Математические структуры и моделирование 2022. № 4 (64). С. 117–121

УДК 004.056
DOI 10.24147/2222-8772.2022.4.117-121

СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА МЕЖДУ ИЕРАРХИЧЕСКИ СВЯЗАННЫМИ УЧАСТНИКАМИ

Н.Ф. Богаченко
к.ф.-м.н., доцент, e-mail: nfbogachenko@mail.ru

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

Аннотация. В статье рассматривается расширение протокола разделения секрета, учитывающее заданное на множестве участников отношение порядка. Порог схемы определяется узлами иерархии, потомки которых образуют полный набор листовых узлов. Алгоритм разделения секрета основан на вычисляемых ключевых материалах.

Ключевые слова: разделение секрета, иерархическая схема, вычисляемые ключи доступа.

Введение

Идея распределения секрета среди некоторой группы участников заложена в схему разделения секрета. При этом вводится понятие (k,n)-пороговой схемы: секрет делится между n участниками так, чтобы любые k и более участников могли восстановить секрет, но никакое меньшее число участников не могло бы получить никаких сведений о секрете. Наиболее известные протоколы разделения секрета — это схема Блэкли, основанная на свойствах пересечения $k-1$-мерных гиперплоскостей в k-мерном пространстве [1,2], и схема Шамира, в основе которой лежит тот факт, что для интерполяции многочлена степени $k-1$ требуется k точек [1,3].

В классических схемах разделения секрета считается, что все субъекты, между которыми делится секрет, равноправны. Предположим теперь, что множество участников протокола (множество субъектов) V является частично упорядоченным. Заданное отношение порядка порождает орграф $G=(V,E)$, описывающий иерархию субъектов. Множество узлов этого орграфа определяется множеством субъектов V, а на множество дуг E накладывается требование отсутствия ориентированных циклов (в силу антисимметричности отношения порядка).

Примером такой иерархии может являться иерархия ролей в ролевой политике разграничения доступа [4,5]. В этом случае каждый участник протокола — элемент множества V — будет представлять группу пользователей или роль. Другие источники, порождающие иерархию субъектов, — это служба каталогов Active Directory или структура распределённой компьютерной информационной системы [6].

Основная идея использования отношения порядка в схеме разделения секрета заключается в следующем: чем выше в иерархии участники протокола, тем меньшее их число необходимо для восстановления секрета. Впервые этот подход был описан в работе [3], при этом предполагалось, что чем выше субъект в иерархии, тем больше долей секрета (теней) он получает. Подобное решение поставленной задачи было расширено до многоуровневой схемы разделения секрета [7], предлагалось делить секрет на несколько теней по числу ярусов в иерархии, а затем каждую тень разбивать на подтени и раздавать на своём уровне. Так называемые совершенные схемы разделения секрета рассмотрены в обзорной работе [8]: задаётся структура доступа в виде графа, который определяет участников, имеющих возможность узнать секрет, если соберутся вместе. При этом ребром соединяются вершины, которые могут восстановить секрет, а любое независимое множество вершин не получает о секрете никаких знаний. В статье [9] представлен протокол разделения секрета, использующий схему Шамира и учитывающий иерархию участников за счёт вычислимых ключевых материалов. В данной работе также используются вычисляемые ключи доступа, подобно алгоритму распределения криптографических ключей, представленному в работе [10].

1. Протокол разделения секрета для древовидной структуры

Пусть требуется разделить секрет S между участниками множества V, на котором задано отношение порядка, определяемое ориентированным деревом $T = (V, E)$. Пусть L — это множество листовых вершин ориентированного дерева T: $L = \{v_{l_1}, \ldots, v_{l_m}\}$ и $|L| = m$. Схема разделения секрета для древовидной иерархии участников протокола состоит из следующих шагов.

1. Ориентированному дереву T сопоставляется помеченное ориентированное дерево T_D по правилу: каждому узлу v_i ориентированного дерева T приписывается метка — уникальный идентификатор D_i. Далее ориентированное дерево T_D называется деревом доступа.
2. Выбирается классическая схема разделения секрета. На её основе реализуется (m, m)-пороговый протокол: секрет S разделяется на m теней $S_1, \ldots, S_m$. При этом для восстановления секрета S требуется собрать все m построенных теней.
3. Выбирается симметричный криптографический алгоритм: $\mathbf{E}$ — функция шифрования, $\mathbf{D}$ — функция расшифрования. В дальнейшем каждая тень секрета S_i будет зашифрована этим алгоритмом.
4. Для корня v_1 дерева доступа T_D выбирается секретный ключ K_1 — ключ доступа.
5. Для каждого узла v_i $(i > 1)$ дерева доступа T_D ключ доступа K_i вычисляется. Правило вычисления K_i следующее: если дуга (v_j, v_i) принадлежит множеству дуг E дерева доступа T_D, то $K_i = \mathbf{h}(K_j \circ D_i)$. Здесь $\mathbf{h}$ — криптографическая хеш-функция, $\circ$ — конкатенация ключа доступа K_j

и идентификатора D_i. В силу свойств ориентированного дерева, в каждый узел, отличный от корня, входит ровно одна дуга, а значит алгоритм вычисления ключей доступа однозначно рассчитает ключи для всех узлов.

6. Тени $S_1, \ldots, S_m$ шифруются на ключах доступа $K_{l_1}, \ldots, K_{l_m}$. Эти ключи доступа вычислены для листовых узлов дерева доступа T_D. Итогом этого шага протокола является набор зашифрованных теней: $\mathbf{E}(K_{l_1}, S_1), \ldots, \mathbf{E}(K_{l_m}, S_m)$.
7. Каждому участнику протокола разделения секрета v_i выдаются следующие материалы: дерево доступа T_D, ключ доступа K_i и зашифрованные доли секрета $\mathbf{E}(K_{l_1}, S_1), \ldots, \mathbf{E}(K_{l_m}, S_m)$.

Пусть теперь $V_k = \{v_{i_1}, \ldots, v_{i_k}\}$ — участники протокола, собравшиеся для восстановления секрета. Процедура восстановления секрета S описывается следующей схемой:

1. Для каждого узла $v_i \in V_k$, зная ключ K_i и дерево доступа T_D, вычисляются ключи доступа для листовых узлов, достижимых из узла v_i. Обозначим это множество листовых узлов $L(v_i)$, а получившиеся ключи доступа K_{i_j}, $j \in \{l | v_l \in L(v_i)\}$.
2. Для каждого узла $v_i \in V_k$ расшифровывается набор теней $S_{i_j} = \mathbf{D}(K_{i_j}, \mathbf{E}(K_{i_j}, S_{i_j}))$, $j \in \{l | v_l \in L(v_i)\}$.
3. Тени всех узлов $v_i \in V_k$ объединяются для восстановления секрета S.

Заметим, что если $V_k = \{v_{i_1}\}$, то в силу определения ориентированного дерева о достижимости всех листовых узлов из корня, $L(v_1) = L$. Это означает, что участник протокола, находящийся в вершине иерархии, сможет расшифровать все тени и восстановить секрет. Если $V_k = L$, то известны все ключи доступа $K_{l_1}, \ldots, K_{l_m}$ и участники протокола также смогут расшифровать все тени и восстановить секрет. В общем случае очевидна справедливость следующего утверждения.

Предложение 1. *Восстановить секрет S возможно тогда и только тогда, когда*

$$L = \bigcup_{v_{i_j} \in V_k} L(v_{i_j}).$$

Доказательство. Восстановить секрет S возможно тогда и только тогда, когда известны все доли секрета $S_1, \ldots, S_m$. Это, в свою очередь, возможно тогда и только тогда, когда известны ключи доступа листовых узлов дерева T_D $K_{l_1}, \ldots, K_{l_m}$. Последнее имеет место тогда и только тогда, когда выполнено условие предложения. ■

2. Произвольная иерархическая структура

Пусть теперь иерархия, порождаемая отношением порядка на множестве V, описывается произвольным орграфом $G = (V, E)$ без ориентированных циклов.

Для реализации представленного протокола разделения секрета необходимо перейти от произвольной иерархии к древовидной. Идея алгоритма перехода от произвольного орграфа к ориентированному дереву следующая. Каждый

узел v исходного графа, полустепень захода которого $d^+(v) > 1$, расщепляется на $d^+(v)$ узлов. К каждому узлу присоединяется дубликат поддерева, порождённого узлами, достижимыми из узла v в исходном орграфе. Запускать процесс расщепления узлов необходимо от узлов наиболее удалённых от вершины иерархии. Алгоритм подробно описан в работе [11]. При этом ограничением на исходный орграф, помимо отсутствия ориентированных циклов, является наличие в орграфе единственного источника. Очевидно для случая нескольких источников ограничение легко достигается добавлением к иерархии фиктивного узла, который дугами соединяется со всеми источниками.

Пусть согласно описанному алгоритму исходному орграфу G сопоставлено ориентированное дерево T_G. Каждому узлу v в орграфе G соответствует множество узлов $T(v)$ в ориентированном дереве T_G. Очевидно, что мощность множества $T(v)$ больше или равна 1.

Тогда схема разделения секрета для иерархии, представленной орграфом G, будет состоять из следующих шагов.

1. Орграфу G сопоставляется помеченный орграф G_D аналогично шагу 1 протокола разделения секрета, описанного в разделе 1.
2. За счёт расщепления узлов с числом входящих дуг большим единицы, орграфу G_D сопоставляется ориентированное дерево T_{G_D}.
3. Для ориентированного дерева T_{G_D} выполняются шаги 2–7 описанного в разделе 1 протокола разделения секрета. На шаге 7 отличие заключается в том, что каждый участник протокола v_i получает несколько ключей доступа, соответствующих узлам множества $T(v_i)$ в ориентированном дереве T_{G_D}.

Заключение

Описанный в работе криптографический протокол можно отнести к классу пороговых схем разделения секрета. Но в классических (k, n)-пороговых схемах параметр k является постоянным. В представленном протоколе, напротив, число участников, необходимое для восстановления секрета, является переменной величиной. Параметр k варьируется на отрезке $[1, m]$, где m – число листовых узлов иерархии участников протокола. Таким образом, восстановить секрет может либо один участник, находящийся в вершине иерархии, либо m участников, являющихся листовыми узлами, либо некоторое промежуточное число участников, потомки которых образуют покрытие множества листовых узлов.

Возвращаясь к интерпретации иерархии участников протокола как иерархии ролей или меток безопасности некоторой политики разграничения доступа, представленный подход можно применить для реализации коллективного разграничения доступа: доступ к ресурсам может получить группа пользователей, занимающих определённый уровень в иерархии.

Литература

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М. : Триумф, 2002. 816 с.
2. Blakley G.R. Safeguarding cryptographic keys (англ.) // Proceedings of the 1979 AFIPS National Computer Conference. Montvale: AFIPS Press, 1979. P. 313–317.
3. Shamir A. How to share a secret // Communications of the ACM. 1979. V. 22, Iss. 11. P. 612–613.
4. Ferraiolo D.F., Kuhn D.R. Role-Based Access Controls // 15th National Computer Security Conference. Baltimore MD, 1992. P. 554–563.
5. Sandhu R.S., Coynek E.J., Feinsteink H.L., Youmank C.E. Role-Based Access Control Models // IEEE Computer. February 1996. V. 29, No. 2. P. 38–47.
6. Богаченко Н.Ф. Разграничение доступа на основе вычислимых криптографических ключей // Омские Научные чтения [Электронный ресурс] : материалы Всероссийской научно-практической конференции (Омск, 11–16 декабря 2017 г.). Омск : Изд-во Ом. гос. ун-та, 2017. С. 312-315.
7. Nojoumian, M., Stinson, D.R. Sequential Secret Sharing as a New Hierarchical Access Structure // J. Internet Serv. Inf. Secur. 2015. V. 5. P. 24–32.
8. Парватов Н.Г. Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2(2). С. 50–57.
9. Belim S.V., Bogachenko N.F. Hierarchical Scheme for Secret Separation Based on Computable Access Labels // Automatic Control and Computer Sciences. 2020. V. 54, No. 8. P. 773–778.
10. Belim S.V., Bogachenko N.F. Distribution of Cryptographic Keys in Systems with a Hierarchy of Objects // Automatic Control and Computer Sciences. 2016. V. 50(8). P. 777–786.
11. Bogachenko N.F. Local Optimization of the Role-Based Access Control Policy // CEUR Workshop Proceedings. 2017. V. 1965.

SSCHEME FOR SHARING A SECRET BETWEEN HIERARCHICALLY RELATED PARTICIPANTS

N.F. Bogachenko
Ph.D.(Phys.-Math.), Associate Professor, e-mail: nfbogachenko@mail.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The article considers an extension of the secret sharing protocol that takes into account the order relation specified on the set of participants. The schema threshold is determined by the hierarchy nodes whose descendants form a complete set of leaf nodes. Secret sharing algorithm based on calculated key materials.

Keywords: secret sharing, hierarchical scheme, computed access keys.

Дата поступления в редакцию: 05.12.2022