволяет каждой паре узлов вычислить секретный ключ на основе ключевых материалов, которые требуют значительно меньше памяти чем примитивная попарная схема. Схема Блома устойчива, если под угрозу поставлено не больше узлов (λ - безопасность). Размер памяти для хранения ключевых материалов существенно зависит от значения . При необходимости построения сети с высоким уровнем защищенности схема Блома также характеризуется плохой масштабируемостью. Схема Блома [1, 2] получила распространение при реализации защищенной передачи информации в компьютерных сетях с большим числом абонентов. В последние годы появилось достаточно много различных модификаций схемы Блома, связанных преимущественно с беспроводными сетями [3, 4, 5, 6, 7, 8]. Ряд работ был направлен на реализацию схемы Блома с ограничениями, связанными с топологией сети, коррекцией ошибок и др. [9, 10, 11, 12]. Модификация KDP-схемы предварительного распределения ключей с учетом запрещенных каналов передачи информации представлена в работах [14, 15]. Схема распределения ключей с использованием хеш-функций в системах с иерархией объектов описана в статье [16].

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

1 Постановка задачи и схема Блома

Пусть в распределенной системе имеется n узлов. Необходимо обеспечить защиту каналов обмена информации для каждой пары узлов и, кроме того, запретить обмен информации некоторым парам узлов. В начальной постановке задачи будем считать, что все каналы информации двухсторонние, то есть если соединение установлено, то оба узла могут получать и отправлять информацию беспрепятственно. Данная задача может быть изображена с помощью матрицы доступов, в ячейках которой расположены ключи для реализации криптографического протокола, если связь разрешена, и нули если канал связи запрещен политикой безопасности. Поставим задачу распределения между узлами некоторой информации, называемой ключевыми материалами, на основе которых каждый узел может либо вычислить необходимый ключ шифрования, либо определить, что данный канал ему запрещен. Пусть подсистема безопасности на каждом узле системы реализована, таким образом, что при нулевом значении ключа следует запрет на установление соединения. В дальнейшем будем считать, что все ключи имеют длину m бит.

Схема Блома предварительного распределения ключей основывается на вычислении значений симметрического многочлена $f(x, y)$ степени $2l$ над кольцом вычетов по модулю M. Если число абонентов n, то $l < n$. Многочлен $f(x, y)$ хранится в секрете на сервере. Каждому участнику сопоставляется число r_i (i=1,...,n). Таблица чисел r_i хранится на сервере в открытом виде. Сервер передаёт каждому абоненту i по защищенному каналу многочлен $g_i(x) = f(x, r_i)$. Общий ключ связи двух абонентов i и j формируется путем подстановки числа r_j в многочлен $g_i(x)$ i-ым абонентом ($k_{ij} = g_i(r_j)$) и подстановкой числа r_i в многочлен $g_j(x)$ j-ым абонентом ($k_{ji} = g_j(r_i)$). Так как многочлен $f(x, y)$ симметричен, то будет выполняться равенство $k_{ij} = k_{ji}$.

Под компроментацией схемы Блома понимается возможность по известному набору ключей получить остальные неизвестные ключи. Как показано в работе [13] схема Блома является устойчивой к компроментации l ключей.

2 Модифицированная схема Блома с запрещенными каналами

Осуществим модификацию схемы Блома таким образом, чтобы она позволяла реализовывать запреты на создание некоторых каналов связи. Пусть в системе наложены ограничения на возможность взаимодействия абонентов. То есть существуют пары абонентов, для которых запрещен обмен информацией. Потребуем, чтобы для разрешенных пар абонентов (i, j) схема генерировала ключ обмена информацией $k_{ij} \neq 0$, для запрещенных пар абонентов $k_{ij} = 0$. Если такая схема будет построена, то далее задача решается техническими средствами с помощью запрета шифрования нулевым ключом.

Будем считать, что в системе имеется n абонентов и задан список пар номеров абонентов L, для которых запрещен обмен информацией. Построим симметричный полином $F(x, y)$, который будет храниться в секрете на сервере и иметь вид: $F(x, y) = d(x, y)f(x, y)$. Здесь $f(x, y)$ (как и в обычной схеме Блома) является симметричным многочленом степени $2l$. Многочлен $f(x, y)$ необходим для формирования ключей обмена информацией. Он обеспечивает стойкость к компрометации ключей. Многочлен d(x,y) также является симметричным и обеспечивает обнуление ключей шифрования для запрещенных пар абонентов. Наложим требование $d(r_i, r_j) = d(r_j, r_i) = 0$, если $(i, j) \in L$, и $d(r_i, r_j) = d(r_j, r_i) \neq 0$, если $(i, j) \notin L$.

Будем искать многочлен d(x,y) в виде произведения:

$$d(x, y) = \prod_{(i,j)\in L} d_{ij}(x, y),$$

где функция $d_{ij}(x, y) = 0$ только при $((x = r_i) \wedge (y = r_j)) \vee ((x = r_j) \wedge (y = r_i))$. Задача сводится к поиску функций $d_{ij}(x, y)$. Очевидно, что для симметричности функции $d(x, y)$ достаточно, чтобы все $d_{ij}(x, y)$ были симметричными. Исходя из того, что все функции $d_{ij}(x, y)$ симметричные следует, что они должны выражаться через элементарные симметричные многочлены:

$$\sigma_1(x, y) = x + y, \quad \sigma_2(x, y) = xy.$$

Следовательно, для функции $d_{ij}(x, y)$, имеющей два корня, можем записать:

$$d_{ij}(\sigma_1, \sigma_2) = (\sigma_1(x, y) - \sigma_1(r_1, r_2))^2 + (\sigma_2(x, y) - \sigma_2(r_1, r_2))^2,$$

или

$$d_{ij}(x, y) = (x + y - r_i - r_j)^2 + (xy - r_i r_j)^2.$$

Функция $d(x,y)$ будет иметь вид:

$$d(x,y) = \prod_{(i,j)\in L} ((x+y-r_i-r_j)^2 + (xy - r_i r_j)^2)$$

Далее организация распределения ключей осуществляется также как в обычной схеме Блома с заменой функции $f(x,y)$ на функцию $F(x,y)$. Легко показать, что при наличии s запрещенных каналов

$$deg\ d(x,y) = 4s.$$

Рассмотрим вопрос компрометации предложенной схемы.

Лемма 1. *Пусть в модифицированной схеме Блома с запрещенными каналами степень многочлена $deg\ f(x,y) = 2l$, а количество запрещенных каналов равно s, тогда схема устойчива к компрометации $l + 2s$ ключевых материалов.*

Доказательство. Как и для обычной схемы Блома для компрометации ключей необходимо вычислить все коэффициенты многочлена $F(x,y)$. Очевидно, что наличие корней многочлена не создает дополнительной утечки информации, так как злоумышленнику неизвестны запрещенные каналы. Степень многочлена

$$deg\ F(x,y) = deg\ f(x,y) + deg\ d(x,y) = 2l + 4s.$$

Согласно теореме для обычной схемы Блома [1] система устойчива к компрометации количества ключевых материалов равному половине степени многочлена:

$$\frac{1}{2} deg\ F(x,y) = l + 2s.$$

■

Также важным является вопрос компрометации запрещенных каналов. Необходимо понять какими минимальными данными должен обладать злоумышленник для восстановления списка запрещенных каналов.

Лемма 2. *Пусть в модифицированной схеме Блома с запрещенными каналами степень многочлена $deg\ f(x,y) = 2l$, а количество запрещенных каналов равно s, тогда для компрометации списка запрещенных каналов, необходима компрометация $l + 2s$ ключевых материалов.*

Доказательство. Для компрометации списка запрещенных каналов, необходимо найти все корни многочлена $F(x,y)$. Для этого надо вычислить все его коэффициенты. Данная задача равносильна полной компрометации всей схемы. Следовательно, согласно утверждению 1, требуется утечка $l + 2s$ ключевых материалов. ■

Классическая матрица доступов разграничивает не только сам факт доступа, но и вид доступа. Предложенная выше схема не обладает данным свойством. Задача разграничения по видам доступа с помощью криптографических методов может быть решена путем введения ключа шифрования для каждого вида доступа. Данный подход может быть реализован с помощью предложенной схемы, однако следует учесть, что это приведет к значительному росту степени многочлена $F(x,y)$. С другой стороны общее количество ключей, которое придется хранить при разграничении доступа по видам доступа также велико и предложенная схема все-равно дает выигрыш.

3 Пример построения модифицированной схемы Блома с запрещенными каналами

Рассмотрим пример построения схемы Блома с запрещенными каналами. Пусть задана матрица доступов для четырех участников U_1, U_2, U_3, U_4.

	U_1	U_2	U_3	U_4
U_1		1	1	0
U_2	1		0	1
U_3	1	0		1
U_4	0	1	1	

В матрице доступов 0 означает запрет на обмен информацией, 1 – обмен разрешен. Таким образом, в приведенной системе два запрещенных канала.

Для построения симметрического многочлена $f(x,y)$ выберем $l=1$, тогда

$$degf(x,y)=2l=2.$$

Для упрощения расчетов будем проводить вычисления над кольцом Z_7. Коэффициенты многочлена $f(x,y)$ выбираются произвольным образом и держатся в секрете на сервере. Пусть

$$f(x,y)=3+2x+2y+4xy+5x^2+5y^2\ (mod\ 7).$$

Выберем также произвольно значения хранящихся открыто чисел r_i (i=1,...,4):

$$r_1=2,\ r_2=5,\ r_3=3,\ r_4=4.$$

Построим симметричный многочлен $d(x,y)$, реализующий запрещенные каналы обмена информацией между парами пользователей $p_1=(U_2,U_3)$, $p_2=(U_1,U_4)$. Найдем значения элементарных многочленов от двух переменных для пар p_1 и p_2:

$$\sigma_1(p_1)=\sigma_1(r_2,r_3)=r2+r3\ (mod\ 7)=1,$$
$$\sigma_2(p_1)=\sigma_2(r_2,r_3)=r2\cdot r3\ (mod\ 7)=1,$$
$$\sigma_1(p_2)=\sigma_1(r_1,r_4)=r1+r4\ (mod\ 7)=6,$$
$$\sigma_2(p_2)=\sigma_2(r_1,r_4)=r1\cdot r4\ (mod\ 7)=1.$$

Следовательно

$$d_1(x,y)=(\sigma_1(x,y)-\sigma_1(r_2,r_3))^2+(\sigma_2(x,y)-\sigma_2(r_2,r_3))^2=x^2y^2+x^2+y^2+5x+5y+2\ (mod\ 7),$$
$$d_2(x,y)=(\sigma_1(x,y)-\sigma_1(r_1,r_4))^2+(\sigma_2(x,y)-\sigma_2(r_1,r_4))^2=x^2y^2+x^2+y^2+2x+2y+2\ (mod\ 7),$$
$$d(x,y)=d_1(x,y)\cdot d_2(x,y).$$
$$F(x,y)=d(x,y)\cdot f(x,y)=(x^2y^2+x^2+y^2+5x+5y+2)\cdot(x^2y^2+x^2+y^2+2x+2y+2)$$
$$\cdot(3+2x+2y+4xy+5x^2+5y^2)\ (mod\ 7).$$

Найдем ключевые материалы для каждого из участников обмена информацией.

$$g_1(x)=F(x,r_1)=6x^6+5x^5+3x^4+4x^3+3x^2+6x+1,$$
$$g_2(x)=F(x,r_2)=6x^6+4x^5+6x^4+3x^3+4x^2+2x+2,$$
$$g_3(x)=F(x,r_3)=3x^6+5x^4+6x^3+6x+5,$$
$$g_4(x)=F(x,r_4)=3x^6+x^5+2x^4+4x^3+3x^2+4x.$$

Для обмена информацией участники будут вырабатывать парные ключи по правилу

$$k_{i,j}=g_i(r_j).$$

Для рассматриваемого примера матрица ключей будет иметь вид:

	U_1	U_2	U_3	U_4
U_1		3	1	0
U_2	3		0	3
U_3	1	0		2
U_4	0	3	2	

Как видим, для запрещенных каналов ключи равны нулю, то есть обмен информацией невозможен. Следует отметить, что для малого количества участников обмена и большого количества запрещенных каналов схема не дает выигрыш в использовании памяти. В рассматриваемом примере вектор из коэффициентов многочлена $g_i(x)$ для каждого из участников содержит 7 координат, тогда как без использования схемы распределения ключей необходимо хранить всего три ключа. Однако это проблема снимается при большом количестве участников обмена.

4 Выводы

В заключение выделим основные результаты. Предложенная модификация схемы Блома позволяет реализовать дискреционное разделение доступа в распределенных системах методами симметричной криптографии. При этом учет запрещенных каналов в рамках схемы Блома приводит к росту объема ключевых материалов, которые необходимо хранить на каждом из узлов сети. Также можно отметить, что учет запрещенных каналов в рамках схемы Блома не приводит к дополнительным утечкам информации по сравнению с традиционной схемой Блома.

Список литературы

[1] R. Blom. An optimal class of symmetric key generation systems. *Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques*, 335–338, 1985.

[2] A. Menezes, P. van Oorschot, S. Vanstone. *Handbook of Applied Cryptography.* CRC-Press, 1996.

[3] W. Du, J. Deng, Y. Han, P. Varshney. A pairwise key pre distribution scheme for wireless sensor networks. *In Proceedings of the Tenth ACM Conference on Computer and Communications Security (CCS 2003)*, 42–51, 2003.

[4] Du W., J. Deng, Y.S. Han, P. Varshney, J. Katz, A. Khalili. A pairwise key pre-distribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(2):228–258, 2005.

[5] D. Liu, P. Ning, R. Li. Establishing pairwise keys in distributed sensor networks. *ACM Trans. Inf Syst. Secur.*, 8:41–77, 2005.

[6] A. Parakh, S. Kak. Efficient key management in sensor networks. *Proceedings IEEE GLOBECOM workshops (GC workshops)*, 1539–1544, 2010.

[7] A. Parakh, S. Kak. Matrix based key agreement algorithms for sensor networks. *Proceedings IEEE 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS)*, 1–3, 2011.

[8] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar. Spins: Security protocols for sensor networks. *Wireless Networks Journal (WINE)*, 8:521–534, 2002.

[9] S. Basagni, K. Herrin, D. Bruschi, E. Rosti. Secure pebblenets. *Proceedings of the 2001 ACM International Symposium on Mobile AdHoc Networking and Computing*, MobiHoc, 156–163, 2001.

[10] F.J. MacWilliams, N.J.A. Sloane. *The Theory of Error-Correcting Codes.* New York, Elsevier Science Publishing Company, Inc., 1977.

[11] A. Parakh, S. Kak. Online data storage using implicit security. *Information Sciences*, 179:3323–3331, 2009.

[12] A. Parakh, S. Kak. Space efficient secret sharing for implicit data security. *Information Sciences*, 181:335–341, 2011.

[13] A.V. Cheremushkin. Combinatorial-geometric approaches to design of pre-shared key distribution patterns (review). *Prikl. Diskretn. Mat.*, 1(1):55–63, 2008.

[14] S.V. Belim, S.Yu. Belim. KDP Scheme of Preliminary Key Distribution in Discretionary Security Policy. *Automatic Control and Computer Sciences*, 50(8):773–776, 2016.

[15] 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`.

[16] S.V. Belim, N.F. Bogachenko. Distribution of Cryptographic Keys in Systems with a Hierarchy of Objects. *Automatic Control and Computer Sciences*, 50(8):777–786, 2016.

The Blom's Scheme Modification for Discretionary Access Control

Sergey V. Belim, Svetlana Yu. Belim

In article the distributed systems with the forbidden channels of information exchange are considered. The Blom's scheme modification, allowing to realize the ban on exchange of information between users is offered. The ban is implemented by means of zeroing of pair keys for the forbidden channels. The Blom's scheme polynomial is constructed on the basis of elementary symmetric polynomials. Implementation of the developed scheme for creation of VPN is suggested.