УДК 681.391.1

РАЗГРАНИЧЕНИЕ ДОСТУПА К РЕСУРСАМ В СИСТЕМАХ КОЛЛЕКТИВНОГО ПОЛЬЗОВАНИЯ

И. Л. Ерош,
д-р техн. наук, профессор
Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)

В статье рассмотрена задача на разграничение доступа в системах коллективного пользования, основанная на булевых преобразованиях двоичных последовательностей. Для обеспечения доступа используется метод сравнения запроса с ответом. Приведены примеры построения булевых функций, применение которых позволяет гибко менять доступ для каждой группы пользователей в зависимости от выбираемых запросов.

In the article task on differentiation of access in shared systems based on Boolean transformations of binary sequences is considered. For providing of access the method of comparison of inquiry with the answer is used. The examples of construction Boolean of functions are given, in which access for each group of the users flexibly varies depending on chosen inquiries.

Введение

При работе нескольких пользователей в компьютерной сети часто требуется ограничивать доступ некоторых пользователей к ресурсам системы. Рассмотрим задачу на разграничение доступа, которую условно назовем «Солдаты и офицеры». Пусть требуется снабдить каждого солдата, офицера и генерала одним электронным ключом, причем таким, чтобы солдат своим ключом мог открыть все помещения, предназначенные для солдат, офицер мог попасть во все солдатские и в офицерские помещения, а генерал мог попасть во все помещения, предназначенные для солдат и офицеров, а также в свой генеральский кабинет. При этом солдат своим ключом не может открыть помещения, предназначенные для офицеров и генералов, а офицер не может открыть генеральский кабинет.

Для обеспечения доступа будем использовать пароли, основанные на булевых преобразованиях, описанных в работах [1, 2]. Напомним общую идею этого метода. Пусть имеются две двоичные последовательности $A(a_1, a_2, ..., a_n)$ и $B(b_1, b_2, ..., b_n)$. При этом $a_i, b_i \in \{0, 1\}, i = 1, 2, 3, ..., n$. Элементы последовательности B будем получать преобразованием последовательности A булевой функцией F, при этом b_i будет результатом булевого преобразования, зависящего от a_i и некоторых элементов из его окружения. Например, если A = 10110001101 и выбрана функция $F = |0^*-1 \vee 2$, то это означает, что каждый элемент b_i последовательности B равен $b_i = |a_i \& a_{i-1} \vee a_{i+2}$. В данном примере из последовательности A будет получена последовательность B = 11001110110.

В настоящей статье по набору запросов и ответов определим соответствующие функции F, которые позволят выполнить требуемые преобразования.

Примеры решения задачи доступа

Пример 1. Для доступа в помещения требуется сравнение с известным паролем обработанного (ответного) кода на запрос. Иными словами, для случайного кода запроса, булева функция ключа вырабатывает пароль на открывание помещения. Если пароль совпадает с требуемым для данного помещения, оно открывается, если нет — не открывается. Таким образом, нужно найти три разные булевы функции (для солдат, офицеров и генералов), такие, чтобы на запросы при доступе к солдатским помещениям все функции вырабатывали один и тот же код, соответствующий коду открывания солдатских помещений. При требовании доступа к офицерским помещениям солдатские ключи должны вырабатывать ложный код, а офицерские и генеральские — требуемый для открывания помещений. При доступе к генеральскому кабинету солдатские и офицерские ключи должны вырабатывать ложные коды и только генеральский — требуемый для открывания.

Для примера выберем коды для открывания в следующем виде: 4C — для солдатских (двоичный код 01001100); D8 — для офицерских (11011000) и E5 — для генеральских (11100101).

Перед доступом в помещение вырабатывается случайный запрос. Для упрощения примера выберем по два байтовых кода для случайного запроса,

например, в таком виде: A6, C9 — перед входом в солдатские помещения; 7E, B5 — перед входом в офицерские и 6D, 4A – перед входом в генеральский кабинет.

Используя методику, описанную в работе [1], получим один из вариантов функций, обеспечивающих ответы на запросы: $F_1 = 3*0*\rceil\!\lfloor\!-2 \vee \rceil 0*\lceil\!-2*\rceil\!\lfloor\!-3 \vee \vee 2*\rceil 0*\lceil\!-1 \vee 1*0*-3$ — функция солдата; $F_2 = 3**\rceil\!\lfloor\!-1*\rceil\!\lfloor\!-2 \vee 2*\rceil 1*0*-1 \vee 2*0*-1*-2 \vee 3*\rceil 1*0*-1 \vee \rceil 0**\rceil\!\lfloor\!-2*\rceil\!\lfloor\!-3 \vee 1*\rceil 0*-1*\rceil\!\lfloor\!-3 \vee 2*\rceil 0*\rceil\!\lfloor\!-1 \vee 1*0*\rceil\!\lfloor\!-1*-3$ — функция офицера; $F_3 = \rceil 0*\rceil\!\lfloor\!-2*\rceil\!\lfloor\!-3 \vee \rceil 2*\rceil 1*\rceil 0*\rceil\!\lfloor\!-2 \vee \vee 3*\rceil\!\lfloor\!-1*\rceil\!\lfloor\!-2 \vee 2*\rceil 1*0*-1 \vee \rceil 2*\rceil 1*\rceil\!\lfloor\!-1*-2*-3 \vee 3*1*\rceil 0**-1 \vee 2*0*-1*-2 \vee 3*\rceil 1*0*-1 \vee 2*\rceil 0*\rceil\!\lfloor\!-1 \vee 1*0*\rceil\!\lfloor\!-2*-3$ — функция генерала.

Число различных случайных запросов может быть выбрано сколь угодно большим. По два запроса на каждом пункте проверки выбрано лишь для простоты иллюстрации излагаемого материала. Результаты представлены в табл. 1.

В данном примере для прохода требовалось совпадение с паролем ответного кода на запрос. Это означает, что система проверки просто сравнивает ответ с паролем. Система может быть усложнена, если на каждом уровне проверки ввести функцию, которая будет проверять соответствие запроса ответу.

Особенность рассмотренной системы заключается в том, что при доступе в солдатские помещения солдат, офицер и генерал неразличимы, при проходе в офицерские — неразличимы офицер и генерал. Иными словами, системе присуща неотслеживаемость доступа через системы проверки.

Пример 2. Задача доступа решается совместно с проверкой «информированности» каждой группы пользователей. Например, при проходе в солдатские помещения задаются k_1 вопросов и сверяются с правильными ответами, при проходе в офицерские и генеральское помещения, соответственно, k_2 и k_3 вопросов. В общем случае число вопросов может быть произвольным, и они могут периодически меняться. Для рассматриваемого примера возьмем $k_1 = 2$, $k_2 = 3$, $k_3 = 4$. Вопросы и правильные ответы выберем следующим образом.

Для солдатского контроля: 6C → 18; D2 → 3E.

Для офицерского контроля: D5 → C6; 47 → B3; 9A → 67.

Для генеральского контроля: 58 → DA; EC → A3; B4 → 7C; 91 → 66.

Как и в предыдущей задаче, генерал должен правильно ответить на все запросы, офицер ошибается в ответах только на генеральские запросы, солдат ошибается в ответах как на офицерские, так и на генеральские запросы. Заметим, что запросы и соответствующие им ответы выбираются случайным образом и периодически могут меняться.

По методике, изложенной в работах [1, 2], получим функции: для солдат $F_1 = \rceil 1*0*\rceil\!\lfloor\!-1 \vee 2*\rceil 0*-1 \vee \vee 1*-2$; для офицеров $F_2 = 1*\rceil\!\lfloor\!-1*-2 \vee \rceil 3*1*-1 \vee \vee \rceil 2*\rceil 1*0*\rceil\!\lfloor\!-1*-3 \vee \rceil 1*\rceil 0*-1*-3 \vee \rceil 2*1*\rceil 0*\rceil\!\lfloor\!-1 \vee \vee 2*\rceil 1*\rceil 0 \vee 0*-1*-2 \vee 5*1*0 \vee 4*-1 \vee 2*\rceil 1*\rceil\!\lfloor\!-1*\rceil\!\lfloor\!-3$; для генералов $F_3 = \rceil 2*1*\rceil 0*\rceil\!\lfloor\!-1 \vee 4*\rceil 0*-1 \vee 2*0*-1*-3 \vee \vee \rceil 3*\rceil 2*1*\rceil 0 \vee -1*-2*-6 \vee -3*-7 \vee \rceil 5*2*\rceil 1*\rceil\!\lfloor\!-1*\rceil\!\lfloor\!-2 \vee \vee \rceil 2*\rceil 1*-1*\rceil\!\lfloor\!-4 \vee \rceil 1*\rceil 0*-3*\rceil\!\lfloor\!-6 \vee \rceil 1*\rceil 0*-1*\rceil\!\lfloor\!-4 \vee \vee \rceil 3*1*0*-1 \vee 5*1*0 \vee 4*\rceil 1*-1 \vee 2*-2*\rceil\!\lfloor\!-3 \vee \rceil 4*\rceil 1*0** *\rceil\!\lfloor\!-1*-3 \vee 1*0*-2*\rceil\!\lfloor\!-4$.

Результаты ответов на запросы показаны в табл. 2.

Из таблицы видно, что система функционирует правильно. Предположим, что злоумышленник овладел информацией как о запросах, так и ответах на них на всех пунктах пропуска. При этом будем считать, что задавались только первые запросы из каждой группы, а именно: 6C → 18 — при солдатском контроле; D5 → C6 — при офицерском контроле; 58 → DA — при генеральском контроле.

Если злоумышленник владеет способом построения булевых функций, обеспечивающих такое преобразование, а это естественно предположить, то он может найти, например, такую функцию:

$F_{злоум} = \rceil 2*1*\rceil 0*\rceil\!\lfloor\!-1 \vee \rceil 2*0*-1*\rceil\!\lfloor\!-4 \vee \rceil 1*\rceil 0*\rceil\!\lfloor\!-1*\rceil\!\lfloor\!-6 \vee \vee \rceil 4*1*0 \vee \rceil 3*2*0*-1 \vee 2*0*\rceil\!\lfloor\!-1*\rceil\!\lfloor\!-3 \vee \rceil 3*\rceil 2*1 \vee 2*\rceil 0*-2$.

С ее помощью злоумышленник на первые запросы из каждой группы ответит верно, поскольку из этих данных и была сформирована функция $F_{злоум}$. На вторые запросы из каждой группы злоумышленник ответит неверно: D2 → E4; 47 → 97; EC → D8 и не пройдет проверку ни на одном пункте контроля.

При нахождении булевой функции в таблицу истинности можно ввести специальную строку, отмечающую время нахождения функции, и по тестовому запросу этой строки определять, когда был получен доступ к данным ресурсам.

Пример 3. Рассмотрим задачу распределения доступа, в котором при ответах на некоторые запросы преимущество имеет генерал, при ответах на другие запросы нет преимуществ ни у кого, а при ответе на третью группу запросов преимущество имеет солдат.

■ ***Таблица 1.*** *Результаты ответов на запросы, сформированные для солдата, офицера и генерала*

Запрос	Солдатская функция F_1	Офицерская функция F_2	Генеральская функция F_3	Комментарий
A6	4C	4C	4C	Все ответили верно
C6	4C	4C	4C	
7E	**EC**	D8	D8	Солдат ответил неверно
B5	**C0**	D8	D8	
CD	**E8**	**FE**	E5	Верно ответил только генерал
4A	**E4**	**E4**	E5	

Примечание. Здесь и далее в таблицах жирным шрифтом отмечены неверные ответы.

■ ***Таблица 2.*** *Результаты ответов на запросы, сформированные для солдата, офицера и генерала, с проверкой «информированности»*

Запрос	Солдатская функция F_1	Офицерская функция F_2	Генеральская функция F_3	Комментарий
6C	18	18	18	Все ответили верно
D2	3E	3E	3E	
D5	**35**	C6	C6	Солдат ответил неверно
47	**40**	B3	B3	
9A	**E6**	67	67	
58	**70**	**F0**	DA	Верно ответил только генерал
EC	**18**	**F8**	A3	
B4	**EC**	**EE**	7C	
91	**F1**	**76**	66	

Выберем восемь пар «запрос—ответ» и найдем функции F_1, F_2 и F_3 такие, чтобы обеспечить сформулированные выше требования.

D2 → 3E — все должны ответить правильно.

47 → B3 — правильно должны ответить офицер и генерал.

EC → A3 — правильно должен ответить только генерал.

В этой первой группе запросов преимущество имеет генерал.

5E → 6A — правильно отвечает только солдат.

F2 → 3D — правильно отвечает только офицер.

B4 → 9C — правильно отвечает только генерал.

В этой второй группе запросов преимуществ нет ни у кого, и каждый отвечает правильно только при доступе в свое помещение.

C5 → 39 — правильно отвечает солдат и офицер.

82 → CD — правильно отвечает только солдат.

В этой третьей группе запросов преимущество имеет солдат, и он может пройти как в офицерские помещения, так и в генеральский кабинет. Если к третьей группе запросов добавить пару D2 → 3E, то офицер сможет пройти в свое помещение и в генеральский кабинет, а генерал — только в свой кабинет.

Булевы функции для солдата (F_1), офицера (F_2) и генерала (F_3) имеют следующий вид:

$$F_1 = \lceil 2^* \rceil 1^* 0^* \rceil - 1^* \rceil - 6 \vee \lceil 1^* \rceil 0^* - 1^* \rceil - 4 \vee \vee 2^* \rceil 0 \vee \lceil 3^* 1^* \rceil 0^* \rceil - 1 \vee 1^* - 3 \vee \rceil 1^* 0^* *-2 \vee 3^* \rceil 1^* 0 \vee 1^* \rceil 0^* - 2 \vee 0^* - 3;$$

$$F_2 = -2 \vee \lceil 2^* \rceil 0^* \rceil - 1 \vee \rceil 1^* \rceil 0^* - 5 \vee 3^* - 1 \vee \rceil 2^* 1^* 0^* *-1 \vee 2^* \rceil 0^* - 1 \vee 0^* - 3^* \rceil - 4;$$

$$F_3 = 2^* 0^* - 3 \vee \lceil 2^* 1^* \rceil 0 \vee 2^* 0^* \rceil - 1^* \rceil - 4 \vee \rceil 1^* - 1^* *-2 \vee \rceil 1^* \rceil - 1^* - 3 \vee 3^* \rceil 0^* - 1 \vee 2^* \rceil 1^* \rceil 0 \vee \lceil 3^* 1^* 0^* - 1.$$

Результаты проверки приведены в табл. 3.

Последний пример показывает, что, не меняя функций доступа у солдат, офицеров и генералов, можно только сменой наборов «запрос—ответ» гибко менять права доступа в различные помещения. Если есть требование, чтобы в помещение имели доступ одновременно несколько человек (например, трое: солдат, офицер и генерал), то можно выбрать группу запросов, аналогичную второй группе рассмотренного примера, и одновременно предъявить все три функции. В этом случае на каждый запрос правильно ответит хотя бы один и помещение станет доступно.

Пример 4. В данном примере рассмотрим пороговую задачу доступа из N доверенных лиц при пороге h. Такая задача может решаться при любом числе N и любом пороге h [3]. Пусть, например, N офицеров получили фрагменты ключа от генеральского кабинета. При этом требуется обеспечить возможность доступа в кабинет лишь в случае, когда соберутся вместе любые h офицеров из N. Если соберется меньше, то открыть его они не могут. Из [3] следует, что если число офицеров, имеющих фрагменты ключа, равно N, и требуется обеспечить порог доступа h, то можно построить таблицу равновесных кодов длины N веса $d = N - h + 1$ и распределять пары «запрос—ответ» в соответствии с таблицей кодов.

Число таких кодов определяется как $P(h-1, N-h+1) = \frac{N!}{(h-1)!(N-h+1)}$.

Для $N = 5$ и $h = 3$ равновесные коды длины 5 веса $d = 3$ для десяти пар "запрос—ответ" приведены в табл. 4.

Значение «1» в таблице для каждого офицера означает, что он правильно отвечает на соответствующие запросы. Из табл. 4 следует, что, если соберутся вместе любые три офицера, они правильно ответят на все десять запросов, если их будет меньше трех ? они не смогут правильно ответить на все запросы.

Выберем произвольные пары «запрос—ответ» и найдем булевы функции для каждого из пяти офицеров.

$$F_1 = \lceil 2^* 1^* \rceil 0^* \rceil - 1 \vee \lceil 2^* 0^* - 1^* \rceil - 4 \vee \rceil 1^* \rceil 0^* \rceil - 1^* \rceil - 6 \vee \vee 3^* \rceil 1^* \rceil - 1 \vee 2^* - 1^* - 4 \vee \rceil 2^* \rceil 1^* 0^* \rceil - 1^* - 3 \vee \vee 3^* \rceil 1^* \rceil 0 \vee 5^* \ 1^* 0 \vee 4^* - 1 \vee 2^* \rceil 1^* \rceil - 1^* \rceil - 3 \vee \vee \rceil 3^* \rceil 2^* 1 \vee 2^* \rceil 0^* - 2;$$

$$F_2 = 2^* \rceil 0^* - 1^* \rceil - 2 \vee 2^* 0^* - 1^* - 3 \vee \rceil 3^* \rceil 2^* 1^* \rceil 0 \vee -1^* - 2^* *-6 \vee -3^* - 7 \vee 5^* 1^* 0 \vee 4^* \rceil 1^* - 1 \vee 2^* - 2^* \rceil - 3 \vee \rceil 4^* \rceil 1^* 0^* *\rceil - 1^* - 3 \vee 1^* 0^* - 2^* \rceil - 4;$$

$$F_3 = \lceil 3^* \rceil 2^* 1^* \rceil - 2 \vee 2^* \rceil 1^* \rceil 0 \vee \rceil 3^* 0^* - 1^* \rceil - 3 \vee 2^* 1^* 0^* *\rceil - 4 \vee - 1^* - 2^* - 6 \vee - 3^* - 5^* - 7 \vee 3^* \rceil 2^* \rceil 1^* \rceil - 1 \vee 1^* - 2^* *\rceil - 3 \vee \rceil 3^* 2^* 0^* - 1 \vee 0^* - 2^* \rceil - 4 \vee \rceil 0^* - 1^* \rceil - 2^* \rceil - 3;$$

■ ***Таблица 3.*** *Результаты ответов на запросы, сформированные для солдата, офицера и генерала при наличии преимуществ*

Запрос	Солдатская функция F_1	Офицерская функция F_2	Генеральская функция F_3	Комментарий
D2	3E	3E	3E	Все ответили верно
47	**F9**	B3	B3	Солдат ответил неверно
EC	**3C**	**7B**	A3	Верно ответил только генерал
5E	6A	**BF**	**FF**	Верно ответил только солдат
F2	**1E**	3D	**FE**	Верно ответил только офицер
B4	**D4**	**7D**	9C	Верно ответил только генерал
C5	39	39	**3A**	Верно ответил солдат и офицер
82	CD	**34**	**1C**	Верно ответил только солдат

■ ***Таблица 4.*** *Равновесные коды для $N = 5$ и $h = 3$*

Номера запросов	Номера офицеров				
	1	2	3	4	5
1	1	1	1	0	0
2	1	1	0	1	0
3	1	1	0	0	1
4	1	0	1	1	0
5	1	0	1	0	1
6	1	0	0	1	1
7	0	1	1	1	0
8	0	1	1	0	1
9	0	1	0	1	1
10	0	0	1	1	1

■ ***Таблица 5.*** *Ответы пяти офицеров на запросы системы доступа*

Запрос	Правильный ответ	1-й офицер	2-й офицер	3-й офицер	4-й офицер	5-й офицер
6C	18	18	18	18	**03**	**FD**
D2	3E	3E	3E	**7D**	3E	**F6**
D5	C6	C6	C6	**72**	**3F**	C6
47	B3	B3	**B1**	B3	B3	**F7**
9A	EE	EE	**67**	EE	**46**	EE
58	DA	DA	**30**	**30**	DA	DA
EC	A3	**D8**	A3	A3	A3	**AD**
B4	7C	**CD**	7C	7C	**BD**	7C
91	66	**BE**	66	**EE**	66	66
CC	AE	**F8**	**E3**	AE	AE	AE

$$F_4 = ⌈3*⌈2*1*⌉-2\vee 2*⌉1*⌉0\vee⌈3*⌈2*0*-1*⌉-3\vee$$
$$\vee⌈1*⌉0*-1*⌉-4\vee⌈2*1*⌉0\vee 2*0*⌉-1*⌉-4\vee⌉0*$$
$$*-5\vee 0*-2*⌉-3\vee 0*-1*-3*⌉-4\vee⌈4*⌉1*0*⌉-1*-3;$$

$$F_5 = ⌈3*0*-1\vee⌈1*⌉0*-1*⌉-4\vee 4*⌉0\vee⌈2*0*-2*$$
$$*-3\vee⌈5*2*0*⌉-2\vee-3*-5\vee 4*⌉-1*⌉-3\vee 1*⌉-1*⌉-3\vee 2*$$
$$*-2*⌉-3\vee⌈3*⌈2*1.$$

Результаты ответов на запросы системы доступа представлены в табл. 5.

Любые три столбца в приведенной таблице содержат в любой строке хотя бы один правильный ответ. Для любых пар столбцов найдется хотя бы один запрос, на который оба офицера ответят неверно.

Влияние длины последовательностей на сложность реализации

В приводимых примерах обрабатывались запросы длиной в 8 бит. Не представляет труда построить функцию и для более длинных запросов. Пусть, например, запросы и ответы имеют длину в 128 бит и имеют вид в шестнадцатеричном коде:

A63CBE9F91BCDA6385BDF2C917ACEBD2 — запрос;
A8BD72910CFDE893DFCBAE7619DEFBA6 — ответ.

Функция F, преобразующая A в B, имеет вид:

$$F = ⌈3*2*1*⌉0*-2\vee 5*2*⌉1*⌉0*⌉-1*$$
$$*-3\vee⌈2*⌉1*0*-1*⌉-4\vee 3*⌈2*1*⌉0*-2\vee 3*1*⌉0*$$
$$*-1*⌉-3\vee 2*⌉1*0*-1*-4\vee 4*0*⌉-1*-2*$$
$$*-4\vee⌈3*⌈2*1*0*-1\vee 4-⌈2*⌉1*⌉0*⌉-2\vee 3*⌉1*$$
$$*⌉-1*⌉-3\vee 2*0*⌉-1*-3*⌉-5\vee 3*1*0*⌉-2*$$
$$*-3\vee⌈6*⌉1*⌉0*-1*-2\vee⌈2*⌉1*⌉0*-1*$$
$$*-3\vee 2*1*⌉0*-1*⌉-4\vee 3*⌈2*0*-2*⌉-3\vee 1*0*⌉-1*$$
$$*-2*-4\vee⌈4*2*0*⌉-2\vee⌉1*0*-1*⌉-2*-3\vee 2*⌉1*$$
$$*-1*⌉-3\vee⌈2*⌉0*⌉-1*-2*⌉-4\vee⌈2*⌉0*⌉-1*$$
$$*⌉-3\vee 4*⌈3*⌉1*0*-2\vee⌈3*1*⌉0*-1*⌉-2*$$
$$*-3\vee 4*2*0*⌉-1*-2\vee 0*-1*⌉-2*-5\vee 1*⌉0*-2*$$
$$*⌉-5\vee⌈4*⌈3*⌉1*⌉-1.$$

Число разных аргументов функции F в данном примере равно 12. Эксперименты показывают, что число используемых аргументов функции возрастает значительно медленнее длины последовательности n. При $n = 256$ их количество составляет примерно 10 %, т. е. математическое ожидание числа аргументов равно 25.

Заключение

Приведенные примеры иллюстрируют метод распределенного доступа в системах коллективного пользования, который может быть применен для управления доступом к вычислительным ресурсам компьютерной сети, для обеспечения доступа с ограничениями в помещения и др.

Литература

1. **Ерош И. Л.** Дискретная математика. Булевы функции, комбинационные схемы, преобразование двоичных последовательностей. Учебное пособие. — СПб: СПбГУАП, 2001. — 38 с.
2. **Ерош И. Л.** Защита информационных потоков в системах распределенного контроля и управления // Информационно-управляющие системы. — 2002. — № 1. — С. 40–46.
3. **Ерош И. Л.** Система передачи данных с закрытыми ключами // В кн.: Информационные системы в промышленности и экономике / Под ред. И. Л. Ероша СПб,1999. — С. 114–116.