А. В. Архангельская, К. Г. Когос

О ПОДХОДЕ К ПРОТИВОДЕЙСТВИЮ УТЕЧКЕ ИНФОРМАЦИИ ПО СКРЫТЫМ КАНАЛАМ

Введение

Первый шаг в решении проблемы передачи данных из защищаемой системы по скрытым каналам — поиск потенциальных скрытых каналов и их идентификация. Далее оценивается ущерб, который они представляют для системы, причем зачастую выполняется расчет пропускной способности канала. Этот анализ особенно важен, поскольку устранение скрытых каналов может оказаться трудоемкой дорогостоящей процедурой. Таким образом, в ряде случаев следует остановиться только на противодействии скрытым каналам с высокой пропускной способностью. Согласно [1], скрытые каналы с пропускной способностью менее 100 бит/с считаются неопасными. После идентификации скрытых каналов необходимо рассмотреть способ их устранения либо ограничения их пропускной способности.

Параллельно с поставленными задачами необходимо проводить обнаружение и аудит скрытых каналов. Заметим, что задачу идентификации скрытых каналов часто путают с задачей обнаружения [2, 3]. Задача идентификации заключается в выявлении потенциальных скрытых каналов, которые могут быть реализованы путем анализа архитектуры системы. Задача обнаружения заключается в нахождении функционирующих скрытых каналов. Данная статья посвящена исследованию описанных этапов противодействия утечке информации по скрытым каналам.

1. Идентификация скрытых каналов

В многоуровневых системах безопасности предлагается несколько методов идентификации скрытых каналов [3–8]. В одной из работ [5] предложен метод определения всевозможных запрещенных информационных потоков, возникающих путем применения разрешенных операций, таких как операции ввода/вывода, копирование и т. д. Пусть $SC = \{A_1,\ldots,A_n\}$ — множество уровней доступа в системе. Определим на множестве SC частичный порядок: $A_i \to A_j$, если объекту с уровнем доступа A_j позволено получать информацию с уровнем доступа A_i. Авторами [5] доказано, что частично упорядоченное множество $\langle SC,\to\rangle$ является решеткой, анализ свойств которой позволяет определить всевозможные запрещенные информационные потоки.

Рассмотрим методы идентификации скрытых каналов, то есть определения неявных, нарушающих политику безопасности информационных потоков через атрибуты ресурсов и простейшие операции, основанные на различных структурах данных:

1) матрице разделяемых ресурсов;

2) дереве скрытых информационных потоков;

3) диаграмме последовательности сообщений.

Матрицы разделяемых ресурсов можно использовать для идентификации скрытых каналов по памяти [4]. В этом методе атрибуты разделяемых ресурсов и простейшие операции являются заголовками строк и столбцов матрицы соответственно. Значения в ячейках матрицы соответствуют действиям пользователя над соответствующими атрибутами (чтение, запись или чтение и запись). Известно, что при включении системного времени в качестве атрибута возможно определение скрытых каналов по времени, однако данный метод разработан для идентификации каналов по памяти, а его распространение на каналы по времени не гарантирует определения всех таких каналов. Рассмотрим пример матрицы разделяемых ресурсов для идентификации

скрытых каналов в системе, описанной в [4]. В анализируемой системе возможны следующие элементарные операции:

1) чтение из файла (ОП1);
2) запись в файл (ОП2);
3) открытие файла для чтения (ОП3);
4) закрытие файла (ОП4);
5) блокирование файла для записи (ОП5);
6) освобождение файла для записи (ОП6);
7) определение того, заблокирован ли файл (ОП7);
8) определение того, открыт ли файл (ОП8).

В системе содержится два типа объектов — процессы и файлы. Рассмотрим атрибуты данных объектов. Атрибуты процессов — идентификатор (А1), права доступа (А2), буфер (А3). Атрибуты файлов — идентификатор (А4); уровень доступа (А5); данные о том, заблокирован ли файл (А6); данные о том, кем заблокирован файл (А7); множество идентификаторов процессов, для которых файл открыт для чтения (А8); значение файла (А9). Также в качестве атрибута выделим идентификатор текущего процесса (А10), так как в каждый промежуток времени только один процесс может быть активным.

Матрица разделяемых ресурсов для описанной системы представлена таблице 1.

Потенциальные скрытые информационные потоки можно найти путем построения транзитивного замыкания матрицы разделяемых ресурсов. Транзитивное замыкание построенной матрицы представлено в таблице 2.

Для идентификации скрытых каналов по памяти необходимо проанализировать атрибуты ресурсов, строки которых содержат буквы «Ч» и «З», на предмет использования их как средства передачи информации.

В таблицах 1, 2 символы имеют следующие обозначения: «Ч» — доступ на чтение; «З» — доступ на запись.

Таблица 1. Пример матрицы разделяемых ресурсов

Элементарные операции / Атрибуты ресурсов		ОП1	ОП2	ОП3	ОП4	ОП5	ОП6	ОП7	ОП8
Процессы	А1								
	А2			Ч		Ч		Ч	Ч
	А3	Ч	З						
Файлы	А4								
	А5			Ч		Ч		Ч	Ч
	А6	Ч		Ч, З	Ч, З				
	А7	Ч		З	Ч	Ч		Ч	
	А8		Ч	Ч		Ч, З	Ч, З		Ч
	А9	З	Ч						
А10		Ч	Ч	Ч	Ч	Ч	Ч		

Возможна модификация данного метода путем объединения скрытых каналов с одними и теми же отправителем и получателем [8]. Данный метод может быть особенно полезен в случае, если взаимодействующие стороны используют более одного способа скрытой передачи информации, пытаясь построить несколько скрытых каналов с низкой пропускной способностью.

Другим методом идентификации скрытых каналов является метод, основанный на построении дерева скрытых информационных потоков. Дерево скрытых информационных потоков используется для целенаправленной идентификации скрытых каналов определенного вида в отличие от метода, основанного на матрице разделяемых ресурсов, где для идентификации всевозможных скрытых каналов строится единственная матрица. Можно поставить такие цели, как «идентификация скрытых каналов по памяти через атрибут *A*» [6], и создавать дерево скрытых информационных потоков для каждой поставленной цели. По сравнению с методом, основанным на матрице разделяемых ресурсов, рассматриваемый метод предлагает более простой способ идентификации скрытых каналов по памяти с использованием множественных ресурсов.

Таблица 2. Транзитивное замыкание матрицы разделяемых ресурсов

Элементарные операции / Атрибуты ресурсов		ОП1	ОП2	ОП3	ОП4	ОП5	ОП6	ОП7	ОП8
Процессы	А1								
	А2	Ч	Ч	Ч	Ч	Ч	Ч	Ч	Ч
	А3	Ч	Ч, З						
Файлы	А4								
	А5	Ч	Ч	Ч	Ч	Ч	Ч	Ч	Ч
	А6	Ч	Ч	Ч, З	Ч, З	Ч	Ч	Ч	Ч
	А7	Ч	Ч	Ч, З	Ч	Ч	Ч	Ч	Ч
	А8	Ч	Ч	Ч	Ч	Ч, З	Ч, З	Ч	Ч
	А9	Ч, З	Ч						
А10		Ч	Ч	Ч	Ч	Ч	Ч	Ч	Ч

Рассмотрим пример построения дерева скрытых информационных потоков, приведенный в [6]. Первым этапом построения дерева является анализ элементарных операций системы. Для каждой элементарной операции строятся три списка атрибутов: список 1 атрибутов, на значения которых ссылаются при выполнении операции; список 2 атрибутов, значения которых меняются при выполнении операции; список 3 атрибутов, значения которых возвращаются операцией. Элементарные операции и их свойства представлены в таблице 3.

Таблица 3. Элементарные операции

Элементарная операция	Список 1	Список 2	Список 3
ОП1	Г	А, Б	–
ОП2	А	Б	–
ОП3	Б	–	Б
ОП4	А	Б, В	А

С учетом описанных элементарных операций дерево скрытых информационных потоков [6], позволяющее идентифицировать скрытые каналы по памяти через атрибут А, представлено на рис. 1. Всевозможные пути построенного дерева от элементарных операций к требованию «Построение скрытого канала по памяти через атрибут А» дают перечень операций, необходимых для скрытой передачи информации.

При построении дерева использованы следующие обозначения:

— требование, необходимое для существования скрытого канала по памяти через атрибут А;

— логический элемент, означающий, что выходное требование выполняется, если выполняется хотя бы одно из входных требований;

— логический элемент, означающий, что выходное требование выполняется, если выполняются все входные требования;

— элементарная операция;

— символ, означающий, что выполнить требование невозможно.

Термин «распознавание», встречающийся в построенном дереве скрытых информационных потоков, означает способность процесса определить факт изменения значения атрибута, но не означает определение нового значения атрибута.

Еще один метод идентификации скрытых каналов в распределенных системах, представленный в [3], основан на построении диаграммы последовательности сообщений. Диаграмму последовательности сообщений можно использовать для определения скрытых каналов по памяти на уровне технических требований на этапе разработки программного обеспечения, что позволяет принять решение о снижении пропускной способности или устранении канала на ранней стадии с минимальными затратами.

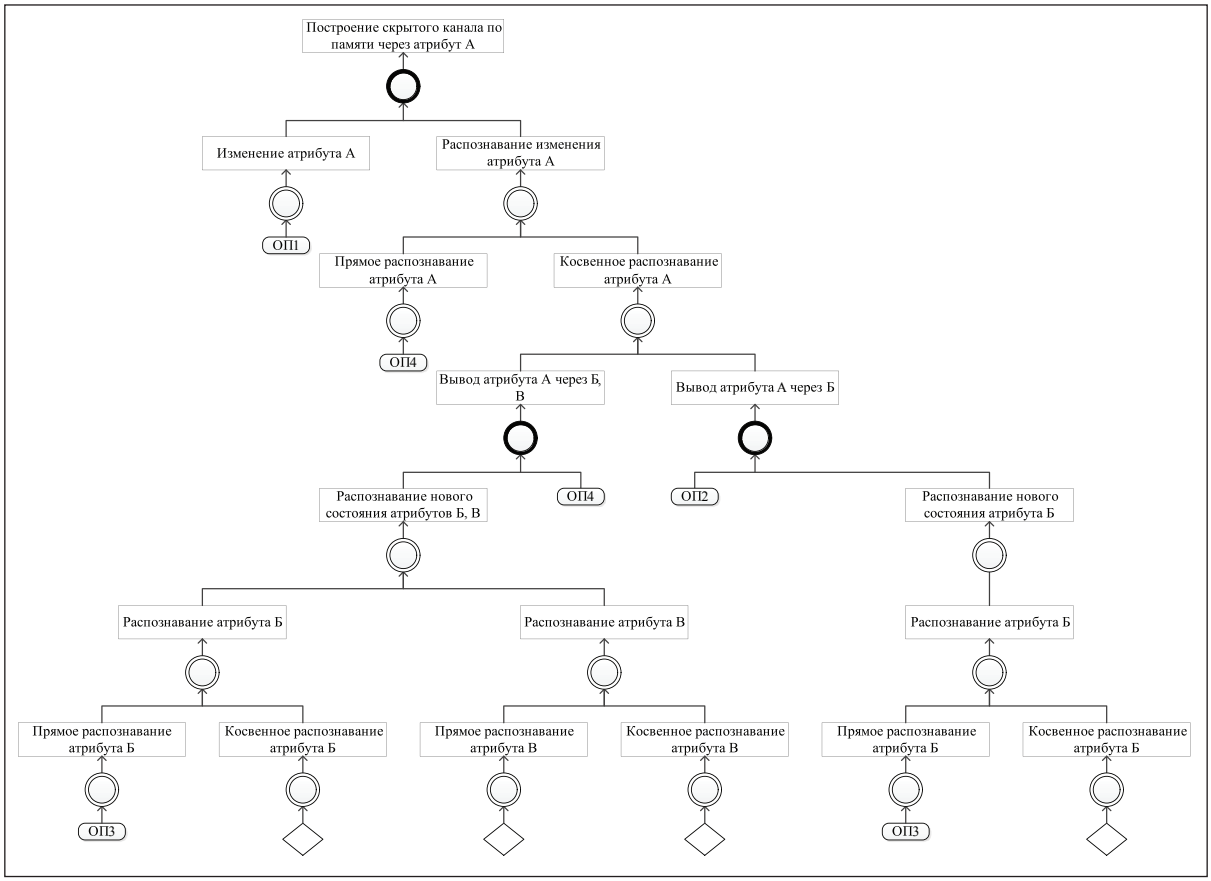

Рис. 1. Пример дерева скрытых информационных потоков

Данный метод основан на языке сценариев, что позволяет идентифицировать скрытые каналы передачи информации, которые являются следствием решений на стадии проектирования системы. Базовая диаграмма последовательности сообщений является графическим представлением взаимодействий в системе, где участвующие объекты представлены вертикальными линиями, а обмен сообщениями представлен стрелками от отправителей к получателям. Формально базовая диаграмма последовательности сообщений представляет собой кортеж $M = \langle E, \leq, A, I, \alpha, \varphi, m \rangle$, где

E — множество событий;

$\leq$ — отношение частичного порядка на множестве E;

A — множество меток событий;

I — множество объектов;

α — отображение множества E во множество A;

φ — отображение множества E во множество I;

m — отображение, связывающее отправление и получение данных.

На рис. 2 представлены пять различных примеров базовых диаграмм последовательностей сообщений (БДПС) [3].

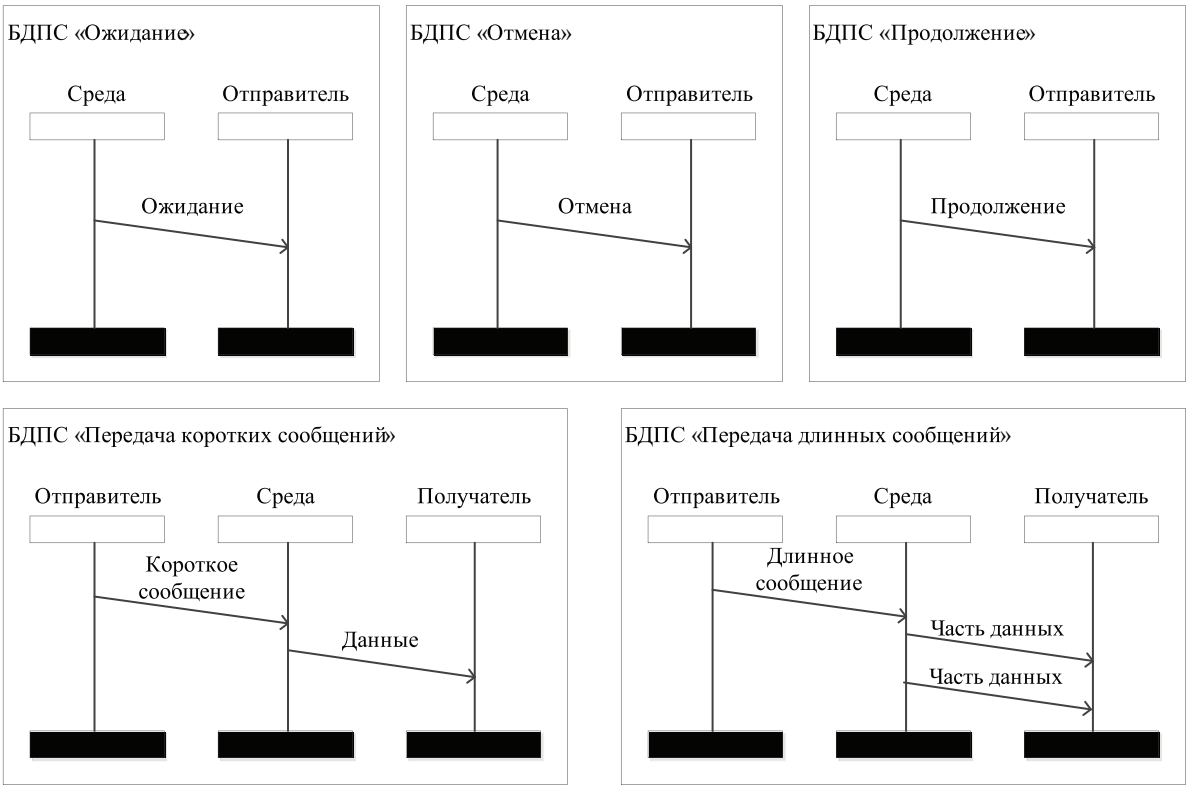

Рис. 2. Базовые диаграммы последовательностей сообщений

Для идентификации скрытых каналов построим высокоуровневую диаграмму последовательности сообщений на основе приведенных базовых диаграмм последовательностей сообщений. Данную диаграмму также опишем в виде кортежа $H = \langle N, \rightarrow, n_0, M \rangle$, где

N — множество узлов;

M — множество базовых диаграмм последовательностей сообщений;

$\rightarrow$ — некоторое подмножество множества $N \times M \times N$;

n_0 — начальный узел.

Высокоуровневая диаграмма последовательности сообщений на основе базовых диаграмм, приведенных на рис. 2, представлена на рис. 3. Диаграмму представим в виде

помеченного ориентированного графа, вершины которого — элементы множества $N = \{n_1, n_2, n_3, n_4\}$. Рассматриваемый метод идентификации скрытых каналов основан на анализе циклов высокоуровневой диаграммы последовательности сообщений [3].

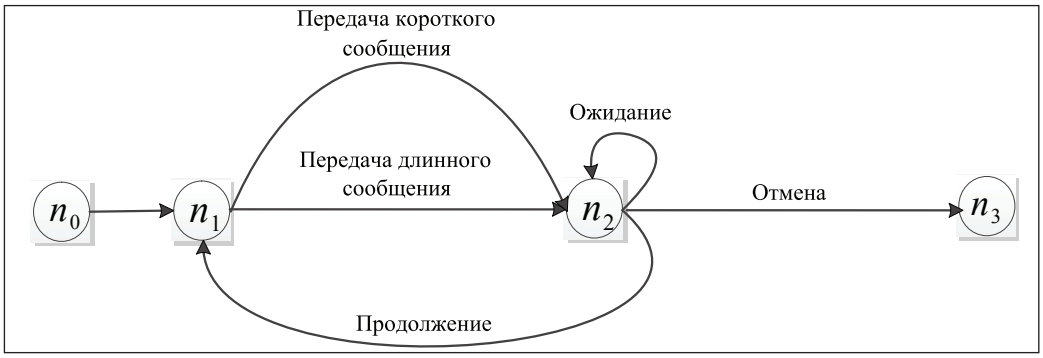

Рис. 3. Высокоуровневая диаграмма последовательности сообщений

За исключением метода, основанного на матрице разделяемых ресурсов, ни один из представленных методов не направлен на определение скрытых каналов по времени. Кроме того, данные методы зависят от вклада системного аналитика в алгоритм идентификации скрытых каналов. Следовательно, все предложенные методы требуют определения всех атрибутов разделяемых ресурсов вручную. Однако скрытые каналы используют для передачи информации атрибут ресурса, который изначально не предполагалось использовать как средство передачи информации (например, головку цилиндра диска [9, 10]). Таким образом, существует возможность, что один из таких атрибутов может быть упущен, а с использованием данного атрибута будет построен скрытый канал.

2. Анализ скрытых каналов

Следующим шагом в противодействии скрытым каналам является анализ каждого идентифицированного на первом этапе скрытого канала с целью оценки ущерба, который несет функционирование канала. Первостепенной задачей является определение количества информации, которое можно передать с использованием идентифицированных каналов, что используется для выявления каналов с высокой пропускной способностью.

Пропускную способность скрытых каналов по памяти можно анализировать, используя модели Маркова, применяя их как к каналам с шумом, так и к каналам без шума [11]. Однако предположения, требуемые для применения модели Маркова, фактически не выполнимы в реальных системах. Более общий подход к анализу скрытых каналов — оценка их пропускной способности путем применения результатов теории информации, то есть с использованием понятия Шеннона о пропускной способности [12]. В теории информации пропускная способность канала определяется как максимальная скорость передачи информации. Для каналов без шума пропускная способность C может быть определена следующим образом [13]:

$$C = \lim_{t \to \infty}\left(\frac{\log(N(t))}{t}\right),$$

где $N(t)$ — количество бит, которые возможно передать за время t.

Рассмотрим другой способ [14] определения пропускной способности с помощью средней взаимной информации. Пусть X, Y — две случайные величины, описывающие входные и выходные характеристики канала соответственно. Если скрытый канал является каналом без шума, то $I(X,Y) = I(X)$. Для каналов по времени количество взаимной информации за единицу времени определяется в виде формулы:

$$I_t = \frac{I(X,Y)}{E(T)},$$

где $E(T)$ — среднее время, требуемое для передачи одного символа.

Для каналов по памяти $E(T)$ — это выбранный в качестве параметра интервал времени. Очевидно, для каналов без шума [13, 15]:

$$I_t = \frac{I(X)}{E(T)}.$$

Тогда пропускную способность можно рассчитать по формуле:

$$C = \max_X (I_t).$$

Очевидно, предложенные методы (асимптотический анализ пропускной способности и анализ на основе количества взаимной информации) являются равноценными при анализе каналов без шума. Однако анализ пропускной способности на основе количества взаимной информации легко расширить для исследования каналов с шумом.

Авторами [16] рассмотрены бинарные скрытые каналы с шумом, где один из символов передается с вероятностью, равной единице. Скрытый канал по памяти данного вида существует, в частности, в протоколе двухфазной фиксации транзакций, как показано в [17]. Такие скрытые каналы называются Z-каналами.

Для каналов, схематично представленных на рис. 4, если отправитель передает «0», то получатель на выходе также примет «0»; однако если отправитель передает «1», то получатель примет «1» лишь с вероятностью ρ, $0 < \rho < 1$. Пусть u — вероятность того, что отправитель передает «1». Тогда пропускная способность Z-канала определяется следующим выражением исходя из анализа количества взаимной информации [18]:

$$C = \max_u (H(up;1-up) - uH(p,q)).$$

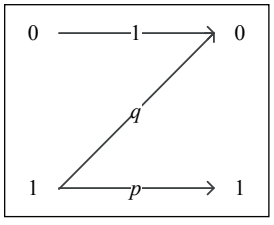

Рис. 4. Схема передачи информации по Z-каналу

Пропускная способность Z-каналов по времени детально проанализирована авторами [16] с учетом анализа времени передачи каждого символа.

Пропускная способность — не единственная мера, которая может использоваться при анализе скрытых каналов. Более того, пропускная способность — асимптотическая мера, которая может ввести в заблуждение. В частности, скрытый канал с нулевой пропускной способностью можно использовать для передачи коротких сообщений, например, для подачи злоумышленником команд агенту для выполнения. Рассмотрим бинарный канал без шума [19], в котором для передачи n-го символа требуется 2^{n-1} тактов.

С одной стороны, пропускная способность построенного скрытого канала равна нулю:

$$C = \lim_{n\to\infty} \frac{\log 2^n}{\sum_{i=0}^{n-1} 2^i} = \lim_{n\to\infty} \frac{n}{2^n - 1} = 0.$$

С другой стороны, сообщение любой длины может быть передано через такой канал передачи информации без шума. Для того чтобы проанализировать такие каналы, авторы [19] вводят критерий коротких сообщений, в котором указаны три фактора, которые должны быть приняты во внимание при анализе скрытых каналов:

1) длина передаваемого сообщения;

2) порог допустимого искажения сообщения при передаче, такой, что передача более искаженного сообщения не будет представлять угрозу безопасности;

3) временной промежуток, в течение которого передача сообщения является актуальной для злоумышленника.

Критерий коротких сообщений необходимо использовать в сочетании с расчетом пропускной способности скрытого канала.

3. Устранение и ограничение пропускной способности скрытых каналов

После идентификации и анализа скрытого канала необходимо устранить канал или ограничить его пропускную способность. Очевидно, пропускная способность скрытого канала может быть ограничена путем настройки параметров, которые фигурируют в формулах пропускной способности. Однако использовать такой метод ограничения пропускной способности скрытых каналов в системах с высоким уровнем обеспечения безопасности и производительности непросто, поэтому необходимы более сложные схемы устранения и ограничения пропускной способности скрытых каналов.

Одной из таких возможных схем является внедрение шума в скрытый канал, что понижает пропускную способность канала, и разъединение системных часов отправителя и получателя. Случайные прерывания порождают случайные сдвиги системных часов с целью нарушения работы системных часов на объектах с разными уровнями доступа [20]. В результате отправитель и получатель скрытого канала не могут совместно использовать системные часы, а значит, не могут построить скрытый канал, используя системные часы в качестве общего ресурса.

Другой способ ограничить пропускную способность скрытого канала, но в то же время обеспечить высокий уровень производительности системы — это использовать так называемый насос данных (от англ. data pump). Данная схема взаимодействия пользователя с высоким уровнем доступа и пользователя с низким уровнем доступа представлена на рис. 5 [21, 22]. «Насос данных» — это буфер для промежуточного хранения данных, контролирующий передачу информации между объектами с разными уровнями доступа. «Насос данных» выполняет следующие функции:

1) хранит сообщение, отправленное пользователем с низким уровнем доступа;

2) уведомляет пользователя с низким уровнем доступа о получении сообщения;

3) передает сообщение пользователю с высоким уровнем доступа;

4) ожидает подтверждения получения сообщения от пользователя с высоким уровнем доступа.

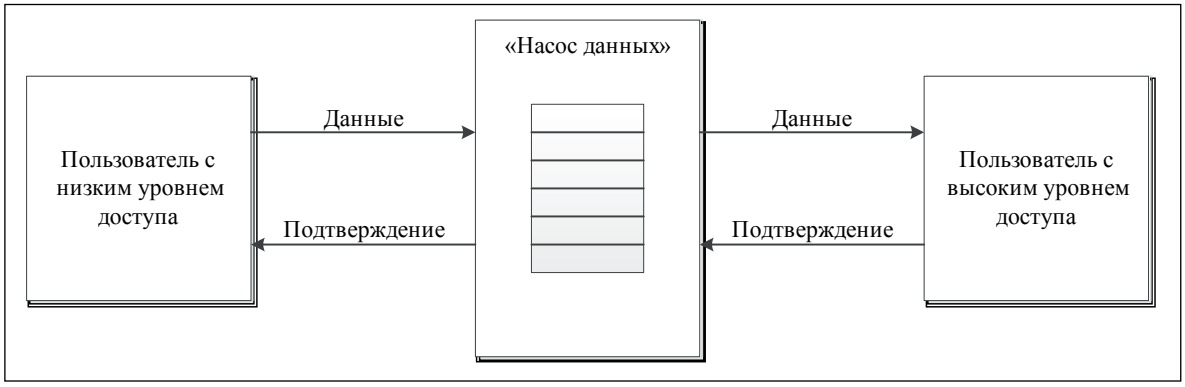

Рис. 5. Схема работы «насоса данных»

Однако если скорость подтверждения получения сообщения пользователем с высоким уровнем доступа ниже скорости передачи сообщения пользователем с низким уровнем доступа, то скрытый канал может быть построен следующим образом. Пользователь с низким уровнем доступа посылает непрерывные сообщения, пока не перестанет получать подтверждения получения посылаемых сообщений. Таким образом, пользователь с низким уровнем доступа блокирует «насос данных». Тогда пользователь с высоким уровнем доступа удаляет одно из сообщений в очереди,

чтобы послать «1», и бездействует, чтобы послать «0». В таком случае, если пользователь с низким уровнем доступа получает подтверждение в течение определенного промежутка времени, то записывает «1», если нет — «0».

Существование этого канала возможно, только если скорость подтверждения получения сообщения пользователем с высоким уровнем доступа не выше, чем скорость передачи сообщения пользователем с низким уровнем доступа. Поэтому очевидный способ устранить такой скрытый канал — уменьшить скорость передачи сообщения пользователем с низким уровнем доступа до скорости подтверждения получения сообщения пользователем с высоким уровнем доступа.

Усовершенствованная модель «насоса данных», разработанная авторами [21, 23], значительно уменьшает пропускную способность описанного скрытого канала. «Насос данных» использует среднее значение скорости подтверждения получения сообщения пользователем с высоким уровнем доступа в качестве скорости передачи подтверждения пользователю с низким уровнем доступа. При каждом полученном пакете подтверждения от пользователя с высоким уровнем доступа среднее значение скорости подтверждения получения сообщения пользователем с высоким уровнем доступа обновляется. После получения сообщения от пользователя с низким уровнем доступа доверенный процесс на стороне «насоса данных», взаимодействующий с пользователем с низким уровнем доступа, отправляет сообщение в буфер. Данный процесс посылает подтверждение пользователю с низким уровнем доступа после временной задержки, являющейся случайной величиной, математическое ожидание которой есть средняя скорость подтверждения получения сообщения пользователем с высоким уровнем доступа. Эта усовершенствованная схема работы «насоса данных» представлена на рис. 6. При помощи данной схемы невозможно полное устранение скрытого канала, описанного выше, однако его пропускная способность значительно ограничена.

На рис. 6 цифрами обозначены: 1 — доверенный процесс, взаимодействующий с пользователем с низким уровнем доступа; 2 — доверенный процесс, взаимодействующий с пользователем с высоким уровнем доступа.

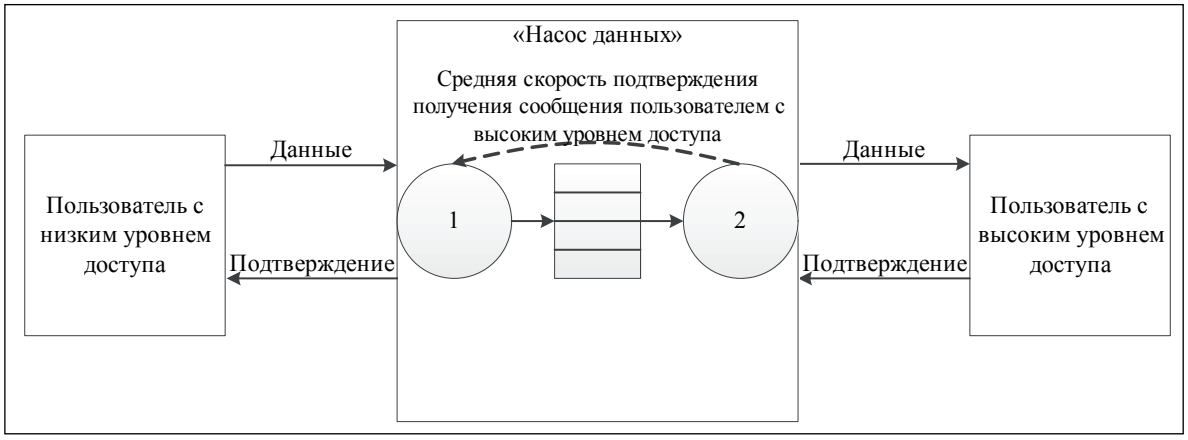

Рис. 6. Схема работы усовершенствованного «насоса данных»

В заключение данного раздела заметим, что авторами [24] разработан высокоскоростной однонаправленный шлюз, обеспечивающий гарантированную доставку данных с исключением возможности обратной передачи, реализуемой с использованием скрытых каналов. Разработанный шлюз предполагает использование протокола UDP в качестве протокола транспортного уровня и позволяет, в случае канала с пропускной способностью 10 Гбит/с, передавать информацию со скоростью 3,3 Гбит/с.

4. Аудит и обнаружение скрытых каналов

Другим важным этапом противодействия передаче информации по скрытым каналам является их аудит и обнаружение. Аудит и обнаружение скрытых каналов применяются для обнаружения вредоносной активности по следующим причинам. Во-первых, это обеспечение механизма препятствования функционированию скрытых каналов. Во-вторых, большинство методов идентификации скрытых каналов требует ввода данных системным аналитиком (в частности, указания общих ресурсов). Из-за человеческого фактора некоторые скрытые каналы могут оставаться неидентифицированными. Аудит и обнаружение могут помочь зарегистрировать такие каналы. В-третьих, устранение скрытых каналов может быть весьма дорогостоящей процедурой для систем с высокой производительностью. В таком случае можно принять решение об аудите канала, а не устранении.

Авторами [25] предложена схема аудита, в рамках которой определяются общие ресурсы для каждого потенциально скрытого канала по памяти и используются векторы аудита для того, чтобы однозначно определить, кто и в каком порядке просматривает или изменяет общие ресурсы. Каждый вектор представляет собой набор из трех элементов:

1) системная переменная или атрибут, который может быть изменен для скрытой передачи информации;

2) элементы доверенной вычислительной базы, которые могут изменять системную переменную или атрибут;

3) элементы доверенной вычислительной базы, которые могут определить значение или распознать изменение значения системной переменной или атрибута.

Обнаружение определенных скрытых каналов производится путем анализа построенных векторов аудита. После обнаружения скрытого канала его следует проанализировать, в частности, оценив его пропускную способность.

Задачу обнаружения скрытых каналов можно классифицировать как обнаружение в режиме реального времени и обнаружение посредством обработки информации из журнала аудита за некоторый период времени. Для методов обнаружения в режиме реального времени важна скорость обнаружения для их эффективного использования при анализе небольшого количества данных. Вторая группа методов обнаружения решает задачу более полного анализа с использованием необходимого для работы метода количества данных. Заметим, что обе группы методов обнаружения существенным образом зависят от качества журнала аудита, создаваемого схемами аудита, одна из которых кратко рассмотрена выше.

Заключение

Обобщая описанные в статье методы идентификации и анализа скрытых каналов, их устранения и ограничения пропускной способности, а также аудита и обнаружения, приведем порядок организации защиты информации, информационных технологий и автоматизированных систем от атак, реализуемых с использованием скрытых каналов [26]. Данный процесс является циклическим и включает в себя следующие этапы, повторяющиеся на каждой из итераций процесса:

1) анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов;

2) выявление скрытых каналов и оценка их опасности для активов организации;

3) реализация защитных мер по противодействию скрытым каналам;

4) организация контроля за противодействием скрытым каналам.

СПИСОК ЛИТЕРАТУРЫ:

1. Department of defence standard. Department of defence trusted computer system evaluation criteria. 1985.
2. *Bishop M.* Computer security: art and science. Boston: Addison Wesley professional, 2002.
3. *Helouet L., Jard C., Zeitoun M.* Covert channels detection in protocols using scenarios // Proceedings of the 2003 workshop on security protocols verification. 2003. P. 21–25.
4. *Kemmerer R. A.* Shared resource matrix methodology: an approach to identifying storage and timing channels // ACM Transactions on computer systems. 1983. Vol. 1. № 3. P. 256–277.
5. *Denning D. E.* A lattice model of secure information flow // Communications of the ACM. 1976. Vol. 19. № 5. P. 236–243.
6. *Porras P. A., Kemmerer R. A.* Covert flow trees: a technique for identifying and analyzing covert storage channels // Proceedings of the 1991 IEEE Computer society symposium on research in security and privacy. 1991. P. 36–51.
7. *Tsai C.-R., Gligor V., Chandersekaran C.* A formal method for the identification of covert storage channels in source code // Proceedings of the 1987 IEEE Computer society symposium on research in security and privacy. 1987. P. 74–87.
8. *Schaefer M., Gold B. B., Linde R., Scheid J.* Program confinement in KVM/370 // Proceedings of the 1977 ACM Annual conference. 1977. P. 404–410.
9. *Karger P. A., Wray J. C.* Storage channels in disk arm optimization // Proceedings of the 1991 IEEE Computer society symposium of research in security and privacy. 1991. P. 52–61.
10. *Wang C., Ju S.* Searching covert channels by identifying malicious subjects in the time domain // Proceedings of the fifth annual IEEE SMC Information assurance workshop. 2004. P. 68–73.
11. *Tsai C.-R., Gligor V.* A bandwidth computation model for covert storage channels and its applications // Proceedings of the 1991 IEEE Computer society symposium on research in security and privacy. 1988. P. 108–121.
12. *Shannon C. E., Weaver W.* The mathematical theory of communication. Urbana: The University of Illinois press, 1964.
13. *Millen J.* Finite-state noiseless covert channels // Proceedings of the 1989 Computer security foundation workshop. 1989. P. 81–85.
14. *Cabuk S.* Network Covert Channels: design, analysis, detection, and elimination. For the degree of doctor of philosophy. Indiana: Perdue University, 2006.
15. *Moskowitz I. S., Miller A. R.* Simple timing channels // Proceedings of the 1994 IEEE Computer society symposium on research in security and privacy. 1994. P. 56–64.
16. *Moskowitz I. S., Greenwald S. J., Kang M. H.* An analysis of the timed Z-channel // Computer society symposium on research in security and privacy. 1996. P. 2–11.
17. *Costich O. L., Moskowitz I. S.* Analysis of a storage channel in the two-phase commit protocol // Proceedings of the fourth computer security foundation workshop. 1991. P. 201–208.
18. *Golomb S. W.* The limiting behavior of the Z-channel // Proceedings of the 1980 IEEE International symposium on information theory. 1980. P. 372.
19. *Moskowitz I. S., Kang M. H.* Covert channels – Here to stay? // Proceedings of the Ninth Annual Conference on computer assurance. 1994. P. 235–244.
20. *Hu W.-M.* Reducing timing channels with fuzzy time // Journal of computer security. 1992. Vol. 1. № 3–4. P. 362–372.
21. *Kang M. H., Moskowitz I. S.* A pump for rapid, reliable, secure communication // Proceedings of the first ACM Conference on computer and communications security. 1993. P. 119–129.
22. *Kang M. H., Moskowitz I. S.* A data pump for communication. Washington: Naval research laboratory, 1995.
23. *Kang M. H., Lee D. C., Moskowitz I. S.* A network version of the pump // Proceedings of the 1995 IEEE Computer society symposium on research in security and privacy. 1995. P. 144–154.
24. *Архангельская А. В., Архангельский В. Г., Калмыков В. В.* О разработке архитектуры шлюза однонаправленной гарантированной передачи данных // Методы и технические средства обеспечения безопасности информации: Материалы 22-й научно-технической конференции. СПб.: Изд-во Политехн. ун-та, 2013. С. 52–55.
25. *Shieh S.-P., Gligor V. D.* Auditing the use of covert storage channels in secure systems // Proceedings of the 1990 IEEE Computer society symposium on research in security and privacy. 1990. P. 285–295.
26. ГОСТ Р 53113.2-2009. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов. Введ. 2009-12-01. М.: Стандартинформ, 2010.