A.I. Belozubova, K.G. Kogos, M.A. Finoshin

The Analysis of Existing Methods to Prevent the Data Leakage Using Covert Channels in IP Networks

Keywords: covert channels, storage channels, timing channels, capacity, limitation, elimination, detection.

Covert channels in IP networks are investigated. The possibilities adversary needs to construct covert channels are given. Current methods of covert channels elimination, detection and capacity limitation are examined. Detection methods are compared using such criteria: alpha and beta errors, an ability of implementation.

А.И. Белозубова, К.Г. Когос, М.А. Финошин

АНАЛИЗ СУЩЕСТВУЮЩИХ СПОСОБОВ ПРОТИВОДЕЙСТВИЯ УТЕЧКЕ ИНФОРМАЦИИ ПО СКРЫТЫМ КАНАЛАМ В IP-СЕТЯХ

Введение

Термин «скрытый канал» впервые введен авторами [1] в 1973 году. В стандарте [2] под скрытым каналом понимается непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности. Требования доверия к безопасности информации, установленные в [3], предполагают, что для систем с оценочным уровнем доверия не ниже пятого предусмотрено проведение обязательного анализа скрытых каналов.

Возможности протокола IP позволяют негласно передавать информацию и строить скрытые каналы, модулируя временные характеристики, значения полей заголовков и длины передаваемых пакетов. Однако известные меры противодействия данной угрозе, состоящие в "нормализации" параметров IP-трафика (т.е., в передаче IP-пакетов фиксированной длины с фиксированными заголовками через равные промежутки времени), приводят к существенному снижению эффективности использования пропускной способности каналов связи, увеличению стоимости их использования и потере функциональных возможностей протокола IP. Широкое распространение протокола IP делает задачу исследования скрытых каналов в IP-сетях актуальной.

Авторами [4] предложена методика противодействия утечке информации по скрытым каналам в IP-сетях, включающая в себя следующие этапы: идентификация, анализ, устранение, ограничение пропускной способности, аудит и обнаружение. Устранение возможности построения части скрытых каналов в IP-сетях приводит к недопустимому ограничению остаточной пропускной способности канала связи. Поэтому после анализа потенциального скрытого канала принимается решение либо о превентивном ограничении его пропускной способности, либо об обнаружении факта передачи информации по данному каналу. Данная статья представляет аналитический обзор существующих методов ограничения пропускной способности и обнаружения скрытых каналов в IP-сетях.

Систематизация способов передачи информации по скрытым каналам в IP-сетях

Традиционно, скрытые каналы по механизму передачи информации разделяют на каналы по памяти и каналы по времени. На рис. 1 приведено продолжение данного разбиения для скрытых каналов в IP-сетях.

Определить скрытые каналы по памяти и времени можно в виде списка условий. Скрытый канал является каналом по памяти при выполнении следующих условий [5]:

- отправитель и получатель должны иметь доступ к элементу общего ресурса;
- отправитель имеет возможность изменить этот элемент разделяемого ресурса;
- получатель должен иметь возможность распознать такое изменение;
- отправитель и получатель имеют возможность инициировать такой диалог, т.е., используют канал с низкой пропускной способностью;
- если не выбран специальный метод кодирования во избежание последовательности одинаковых символов, отправитель и получатель должны иметь возможность предварительно договориться о временном интервале, в течение которого получатель будет наблюдать за изменениями в канале.

Аналогично, скрытый канал является каналом по времени при выполнении следующих условий [5]:

- отправитель и получатель должны иметь доступ к элементу общего ресурса;
- отправитель и получатель должны разделять основную частоту (синхронизация);
- отправитель должен иметь возможность изменять время ответного сигнала получателя для выявления изменения в данном элементе разделяемого ресурса;
- отправитель и получатель могут инициировать такой диалог, т.е., используют канал с низкой пропускной способностью.

Рис. 1. Систематизация скрытых каналов в IP-сетях

Для дальнейшего рассуждения выделены следующие группы способов передачи информации по скрытым каналам в IP-сетях:

К1 – изменение полей заголовков передаваемых пакетов;

К2 – изменение длин передаваемых пакетов;

К3 – изменение длин межпакетных интервалов;

К4 – переупорядочивание пакетов, подлежащих отправке.

В оставшейся части статьи не рассматриваются скрытые каналы по времени, основанные на изменении скорости передачи пакетов, так как такие каналы считаются не стойкими к обнаружению. Возможности нарушителя, необходимые для построения скрытых каналов типов К1-К4, представлены в табл. 1: «Да» означает, что данная возможность нарушителя может быть использована для построения скрытого канала; «Нет» – возможность нарушителя не позволяет построить скрытый канал.

Иногда к скрытым каналам относят также каналы, в которых для сокрытия информации используют поле «Данные» пакета. Информация передается в поле «Данные», которое и является контейнером для передачи данных. С другой стороны, данные каналы не предполагают нарушения правил политики безопасности. Поэтому описанные каналы передачи информации не отнесены к классу скрытых каналов.

Таблица 1. Возможности нарушителя, необходимые для построения скрытых каналов

Возможности нарушителя, необходимые для построения скрытых каналов	Способы построения скрытых каналов			
	К1	К2	К3	К4
Изменение содержимого полей пакетов	Да	Нет	Нет	Да
Изменение длин передаваемых пакетов	Нет	Да	Нет	Нет
Формирование фиктивных пакетов	Да	Да	Да	Нет
Буферизация пакетов, подлежащих отправке, и передача в определенный момент времени	Нет	Да	Да	Да
Добавление случайных временных задержек при передаче пакетов	Нет	Нет	Да	Нет

Ограничение пропускной способности скрытых каналов в IP-сетях

Скрытые каналы по памяти в IP-сетях типа К1 могут быть устранены путем шифрования либо нормализации значений полей заголовков пакетов. Таким образом, построение скрытых каналов данного вида невозможно при наличии шифрования трафика, что является стандартным способом сетевой защиты. Этой особенностью обладают и скрытые каналы по времени типа К4.

Выравнивание длин передаваемых пакетов и установление единой скорости передачи пакетов являются способами устранения скрытых каналов по памяти типа К2 и скрытых каналов по времени типа К3 соответственно. Однако данные методы приводят к существенному понижению остаточной пропускной способности канала связи. Параметры данных методов выбираются как компромисс между остаточной пропускной способностью скрытого канала и остаточной пропускной способностью самого канала связи.

В табл. 2 приведены способы устранения и ограничения пропускной способности скрытых каналов в IP-сетях типов К1-К4. Символы имеют следующие обозначения:

«+» – устранение возможности построения скрытого канала;

«±» – ограничение пропускной способности скрытого канала;

«–» – пропускная способность скрытого канала не ограничена.

Таблица 2. Способы ограничения пропускной способности скрытых каналов

Способы устранения и ограничения пропускной способности скрытых каналов	Способы построения скрытых каналов			
	К 1	К 2	К 3	К 4
С1 – Нормализация значений полей заголовков пакетов	+	–	–	+
С2 – Нормализация длин пакетов	–	+	–	–
С3 – Нормализация длин межпакетных интервалов	–	–	+	–
С4 – Фрагментация и агрегирование пакетов	–	±	±	±
С5 – Шифрование трафика	+	–	–	±
С6 – Генерация фиктивного трафика	±	±	±	±
С7 – Увеличение длин пакетов случайным образом перед отправкой [6]	–	±	–	–
С8 – Введение случайных задержек перед отправкой пакетов	–	–	±	±
С9 – Использование промежуточных шлюзов [7]	+	+	±	+
С10 – Установление нескольких допустимых скоростей передачи пакетов	–	–	+	–

Так как время следования пакета – случайная величина, имеющая характеристики, присущие гамма-распределению [8], ошибки при передаче информации по скрытому каналу, основанному на изменении длин межпакетных интервалов, могут привести к рассинхронизации отправителя и получателя. С другой стороны, способы ограничения пропускной способности С4, С6, С7, С8 также приводят к рассинхронизации. Необходимость периодической синхронизации также понижает пропускную способность скрытого канала. Авторами [9] предложены способы поддержания синхронизма отправителя и получателя, основанные на:

- отправке пакетов специального вида;
- введении «интервалов тишины» для изменения параметров кодирования;
- введении «интервалов регулировки» для изменения параметров кодирования в режиме реального времени;
- фазовой автоподстройке частоты.

Способы реализации методов ограничения пропускной способности С4, С6, С7, С8 разработаны авторами [10] путем расширении заголовка протокола IPSec. Перспективное направление дальнейших исследований – получение количественных характеристик данных методов, позволяющих понизить пропускную способность потенциального скрытого канала до значения, такого что функционирование скрытых каналов с меньшей пропускной способностью считается неопасным.

Обнаружение скрытых каналов по времени в IP-сетях

Альтернативой превентивному ограничению пропускной способности скрытых каналов является обнаружение функционирующих каналов. Преимуществом данного подхода – отсутствие дополнительной нагрузки на канал связи. Однако наличие ненулевых ошибок первого и второго рода, а также вероятность утечки критически важной информации до срабатывания метода делают необходимым применять методы обнаружения совместно с методами ограничения пропускной способности. В дальнейшем изложении рассмотрены методы обнаружения скрытых каналов по времени в IP-сетях,

основанные на модуляции длин межпакетных интервалов, так как известны не обнаруживаемые схемы передачи информации, основанные на модуляции длин передаваемых пакетов. С другой стороны, каналы по памяти, основанные на изменении битов заголовков пакетов, могут быть устранены путем шифрования трафика или нормализации значений полей заголовков.

Методы обнаружения скрытых каналов по времени в IP-сетях по принципу работы могут быть разделены на следующие группы:

- обнаружение путем сравнения с «эталонной» моделью трафика [11] (О1);
- обнаружение путем анализа закономерностей в потоке трафика (О2);
- обнаружение скрытых каналов, основанных на изменении длин межпакетных интервалов (О3).

Работа методов группы О1 заключается в оценке близости эмпирических функций распределения, отвечающих распределениям длин межпакетных интервалов в случаях отсутствия и предполагаемого наличия скрытого канала. Оценка близости происходит с использованием методов математической статистики: критерия согласия Пирсона [12] и теста Колмогорова-Смирнова [13]. Работа методов группы О2 основана на предположении, что при наличии скрытого канала трафик становится более предсказуем. Особый интерес представляет исследование методов групп О2 и О3, так как данные методы специальным образом спроектированы для обнаружения скрытых каналов в IP-сетях. Сравнительный анализ методов представлен в табл. 3.

Таблица 3. Сравнительный анализ методов обнаружения скрытых каналов в IP-сетях

<table>
<tr><th colspan="2" rowspan="2">Метод обнаружения</th><th colspan="3">Критерий сравнения</th></tr>
<tr><th>Ошибки 1 рода</th><th>Ошибки 2 рода</th><th>Возможность реализации</th></tr>
<tr><td colspan="2">Группа методов О3</td><td>При построении скрытого канала с высоким уровнем шума</td><td>Отсутствуют</td><td>–*</td></tr>
<tr><td rowspan="6">Группа методов О2</td><td>Анализ дисперсии [9]</td><td>При введении шума, изменении схемы кодирования</td><td rowspan="6">При передаче пакетов с максимальной скоростью</td><td>+</td></tr>
<tr><td>Метод «ε-близости» [9]</td><td>При введении шума</td><td>+</td></tr>
<tr><td>Анализ колмогоровской сложности [13]</td><td>Зависят от выбора схемы подсчета колмогоровской сложности</td><td>–</td></tr>
<tr><td>Анализ энтропии [13]</td><td rowspan="2">Зависят от параметров метода</td><td>_**</td></tr>
<tr><td>Анализ условной и скорректированной энтропии [13]</td><td>_***</td></tr>
</table>

Проведенные исследования показывают, что существующие методы обнаружения нельзя считать надежными: во всех методах имеется ненулевая ошибка первого рода при построении скрытого канала с шумом, введении шума и периодическом изменении

схемы кодирования. Однако параметры данных методов неизвестны: отсутствуют количественные характеристики (пропускная способность, уровень ошибок и так далее) скрытого канала, стойкого к существующим методам обнаружения. Перспективным направлением дальнейшей работы является анализ возможности построения скрытых каналов, не обнаруживаемых существующими методами обнаружения, и получение количественных характеристик таких каналов.

Заметим, что авторами [14,15] доказана возможность построения невидимого скрытого канала, если нарушителю известна схема обнаружения. Однако данные результаты носят аналитический характер: ввиду ограниченного спектра способов построения скрытых каналов и небольшого числа методов их обнаружения практическая применимость данных результатов при анализе скрытых каналов в IP-сетях незначительна.

Заключение

Данная статья представляет аналитический обзор существующих методов ограничения пропускной способности и обнаружения скрытых каналов в IP-сетях. Даны перспективные направления дальнейших исследований: оценка количественных характеристик некоторых методов ограничения пропускной способности, которые выбираются как компромисс между максимальной пропускной способностью скрытого канала и остаточной пропускной способностью самого канала связи, и оценка количественных характеристик стойкого к одному или нескольким методам обнаружения скрытого канала.

СПИСОК ЛИТЕРАТУРЫ:

1. Lampson B.W. A Note on the Confinement Problem // Communications of the ACM. 1973. С. 613-615.
2. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. – Введ. 2009-10-01. М.: Стандартинформ, 2009. 12 с.
3. ГОСТ Р 15408-3-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Введ. 2002-04-04. М.: ИПК Издательство стандартов, 2002. – 108 с.
4. Архангельская А.В., Когос К.Г. О подходе к противодействию утечке информации по скрытым каналам // Безопасность информационных технологий. 2013. Выпуск 4. С. 10-20.
5. KemmererR.A. Sharedresourcematrixmethodology: anapproachtoidentifyingstorageandtimingchannels // ACMTransactionsoncomputersystems. 1983. Vol. 1, No. 3. С. 256-277.
6. Архангельская А.В., Когос К.Г. Пропускная способность скрытых каналов, основанных на модуляции длин передаваемых пакетов, при увеличении длин пакетов случайным образом // Методы и технические средства обеспечения безопасности информации: Материалы 23-й научно-технической конференции. СПб.: Изд-во Политехн. ун-та. 2014. С. 40-42.
7. 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.
8. Yao L., Zi X., Pan L., Li J. A study of on/offtiming channel based on packet delay distribution // Computers and security. 2009. Vol. 28, No. 8. С. 785-794.
9. Cabuk S., Brodley C.E., Shields C. IP covert timing channels: design and detection // Proceedings of the eleventh ACM conference on computer and communications security. 2004. С. 178-187.
10. Kiraly C., Teofili S., Bianchi G., Cigno R. Lo, Nardelli M., Delzeri E.Traffic flow confidentially in IPsec: protocol and implementation // The International federation for information processing. 2008. Vol. 262.
11. Berk V., Giani A., Cybenko G. Detection of covert channel encoding in network packet delays: Technical report TR2005-536. – New Hampshire: Thayer school of engineering of Dartmouth college, 2005. Режим доступа: http://www.ists.dartmouth.edu/library/149.pdf. – 01.06.2013.
12. Никулин М.С. О критерии хи-квадрат для непрерывных распределений // Теория вероятностей и ее применения. 1973. С. 675-676.
13. Walls R.J., Kothari K., Wright Liquid M. A detection-resistant covert timing channel based on IPD shaping // Computer networks. 2011. Vol. 55, issue 6. С. 1217-1228.

14. Грушо А. А. Скрытые каналы и безопасность информации в компьютерных системах // Дискретная математика. 1998. Том 10. Выпуск 1. – С. 3-9.
15. Грушо А. А. О существовании скрытых каналов // Дискретная математика. 1999. Том 11. Выпуск 1. С. 24-28.

REFERENCES:

1. Lampson B.W. A Note on the Confinement Problem // Communications of the ACM. 1973. P. 613-615.
2. GOSTR 53113.1-2008. Informationtechnology. Zaschitainformatcionnyhtechnologijiavtomatizirovannyhsistemotugroz, realizyemyhsispolzovaniemskrytyhkanalov. Chast 1. Obschie polozheniyza. Vved. 2009-10-01. M.: Standartinform, 2009. 12 p.
3. ГОСТ Р 15408-3-2008. Information technology. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnyh technologij. Chast 3. Trebovaniya doveriya k bezopasnosti. Vved. 2002-04-04. M.: IPK: Izdatelstvo standertov, 2002. 108 p.
4. Arkhangelskaya A.V., Kogos K.G.O podhode k protivodeistviu utechke informatsii po skrytym kanalam // Bezopasnost informatsionnyh technologij. 2013. Vypusk 4. P. 10-20.
5. KemmererR.A. Sharedresourcematrixmethodology: anapproachtoidentifyingstorageandtimingchannels // ACMTransactionsoncomputersystems. 1983. Vol. 1, No. 3. P. 256-277.
6. Arkhangelskaya A.V., Kogos K.G.Propusknaya sposobnost skrytyh kanalov, osnovannyh na modulyatsii dlin peredavaemyh paketov, pri uvelichenii dlin paketov sluchainym //Metody i technicheskie sredstva obespecheniya bezopasnosti informatsii: Materialyof 23thnauchno-technicheskoi konferentsii. SPb.: Izd-voPoliitehn. un-ta. 2014. P. 40-42.
7. Arkhangelskaya A.V., Arkhangelskij V.G., KalmykovV.V. O razrabotke architektury shluza odnonapravlennoi garantirovannoi peredachi dannyh //Metody i technicheskie sredstva obespecheniya bezopasnosti informatsii: Materialyof 22thnauchno-technicheskoi konferentsii. SPb.: Izd-voPoliitehn. un-ta. 2013. P. 52-55.
8. Yao L., Zi X., Pan L., Li J. A study of on/offtiming channel based on packet delay distribution // Computers and security. 2009. Vol. 28, No. 8. P. 785-794.
9. Cabuk S., Brodley C.E., Shields C. IP covert timing channels: design and detection // Proceedings of the eleventh ACM conference on computer and communications security. 2004. P. 178–187.
10. Kiraly C., Teofili S., Bianchi G., Cigno R. Lo, Nardelli M., Delzeri E. Traffic flow confidentially in IPsec: protocol and implementation // The International federation for information processing. 2008. Vol. 262.
11. Berk V., Giani A., Cybenko G. Detection of covert channel encoding in network packet delays: Technical report TR2005-536. – New Hampshire: Thayer school of engineering of Dartmouth college, 2005. Режим доступа: http://www.ists.dartmouth.edu/library/149.pdf. – 01.06.2013.
12. Nikulin M.S. O kriterii hi kvadrat dlya nepreryvnyh raspredelenij // Teorija veroyatnostej i ee primeneniya. 1973. P. 675-676.
13. Walls R.J., Kothari K., Wright LiquidM. A detection-resistant covert timing channel based on IPD shaping // Computer networks. 2011. Vol. 55, issue 6. P. 1217-1228.
14. Grusho A.A. Skrytye kanaly i bezopasnost informatsii v komputernyh sistemah // Diskretnaya matematika. 1998. T. 10. Vypusk 1. P. 3-9.
15. Grusho A.A. O suschestvovanii skrytyh kanalov // Diskretnaya matematika. 1999. T. 11. Vypusk 1. P. 24-28.