О применении политики разграничения доступа к предварительному распределению ключей на основе векторной схемы разделения секрета

С.В. Усов
raintower@mail.ru

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

Аннотация

Традиционные алгоритмы предварительного распределения ключей игнорируют политику безопасности системы. В данной работе удалось предложить основанный на схеме Блэкли подход к распределению ключей, нивелирующий этот недостаток. В предложенной схеме получение общего ключа возможно лишь для пар участников схемы, обмен информацией между которыми разрешен политикой безопасности. При этом учитывается направление потока данных и тип доступа, как, например, на чтение и на запись.

1 Схемы предварительного распределения ключей, учитывающие ограничения на доступ, предопределенные политикой безопасности

Схемы предварительного распределения ключей и политики разграничения доступа принято рассматривать независимо друг от друга. Все схемы предварительного распределения ключей подразумевают возможность связи каждого абонента сети с каждым. Однако в реальных системах существует необходимость согласования между механизмами обеспечения информационной безопасности. Базовой политикой безопасности является дискреционное разделение доступа, заданное в виде матрицы доступов, определяющих разрешенные каналы передачи информации.

Если обмен информацией между двумя выбранными пользователями является нежелательным, необходимо построить схему, в которой выработка общего ключа этими пользователями была бы невозможной. С этой целью в работах [1, 2, 3] были предложены схемы предварительного распределения ключей (в частности, модифицированная схема Блома), учитывающие дискреционную политику безопасности. Однако в представленных алгоритмах выработанный общий ключ подразумевал доступ к симметричному каналу связи между пользователями, то есть обмен информацией происходил в обоих направлениях, что, например, невозможно при применении мандатной политики разграничения доступа. В данной работе мы предложим схему, подходящую для более общего случая.

Пусть в распределенной системе имеется множество $\mathbf{S} = \{s_1 \dots s_N\}$ субъектов (пользователей, участников схемы). Необходимо обеспечить защиту каналов обмена информации для каждой пары субъектов и, кроме того, запретить обмен информации некоторым парам субъектов. Поставим задачу распределения между субъектами некоторой информации, называемой ключевыми материалами, на основе которых каждый субъект может либо вычислить необходимый ключ шифрования, либо определить, что данный канал

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

ему запрещен. Пусть подсистема безопасности для каждого субъекта системы реализована таким образом, что при невозможности вычисления ключа следует запрет на установление соединения.

Учитывая вышесказанное, разумно выделить два класса политик безопасности разной степени общности. Будем называть политику разграничения доступа симметричной, если субъект s_i обладает доступом к субъекту s_j одновременно с тем, что субъект s_j обладает доступом к субъекту s_i. Политику, в которой данное ограничение отсутствует, назовем асимметричной.

Для начала будем считать политику разграничения доступа симметричной.

2 Модификация векторной схемы разделения секрета до схемы предварительного распределения ключей

В схеме Блэкли [4] каждый участник схемы в качестве своей доли секрета получает уравнение $(n-1)$-мерной плоскости в n-мерном пространстве. Все эти гиперплоскости имеют одну общую точку, которая и является хранимым секретом, для получения которого каждый участник схемы должен, очевидно, скомпрометировать свою долю секрета. Мы также будем работать в n-мерном пространстве. Предложим следующую модификацию векторной схемы разделения секрета до схемы предварительного распределения ключей.

Долю секрета пользователя s_i, а в модифицированной схеме – его долю ключевых материалов, составляет множество точек $X(i)$ в k-мерном подпространстве $L(i)$. В открытом доступе хранится m-мерное подпространство $Y(i)$, сопоставленное i-тому пользователю, причем $L(i)$ является подпространством $Y(i)$, то есть $k < m < n$.

Алгоритм выработки общего ключа между i-м и j-м пользователями следующий:
Дано:
1) множество всевозможных ключей $\mathbf{K}$,
2) размерности пространства и подпространств $k < m < n$;
для каждого пользователя s_i:
3) его доля секрета $X(i)$,
4) секретное подпространство $L(i)$,
5) открытое подпространство $Y(i)$,
6) также для каждой пары пользователей s_i и s_j задана ключевая функция $\Phi_{i,j} : \mathbb{R}^{k+m} \to \mathbf{K}^*$, помогающая выработать общий ключ.

Получить: для каждой пары пользователей (s_i, s_j) ключевые множества $K(i,j), K(j,i) \subset \mathbf{K}$, имеющие общий элемент, который и будет являться общим ключом пользователей s_i и s_j, либо установить, что получение таких множеств невозможно (а значит, обмен информацией между s_i и s_j запрещен).

1. Пользователь s_i находит пересечение множеств $L(i)$ и $Y(j)$. Если пересечение пусто, выработка общего ключа невозможна. Это значит, что обмен информации между i-м и j-м пользователями запрещен политикой безопасности.

2. Если $L(i) \cap Y(j)$ содержит непустое множество точек, то пользователь s_i вычисляет определенную функцию $\Phi_{i,j}$ от координат этих точек. Результатом вычисления функции является некоторое множество. Если оно пусто, либо бесконечно, выработка общего ключа невозможна.

3. В противном случае результат вычисления функции $\Phi_{i,j}(X(i) \cap Y(j))$ обозначим через $K(i,j)$.

4. Симметричные действия предпринимает пользователь s_j по отношению к s_i. Его результат обозначим через $K(j,i)$.

5. Пользователи сравнивают результаты. Если $K(i,j) \cap K(j,i) \neq \varnothing$ (если у каждого пользователя получилось некоторое множество результатов, то должен совпадать хотя бы один элемент этих множеств), то элемент из $K(i,j) \cap K(j,i)$ является общим ключом связи между пользователями.

6. Если же результаты не совпадают, то обмен информации между i-м и j-м пользователями запрещен политикой безопасности.

Пример 1. $k = 1$, $X(i) = L(i)$ (прямая), $m = n - 1$. Пользователь s_i ищет множество точек пересечения своей (секретной) прямой и подпространства $Y(j)$ пользователя s_j, которое находится в открытом доступе. С учетом размерностей, возможны четыре варианта:

а) Точек пересечения нет, то есть прямая $X(i)$ параллельна подпространству $Y(j)$. Доступ запрещен.

б) Точек пересечения бесконечно много, то есть прямая $X(i)$ целиком лежит в подпространстве $Y(j)$. Доступ запрещен.

в) Прямая $X(i)$ и подпространство $Y(j)$ пересекаются в единственной точке. Однако прямые $X(i)$ и $X(j)$ не имеют общих точек (скрещиваются). В этом случае точка, полученная пользователем s_i не совпадет с точкой, полученной пользователем s_j. Доступ запрещен.

г) Прямая $X(i)$ и подпространство $Y(j)$ пересекаются в единственной точке. Причем эта точка лежит на $X(j)$. Такая точка пересечения прямых – единственная, поэтому пользователь s_j получит ту же точку. Общим ключом может служить, например, n-я координата точки. Доступ разрешен.

Итак, мы построили схему предварительного распределения ключей с разграничением доступа. Теперь рассмотрим ее недостатки.

Во-первых, если три пользователя A, B и C обладают взаимным доступом, то схема легко компрометируется. Действительно, ведь тогда их прямые лежат в одной двумерной плоскости, а открытые $n-1$-мерные пространства этих пользователей, пересеченные с уравнением общей плоскости, позволяют злоумышленнику получить секрет каждого из пользователей A, B, C. Одним из решений данной проблемы может стать запрет на циклы длины 3 в графе доступов системы, что накладывает существенные ограничения на область применения данной схемы.

Во-вторых, раскрытие секретов только двух участников схемы компрометирует всю схему. Достаточно найти точки пересечения прямых пользователей A и B с прямой третьего участника C, и восстановить его прямую по двум точкам.

Предложим и два способа исправления недостатков.

1. Секретом каждого участника будет k-мерное пространство, а в качестве открытой информации об участнике на сервере будет предоставляться $n - k$-мерное подпространство, причем $n \geq 2k$.

2. Секретом каждого участника будет не прямая, а некоторое множество точек (например, кривая или поверхность), которое легко задается аналитически. Более того, в качестве открытой информации на сервере можно также использовать $n - 1$-мерные поверхности, а не плоскости.

Результатом исправления недостатков может стать, например, следующая модель:

Пример 2. $k = 2$, $X(i)$ – кривая (например, окружность) в плоскости $L(i)$, $m = n - 2$. Пользователь s_i ищет множество точек пересечения своей (секретной) кривой и подпространства $Y(j)$ пользователя s_j, которое находится в открытом доступе. С учетом размерностей, возможны несколько вариантов:

а) Кривая $X(i)$ не пересекается с подпространством $Y(j)$. Доступ запрещен.

б) Кривая $X(i)$ вместе с плоскостью $L(i)$ целиком лежит в подпространстве $Y(j)$. Доступ запрещен.

в) Подпространства $L(i)$ и $Y(j)$ пересекаются по прямой. Однако кривые $X(i)$ и $X(j)$ не имеют общих точек. В этом случае точка, полученная i-м пользователем не совпадет с точкой, полученной j-м пользователем. Доступ запрещен.

г) Подпространства $L(i)$ и $Y(j)$ пересекаются по прямой. Кривая $X(i)$ и подпространство $Y(j)$ пересекаются в единственной точке. Причем эта точка лежит на $X(j)$. Такая точка пересечения прямых – единственная, поэтому пользователь s_j получит ту же точку. Общим ключом может служить, например, n-я координата точки. Доступ разрешен.

д) Подпространства $L(i)$ и $Y(j)$ пересекаются по прямой. Прямая $X(i)$ и подпространство $Y(j)$ пересекаются в нескольких точках. Правило вычисления ключа $K(i, j)$ позволяет определить его точное значение, либо выдает конечный (небольшой) набор возможных значений, которые можно перебрать. Пользователь s_j также смог получить свой конечный набор значений $K(j, i)$, причем $K(i, j) \cap K(j, i) \neq \varnothing$. Пользователям осталось перебрать элементы своих ключевых множеств, чтобы найти общий ключ. Доступ разрешен.

е) Подпространства $L(i)$ и $Y(j)$ пересекаются по прямой. Прямая $X(i)$ и подпространство $Y(j)$ пересекаются в нескольких точках. Правило вычисления ключа $K(i, j)$ не позволяет определить его точное значение, либо выдает большой (бесконечный) набор возможных значений, которые нет возможности перебрать за разумное время. Либо подобная ситуация произошла с пользователем s_j. Доступ запрещен.

Еще несколько вариантов событий, симметричных описанным с точки зрения пользователя s_j, рассматриваются аналогично.

Приведем, наконец, еще один простой пример схемы предварительного распределения ключей, на этот раз с определенными значениями всех множеств и функций.

Пример 3. Пусть n=4, m= 3, k=2. Значения $X(i)$, $L(i)$ и $Y(i)$ для каждого участника схемы ($i = 1 \dots 4$) занесем в таблицу 1. Координаты точек 4-мерного пространства будем обозначать через x, y, z, t.

Таблица 1: Исходные данные к схеме предварительного распределения ключей

i	$Y(i)$	$L(i)$	$X(i)$
1	$\{x = 0\}$	$\{x = 0, y = 0\}$	$\{x^2 + t^2 = 1\} \cap L(1)$
2	$\{y = 0\}$	$\{y = 0, z = 0\}$	$\{-y^2 + t^2 = 1\} \cap L(2)$
3	$\{z = 0\}$	$\{z = 0, t = 0\}$	$\{x^2 + y^2 + t^2 = 1\} \cap L(3)$
3	$\{t = 0\}$	$\{t = 0, x = 0\}$	$\{y^2 + yz = 1\} \cap L(4)$

Теперь для каждой пары участников (s_i, s_j) вычислим и занесем в таблицу 2 пересечения $X(i) \cap Y(j)$.

Таблица 2: Промежуточный этап попытки вычисления общих ключей для каждой пары участников

i, j	1	2	3	4
1		$\{(0, 0, z, \pm 1)\}$	$\{(0, 0, 0, \pm 1)\}$	$\varnothing$
2	$\{(0, 0, 0, \pm 1)\}$		$\{(x, 0, 0, \pm 1)\}$	$\varnothing$
3	$\{(0, \pm 1, 0, 0)\}$	$\{(0, 0, z, \pm 1)\}$		$\{x^2 + y^2 = 1, z = t = 0\}$
3	$\{y^2 + yz = 1, t = x = 0\}$	$\varnothing$	$\{(0, \pm 1, 0, 0)\}$	

Уже на этом этапе становится понятным, что выработка общего ключа для пар участников (s_1, s_4) и (s_2, s_4) невозможна, то есть взаимный доступ этих участников друг к другу запрещен, поскольку пересечения $X(1) \cap Y(4)$ и $X(2) \cap Y(4)$ пусты.

Для построения ключевых множеств $K(i, j)$ остальных пар участников нам потребуется ключевая функция $\Phi_{i,j}$. Здесь мы будем считать, что значением $\Phi_{i,j}(X(i) \cap Y(j))$ (а значит, возможным ключом) будет одна или несколько точек из множества $X(i) \cap Y(j)$. На самом деле, конечно, можно задать ключевую функцию и другим способом. Например, использовать только одну координату из четырех, или сумму координат, и т.д. Такие способы задания ключевой функции позволяют выработать общий ключ пользователям s_i и s_j даже в том случае, когда множества $X(i)$ и $X(j)$ не имеют общих точек. Однако в этом случае сложнее будет доказать, что такой же ключ не сможет получить кто-нибудь еще из участников схемы, и тем самым выдать себя за другого. Да и в целом лучше свести роль ключевой функции к минимуму. Кроме того, будем считать, что $\Phi_{i,j} = \Phi_{j,i}$, хотя это условие также не выглядит обязательным.

В рамках введенных нами предположений становится ясно, что какую бы мы ни выбрали ключевую функцию, $K(1, 3) \cap K(3, 1) = \varnothing$. Если бы в качестве $\Phi_{1,3} = \Phi_{3,1}$ мы выбрали сумму координат точки, результат был бы иным. Аналогичная ситуация возникает между вторым и третьим пользователями.

Итак, пусть $\Phi_{1,2} = \Phi_{2,1}$ выбирает точку с суммой всех координат, равной единице. Тогда $K(1, 2) = \{(0, 0, 2, -1), (0, 0, 0, 1)\}$, $K(2, 1) = \{(0, 0, 0, 1)\}$, и общим ключом первого и второго участников является $(0, 0, 0, 1)$. Как только первый участник выберет подходящий ключ, они смогут обмениваться информацией друг с другом.

Далее, пусть $\Phi_{3,4} = \Phi_{4,3}$ выбирает точку с наибольшей координатой по y. Тогда $K(3, 4) = \{(0, 1, 0, 0)\} = K(4, 3) = \{(0, 1, 0, 0)\}$, и эти два участника также смогут обмениваться информацией друг с другом.

Приведенная в примере схема согласована с дискреционной политикой безопасности с матрицей доступов, представленной в таблице 3 (0 означает отсутствие взаимного доступа, то есть запрет на обмен информацией, 1 – наличие взаимного доступа, то есть разрешение на информационный обмен).

Однако, на практике более важной является обратная задача: по данной матрице доступов построить схему предварительного распределения ключей, удовлетворяющую задаваемой матрицей дискреционной политике разграничения доступа. К сожалению, в случае, когда секретные доли ключей участников задаются сложными множествами (такими, как кривые или поверхности), решить эту задачу становится довольно сложно.

Таблица 3: Матрица доступов для участников схемы предварительного распределения ключей

i, j	1	2	3	4
1		1	0	0
2	1		0	0
3	0	0		1
3	0	0	1	

3 Схема предварительного распределения ключей с учетом асимметричной политики безопасности

Ранее мы провели адаптацию схемы Блэкли разделения секрета к схеме предварительного распределения ключей для симметричных политик безопасности. Теперь наша цель – расширить упомянутую конструкцию на более широкий класс асимметричных моделей. Считая саму схему векторного разделения секрета широко известной, опишем только построенную на ее основе асимметричную политику разграничения доступа.

Долю секрета пользователя s_i по праву доступа r составляет множество точек $X(i, r)$ в k-мерном подпространстве $L(i)$. Здесь под r может пониматься, например, право на чтение субъектом s_i объектов, принадлежащих другому субъекту, который, в свою очередь, не получает права чтения объектов, принадлежащих субъекту s_i. То есть в описании права доступа обязательно указывается, исходящее это право, либо входящее. В открытом доступе хранится m-мерное подпространство $Y(i)$, сопоставленное пользователю s_i, причем $L(i)$ является подпространством $Y(i)$, то есть $k < m < n$.

Алгоритм выработки общего ключа между i-м и j-м пользователями следующий:
Дано:
1) множество всевозможных ключей $\mathbf{K}$,
2) множество прав доступа $\mathbf{R}$ (причем для каждого права в процессе выработки ключа дополнительно указывается, исходящее оно или входящее для участвующего в выработке ключа пользователя),
3) размерности пространства и подпространств $k < m < n$;
для каждого пользователя s_i: 4) его доли секрета $X(i, r\_in)$, $X(i, r\_out)$ относительно каждого права $r \in \mathbf{R}$,
5) секретное подпространство $L(i)$,
6) открытое подпространство $Y(i)$;
7) также для каждой пары пользователей (s_i, s_j) и права r задана ключевая функция $\Phi_{i,j,r} : \mathbb{R}^{k+m} \to \mathbf{K}^*$, помогающая выработать общий ключ.

Здесь постфикс out в названии права показывает, что право доступа принадлежит пользователю s_i по отношению к другому пользователю, а постфикс in – что другой пользователь применяет право доступа по отношению к пользователю s_i.

Получить: для каждой пары пользователей (s_i, s_j) ключевые множества $K(i, j, r), K(j, i, r) \subset \mathbf{K}$, имеющие общий элемент, который и будет являться общим ключом пользователей s_i и s_j, либо установить, что получение таких множеств невозможно (а значит, s_i не обладает правом доступа r по отношению к s_j).

1. Пользователь s_i находит пересечение множеств $X(i, r\_out)$ и $Y(j)$. Если пересечение пусто, выработка общего ключа невозможна. Это значит, что пользователь s_i не обладает правом доступа r к объектам пользователя s_j в рамках применяющейся политики безопасности.

2. Если $X(i, r\_out) \cap Y(j)$ содержит непустое множество точек, то пользователь s_i вычисляет ключевую функцию Φ_{i,j,r_out} от координат этих точек. Результатом вычисления функции является некоторое множество. Если оно пусто, либо бесконечно, выработка общего ключа невозможна (пользователь s_i не обладает правом доступа r к объектам пользователя s_j в рамках применяющейся политики безопасности).

3. Если $\Phi_{i,j,r\_out}(X(i, r\_out) \cap Y(j))$ непусто и конечно, обозначим это множество через $K_i(i, j, r)$.

4. Пользователь s_j находит пересечение множеств $X(j, r\_in)$ и $Y(i)$. Если пересечение пусто, выработка общего ключа невозможна. Это значит, что пользователь s_i не обладает правом доступа r к объектам пользователя s_j в рамках применяющейся политики безопасности.

5. Если $X(j, r\_in) \cap Y(i)$ содержит непустое множество точек, то пользователь s_j вычисляет ключевую функцию Φ_{j,i,r_in} от координат этих точек. Результатом вычисления функции является некоторое множество. Если оно пусто, либо бесконечно, выработка общего ключа невозможна (пользователь s_i не обладает правом доступа r к объектам пользователя s_j в рамках применяющейся политики безопасности).

6. Если $\Phi_{j,i,r\_in}(X(j, r\_in) \cap Y(i))$ непусто и конечно, обозначим это множество через $K_j(i, j, r)$.

   Стоит обратить внимание на порядок параметров множеств K_i и K_j, который показывает, что право r рассматривается как право субъекта s_i в отношении субъекта s_j, но не в обратную сторону (то есть право r является исходящим), что учитывает асимметричность распределения прав доступа в системе. Однако если для всех субъектов и прав доступа системы выполнено равенство $K_i(i, j, r) = K_j(j, i, r)$, получаем симметричную политику безопасности в качестве частного случая.

7. Пользователи сравнивают результаты. Если $K_i(i, j, r) \cap K_j(i, j, r)$ непусто (если у каждого пользователя получилось некоторое множество результатов, то должны совпадать хотя бы какие-то элементы этих множеств), то элемент из $K_i(i, j, r) \cap K_j(i, j, r)$ является общим ключом связи между пользователями, то есть субъект s_i получает право доступа r в отношении субъекта s_j.

8. Если же пересечение пусто, то i-й пользователь не обладает правом доступа r к объектам j-го пользователя в рамках применяющейся политики безопасности.

Поскольку состояние подсистемы безопасности изменяется со временем, то субъекты в процессе функционирования системы могут получать новые права доступа, а также лишаться старых. В случае дискреционной политики безопасности, например, происходит модификация матрицы доступов. Чтобы данные изменения нашли отражение в схеме распределения ключей, достаточно переслать по защищенному каналу каждому пользователю, которого коснулись соответствующие изменения, новую версию множеств $X(i, r)$.

Приведенная схема хорошо согласуется не только с дискреционными политиками разграничения доступа наподобие HRU, базирующимися на матрицах доступа, но и с мандатными политиками безопасности. Рассмотрим пример применение схемы к мандатной политике разграничения доступа с линейным порядком на уровнях доступа (как правило, более сложные частичные порядки редко применяются на практике).

Пусть мандатная политика безопасности подразумевает три уровня секретности (упорядоченные линейно): A – секретная информация, B – информация с ограниченным доступом, C – информация для свободного доступа. Заодно метки A, B, C будем использовать для индексации субъектов, находящихся на соответствующих уровнях доступа. Множество прав доступа рассмотрим следующее: $\mathbf{R} = \{read\_out, read\_in, write\_out, write\_in\}$.

Пример 4. Пусть k =2, $X(i, r)$ – круг в плоскости $L(i)$ радиуса 1, 2 или 3, $m = n - 2$. Функция $\Phi_{i,j,r}$ будет возвращать упорядоченный набор координат концов отрезка, по которому пересекутся круг и плоскость, и пустое значение, если пересечение пусто, либо не является отрезком.

Рассмотрим пользователя s_A. Он обладает четырьмя секретными множествами $X(A, read\_out)$, $X(A, write\_in)$, $X(A, read\_in)$ и $X(A, write\_out)$, первые два – круги радиуса 3, последние два – радиуса 1 (в данном примере будем считать все круги концентрическими). Радиусы кругов определены в соответствии с принципами мандатной политикой безопасности «нет чтения вверх» и «нет записи вниз».

Так, например, плоскость $L(C)$ пользователя, находящегося на уровне доступа C, будет пересекаться с плоскостью $L(A)$ по прямой, расстояние до которой от общего центра кругов лежит в интервале от 2 до 3. Таким образом, в пересечение попадут точки кругов $X(A, read\_out)$ и $X(A, write\_in)$, но пользователь s_C не получить права читать информацию пользователя s_A, в то время как пользователь s_A не сможет писать информацию в объекты пользователя s_C.

Далее, $L(B)$ в пересечении с $L(A)$ пройдет на расстоянии от 1 до 2 от центра кругов пользователя s_A. Наконец, плоскость пользователя s_A^*, обладающего тем же правом доступа, что и s_A, пересечется с $L(A)$ по прямой, расстояние до которой от центра кругов не будет превышать 1, то есть пользователи одного уровня могут получить полный доступ друг к другу.

Теперь рассмотрим пользователя s_B. Все его секретные множества $X(B, read\_out)$, $X(B, write\_in)$, $X(B, read\_in)$ и $X(B, write\_out)$ – круги радиуса два. Правила пересечения с плоскостями других пользователей – те же. Таким образом, s_B не сможет читать информацию из объектов s_A и писать информацию в объекты s_C, и наоборот, s_A не сможет писать в объекты s_B, а s_C – читать из объектов s_B.

У пользователя s_C ситуация аналогичная, только теперь круги $X(C, read\_out)$ и $X(C, write\_in)$ имеют радиус 1, а $X(C, read\_in)$ и $X(C, write\_out)$ – радиус 3.

В результате $X(A, read\_in)$ и $X(B, read\_out)$ будут пересекаться по пустому множеству, и выработка общего ключа на чтение пользователем s_B материалов пользователя s_A невозможна. Напротив, пересечения $X(B, read\_in)$ с $L(A)$ и $X(A, read\_out)$ с $L(B)$ непусты, пусть это отрезки. Если в рамках мандатной политики безопасности нет дополнительных ограничений на потоки информации, то эти отрезки совпадают, а значит совпадают и наборы координат их концов, что приводит к выработке общего ключа на чтение пользователем s_A материалом пользователя s_B: $K_A(A, B, read) = K_B(A, B, read)$.

Необходимо сразу заметить, что требования на концентричность всех кругов одного пользователя, на радиус этих кругов и расстояние от центра кругов до прямой пересечения серьезно усложняют построение действующей модели, но не являются обязательными. Более того, не обязательно выбирать именно круги в качестве секретных множеств: это было сделано исключительно ради примера. Реализовать схему разделения секрета с учетом мандатной политику безопасности можно и менее строгим способом.

Приведем еще один пример, на этот раз для дискреционной политики безопасности.

Пример 5. В условиях примера 3 рассмотрим множество прав $\mathbf{R} = \{read\_out, read\_in\}$. Секретные множества $X(i, read\_in) = X(i, read\_out)$ примем совпадающими с исходными $X(i)$ для каждого пользователя s_i, так чтобы пересечения $X(i, r) \cap Y(j)$ по каждому праву доступа $r \in \mathbf{R}$ совпадали с занесенными в таблицу 2. Наконец, переопределим ключевые функции следующим образом:

$\Phi_{1,2,read\_in}$, $\Phi_{2,1,read\_out}$ и $\Phi_{2,1,read\_in}$ выбирают точку с суммой всех координат, равной единице, а $\Phi_{1,2,read\_out}$ выбирает точку с суммой всех координат, равной нулю. Тогда $K_1(1, 2, read) = \{(0, 0, 1, -1), (0, 0, -1, 1)\}$, $K_2(1, 2, read) = \{(0, 0, 0, 1)\}$, $K_1(2, 1, read) = \{(0, 0, 2, -1), (0, 0, 0, 1)\}$, $K_2(2, 1, read) = \{(0, 0, 0, 1)\}$. Поскольку $K_1(1, 2, read) \cap K_2(1, 2, read) = \varnothing$, первый участник схемы не получит права читать информацию второго участника. Однако второй получит право читать информацию первого, так как будет выработан общий ключ $K_1(2, 1, read) \cap K_2(2, 1, read) = \{(0, 0, 0, 1)\}$.

Далее, пусть $\Phi_{3,4,read\_in}$, $\Phi_{4,3,read\_out}$ выбирают точки с наибольшей координатой по y, а $\Phi_{3,4,read\_out}$ и $\Phi_{4,3,read\_in}$ выбирает точки с положительным значением координаты y. Тогда $K_3(4, 3, read) = K_4(4, 3, read) = \{(0, 1, 0, 0)\}$, и четвертый участник получит право читать информацию третьего. Однако, вычислить $K_3(4, 3, read)$ не удается, и третий участник схемы не сможет читать информацию четвертого.

Приведенная в примере схема согласована с дискреционной политикой безопасности со следующей матрицей доступов (0 на пересечении i-той строки и j-го столбца означает отсутствие права доступа участника s_i к участнику s_j, заполненная правом r ячейка – наличие соответствующего права участника s_i по отношению к участнику s_j):

Таблица 4: Матрица доступов для участников асимметричной схемы предварительного распределения ключей

i, j	1	2	3	4
1		0	0	0
2	read		0	0
3	0	0		0
3	0	0	read	

Список литературы

[1] S.V. Usov. On the possibility of implementation of the threshold key exchange protocol with discretionary access control based on Blakley"s secret sharing scheme. *Shestoj tehnologicheskij uklad: mehanizmy i perspektivy razvitija. Chast' 1. Sbornik materialov III Mezhdunarodnoj nauchno-prakticheskoj konferencii*, Hanty-Mansijsk: JuGU, 58–59, 2015 (In Russian).

[2] 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 (In Russian).

[3] 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.

[4] G.R. Blakley. Safeguarding cryptographic keys. *Proceedings of the 1979 AFIPS National Computer Conference. Monval, NJ, USA: AFIPS Press*, 313–317, 1979.

On the Application of the Access Control Policy to the Threshold Key Exchange Protocol Based on the Blakley's Scheme of Secret Sharing

Sergey V. Usov

Traditional pre-distribution algorithms ignore the security policy of the system. In this paper, we succeeded in proposing an approach based on the Blackley's scheme for the distribution of keys, leveling this shortcoming. In the proposed scheme, obtaining a public key is only possible for those pairs of participants in the scheme, the exchange of information between which is allowed by the security policy. Moreover, the proposed scheme takes into account the direction of the data flow and the type of access, such as read and write.