Константин Г. Когос[1], Михаил А. Финошин[2], Сергей В. Айрапетян[3]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, Москва, 115409, Россия
[1]*e-mail: KGKogos@mephi.ru, https://orcid.org/0000-0002-8090-678X*
[2]*e-mail: MAFinoshin@mephi.ru, https://orcid.org/0000-0003-4374-1645*
[3]*e-mail: sergey.hayrapetyan@mail.ru, https://orcid.org/0000-0002-3415-8530*

МЕТОД ИДЕНТИФИКАЦИИ СКРЫТЫХ КАНАЛОВ ПО ПАМЯТИ В СЕТЯХ ПАКЕТНОЙ ПЕРЕДАЧИ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2021.3.04

Аннотация. Целью статьи является описание разработанного метода идентификации сетевых скрытых каналов. Традиционно схему противодействия утечке информации по скрытым каналам разделяют на несколько этапов. Первым этапом является идентификация скрытых каналов – выявление потенциально возможных скрытых каналов в системе. Для идентификации скрытых каналов используются методы, основанные на матрице разделяемых ресурсов, дереве скрытых информационных потоков и графе скрытых информационных потоков. При этом возникает необходимость конкретизировать формальное описание этапов вышеуказанных методов идентификации в случае сетевых скрытых каналов. В статье приведено описание разработанного метода идентификации сетевых скрытых каналов по памяти, а также результаты тестирования программной реализации данного метода, для скрытого канала, основанного на изменении поля TTL заголовка IP-пакета. Результаты могут быть расширены и для других сетевых скрытых каналов по памяти в IP сетях, основанных на изменении полей заголовков пакетов.
Ключевые слова: скрытый канал, метод идентификации, общий ресурс, атрибут, информационный поток.
Для цитирования: КОГОС, Константин Г.; ФИНОШИН, Михаил А.; АЙРАПЕТЯН, Сергей В. МЕТОД ИДЕНТИФИКАЦИИ СКРЫТЫХ КАНАЛОВ ПО ПАМЯТИ В СЕТЯХ ПАКЕТНОЙ ПЕРЕДАЧИ ДАННЫХ. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 56–64, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1362. DOI: http://dx.doi.org/10.26583/bit.2021.3.04.

Konstantin G. Kogos[1], Mihail A. Finoshin[2], Sergey V. Airapetyan[3]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe highway, 31, Moscow, 115409, Russia
[1]*e-mail: KGKogos@mephi.ru, https://orcid.org/0000-0002-8090-678X*
[2]*e-mail: MAFinoshin@mephi.ru, https://orcid.org/0000-0003-4374-1645*
[3]*e-mail: sergey.hayrapetyan@mail.ru, https://orcid.org/0000-0002-3415-8530*

Method for identifying network covert channels

DOI: http://dx.doi.org/10.26583/bit.2021.3.04

Abstract. The aim of this paper is to describe the created method for identifying network covert channels. Traditionally, the scheme for countering information leakage through covert channels is divided into several stages. The first stage is the covert channels identification, that is, the identification of potentially possible covert channels in the system. To identify covert channels, methods based on a shared resources matrix, a tree of covert information flows and a graph of covert information flows are used. Thus, it becomes necessary to concretize the formal description of the stages of the above identification methods in the case of network covert channels. The article describes the created method for identifying network storage covert channels, as well as the results of testing the software implementation of this method for covert channel based on changing the TTL field of the IP packet header. The results can be extended for other network storage covert channels in IP networks, based on the packet header fields changes.
Keywords: covert channel, identification method, shared resource, attribute, information flow.
For citation: KOGOS, Konstantin G.; FINOSHIN, Mihail A.; AIRAPETYAN, Sergey V. Method for identifying

network covert channels. IT Security (Russia), [S.l.], v. 28, n. 3, p. 56-64, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1362. DOI: http://dx.doi.org/10.26583/bit.2021.3.04.

Введение

Понятие скрытого канала впервые было введено Лэмпсоном в [1]. Лэмпсон определил скрытый канал как коммуникационный канал, который изначально не был предназначен для передачи информации. Были предложены и другие подходы к определению скрытого канала. В отечественном стандарте[1] скрытый канал определен как не предусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности. Под политикой безопасности информации в этом случае понимают совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности. В [2] скрытый канал определен через понятие информационных потоков. Здесь все информационные потоки в системе делятся на два непересекающихся подмножества (разрешенные и неразрешенные), и в силу того, что политика безопасности также определяется через понятие информационных потоков, система защиты должна обеспечивать поддержку разрешенных потоков и препятствовать запрещенным потокам. Тогда скрытый канал – неразрешенный информационный поток, не выявляемый системой защиты.

Таким образом, скрытый канал может использоваться для несанкционированного доступа к информации ограниченного доступа, а передача информации по скрытому каналу осуществляется способом, не предполагаемым разработчиками данной автоматизированной системы как способ передачи информации. В связи с этим встает задача противодействия утечке информации по скрытым каналам. Авторы в [3] предложили методику противодействия утечке информации по скрытым каналам, включающую в себя следующие этапы: идентификация, анализ, устранение, ограничение пропускной способности, аудит и обнаружение. На этапе идентификации рассматриваются всевозможные потенциальные скрытые каналы, которые могут реализовываться в системе.

Из-за широкого распространения протокола IP в области передачи информации актуальной задачей является задача противодействия утечке информации по скрытым каналам, функционирующих в рамках IP-сетей [4–10]. Для реализации первого этапа упомянутой выше методики [3] были предложены различные методы идентификации скрытых каналов [11–13]. Стоит отметить необходимость уточнения этапов работы методов идентификации в случае сетевых скрытых каналов, так как в данном случае существует ограниченный набор возможностей как для построения системы защиты, так и для реализации скрытого канала. В связи с этим целью настоящей работы является разработка метода идентификации сетевых скрытых каналов для повышения защищенности сетей пакетной передачи данных.

1. Методы идентификации скрытых каналов

В [11] предложен метод, основанный на матрице разделяемых ресурсов, и набор условий, необходимых для существования скрытых каналов. Для существования скрытого канала по памяти должны выполняться следующие необходимые условия:

[1]ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов – Введ. 2009-10-01. М.: Стандартинформ, 2009. – 13 с.

– процессы отправки и получения информации должны иметь доступ к одному и тому же атрибуту общего ресурса;

– должны быть средства, с помощью которых процесс отправки может заставить общий атрибут измениться;

– должны быть средства, с помощью которых принимающий процесс может обнаружить изменение атрибута;

– должен существовать механизм для инициирования связи между процессами отправки и получения информации.

Необходимые условия для существования скрытого канала по времени:

– процессы отправки и получения информации должны иметь доступ к одному и тому же атрибуту общего ресурса;

– процессы отправки и получения должны иметь доступ к временной привязке, например, к часам реального времени;

– отправитель должен быть способен модулировать время отклика получателя для обнаружения изменения в общем атрибуте;

– должен существовать механизм для инициирования связи между процессами отправки и получения информации.

В [12] предложен другой метод идентификации скрытых каналов, основанный на построении дерева скрытых информационных потоков. Информация, необходимая для построения дерева скрытых информационных потоков, по существу является той же самой информацией, необходимой для построения базовой матрицы разделяемых ресурсов. Каждая операция характеризуется в терминах списка ссылок, списка изменений и списка возврата.

В [13] предложен метод идентификации скрытых каналов, основанный на построении графа скрытых информационных потоков. Граф скрытых информационных потоков – структура данных, моделирующая поток информации от одного атрибута общего ресурса к другому с целью идентификации последовательности операций, которые поддерживают потенциальные каналы связи, используемые двумя пользователями.

2. Предложенный метод идентификации скрытых каналов по памяти

Постановка задачи, которую необходимо решить в рамках исследования: дана сеть, состоящая из N узлов, и необходимо описать метод, выявляющий все возможные сетевые скрытые каналы в данной сети. В рамках исследования рассматриваются только сетевые скрытые каналы по памяти.

В рассмотренных выше методах идентификации скрытых каналов используются различные структуры данных, однако информация, необходимая для построения всех структур, по существу является одной и той же. Данная информация включает в себя все атрибуты общих ресурсов в системе, а также все операции в системе, которые определяются на первом этапе методов [11–13]. В случае двух узлов, один из которых является получателем, а другой отправителем, общим ресурсом будет являться передаваемый пакет. Так как в рамках данного исследования рассматриваются только скрытые каналы по памяти, то атрибутами общего ресурса (передаваемого пакета) будут являться поля заголовка пакета и его длина. Согласно методам идентификации [11–13], после определения атрибутов необходимо определить элементарные операции во всей системе. Для реализации скрытого сетевого канала операции должны иметь возможность модифицировать атрибуты. Пусть некоторая операция модифицирует атрибут A общего

ресурса. Для реализации скрытого канала изменения атрибута *A* недостаточно, так как после изменения пакет все еще находится у отправителя, и получатель не имеет доступ к атрибуту *A*. Таким образом, вместе с выполнением операции (или последовательности операций), в результате которого атрибут *A* будет модифицирован, должна выполняться передача атрибута *A* получателю. Если в качестве примера рассматривать операционную систему Linux [14], то для реализации сетевого скрытого канала необходимо, чтобы в системе функционировал сетевой сервис, который вызывает функции для модификации атрибутов пакета и обеспечивает отправку пакета получателю. Однако и этого может быть недостаточно. Из-за сложной структуры стека протоколов TCP/IP может случиться, что после получения пакета с модифицированным атрибутом *A* у получателя не будет доступа к атрибуту *A*. Следовательно, для реализации сетевого скрытого канала необходимо, чтобы в системе приемника функционировал сетевой сервис, который обеспечивает получение пакета и вызывает функции для распознавания значения атрибута *A*. Таким образом, для выявления скрытых каналов в сети необходимо провести анализ каждого узла на наличие сервисов, удовлетворяющих вышеперечисленным требованиям.

На основе анализа узлов сети строится граф скрытых информационных потоков в IP-сетях, вершинами которого являются узлы сети и существует дуга из вершины *i* в вершину *j*, если существует возможность построения скрытого канала, где отправителем является узел *i*, а получателем – узел *j*. При этом каждой дуге ставится в соответствие множество атрибутов, по которым возможна реализация скрытого канала.

На следующем этапе определяются скрытые информационные потоки во всей сети. После выбора атрибутов, в рамках которых будет рассматриваться наличие скрытых каналов в сети, рассматриваются множества, соответствующие дугам графа. Если во множестве нет выбранных атрибутов, в рамках которого будет проведено выявление скрытых каналов, то дуга, соответствующая данному множеству, удаляется из графа. После удаления дуг строится транзитивное замыкание графа, которое и выявляет все скрытые информационные потоки в сети, в рамках выбранных атрибутов.

Таким образом, метод идентификации скрытых каналов по памяти в IP-сетях включает следующие этапы:

– определение всех атрибутов общих ресурсов в сети, которые могут быть использованы для построения скрытых каналов по памяти;
– анализ каждого узла сети, включающий:
  - выделение портов, подлежащих анализу, и связанных с ними сокетов;
  - определение процессов, использующих данный сокет;
  - выявление сервисов, запустивших эти процессы;
  - анализ сервисов, включающий в себя выявление системных вызовов, изменяющих и считывающих определенные на первом этапе атрибуты.
– построение графа скрытых информационных потоков в IP-сетях на основе анализа узлов сети;
– выбор атрибутов, в рамках которых будет рассматриваться наличие скрытого канала в сети и выделение подграфа;
– нахождение транзитивного замыкания подграфа.

3. Реализация предложенного метода идентификации

Первым этапом метода идентификации является определение всех атрибутов общих ресурсов в сети. Как было отмечено выше, общим ресурсом в данном случае является передаваемый пакет и связанные с ним характеристики. В рамках данной работы рассматриваются только атрибуты, связанные с протоколом IPv4. На рис. 1 представлен

формат заголовка IPv4 [15]. Как правило, поля «Version», «Source IP address» и «Destination IP address», содержащие версию протокола IP, адрес отправителя и адрес получателя соответственно, не изменяемы и не могут служить атрибутом для передачи информации по скрытому каналу.

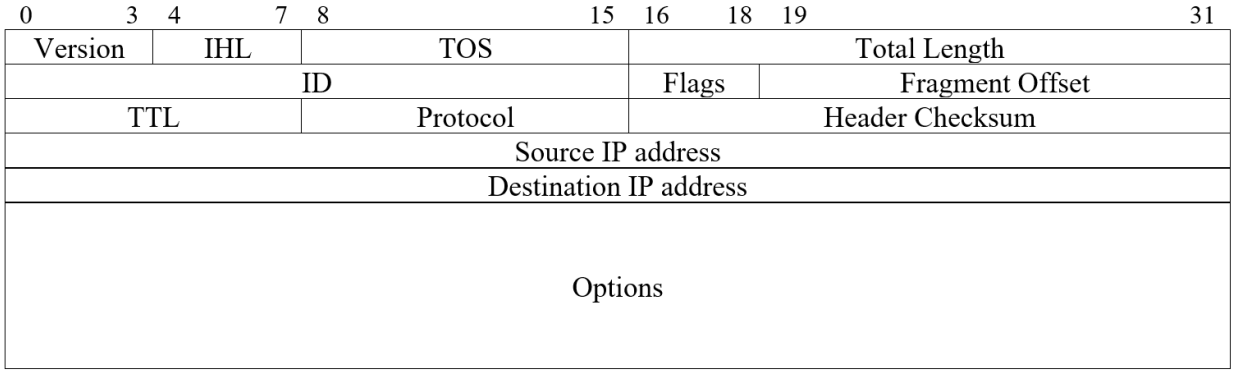

Рис. 1. Формат заголовка IPv4
Fig. 1. IPv4 header format

Поля «Total Length» и «Header Checksum», содержащие длину пакета и контрольную сумму заголовка соответственно, устанавливаются ядром операционной системы и не могут быть изменены напрямую. Однако можно использовать расширения полей заголовка (поле «Options») и заполнить их таким образом, чтобы получить требуемое значение в поля «Header Checksum» [15]. Это дает возможность рассматривать поле «Header Checksum» как атрибут при передаче информации по скрытому каналу. По такому же принципу в качестве атрибута можно рассматривать поле «IHL», в котором содержится размер заголовка IP-пакета. В случае поля «Total Length» требуемое значение поля можно получить, изменяя полезную нагрузку IP-пакета. Известны скрытые каналы, основанные на модификации поля «TTL» заголовка IP-пакета, один из которых описан в [4]. Поле «Protocol» содержит идентификатор протокола транспортного уровня в передаваемом пакете и не может изменяться при использовании в сети транспортного уровня. Согласно [5], существует возможность создания скрытого канала путем модификации поля «ID». При отсутствии фрагментации поле «Fragment offset» также может использоваться при создании скрытого канала [6]. Первый бит поля «Flags» зарезервирован и не используется при передаче пакета, что дает возможность рассматривать его в качестве атрибута. Наконец, поле «TOS», отвечающее за тип обслуживания в сети, также может рассматриваться в качестве атрибута при создании скрытого канала.

На втором этапе разработанного метода идентификации скрытых каналов проводится анализ каждого узла сети. Анализ каждого узла сети подразумевает выполнение четырех шагов. На первом шаге выделяются порты, подлежащие анализу, и связанные с ними сокеты. В зависимости от сети и узла, выбор портов для дальнейшего анализа может быть различным. Существуют различные утилиты для идентификации портов и связанных с ними сокетов в операционной системе Linux. Одним из примеров такой утилиты является *ss* [16], которая была использована при разработке программного средства идентификации сетевых скрытых каналов. Утилита *ss* предоставляет подробную информацию о сокете, в том числе информацию о процессе, который использует данный сокет, а также информацию о сервисе, запустившем этот процесс, что является вторым и третьим шагом при анализе узла. На четвертом шаге проводится анализ сервиса,

выделенного на третьем шаге, и идентифицируются все те системные вызовы, которые изменяют и считывают атрибуты, определенные на первом этапе.

В [17] представлено программное средство идентификации сетевых скрытых каналов, разработанное авторами статьи. На вход программному средству подается порт, который необходимо проанализировать. Программное средство идентифицирует процесс, связанный с данным портом, и сервис, запустивший этот процесс. После этого программное средство идентифицирует все системные вызовы, относящиеся к данному сервису, и выделяет те, которые предоставляют доступ к атрибутам. Затем проводится анализ аргументов данных системных вызовов и на основе анализа принимается решение о возможном существовании скрытого канала.

Данное программное средство идентифицирует скрытые каналы, основанные на изменении поля «TTL» заголовка IP-пакета путем сравнения значения поля «TTL», устанавливаемого ядром ОС, и значения, передаваемого системному вызову в качестве аргумента. Стоит отметить, что приведенный подход может быть применен и для идентификации других видов скрытых каналов.

Например, при отсутствии фрагментации пакетов ядро устанавливает значение поля «Fragment offset», равное нулю. Таким образом, можно идентифицировать скрытый канал, основанный на использовании атрибута «Fragment Offset», путем выявления передачи системным вызовам значения поля «Fragment offset», отличного от нуля.

Реализована одноранговая сеть со встроенными скрытыми каналами [17] для тестирования разработанного программного средства идентификации скрытых каналов. На рис. 2 представлен процесс идентификации скрытых каналов в одноранговой сети при применении разработанного метода идентификации сетевых скрытых каналов.

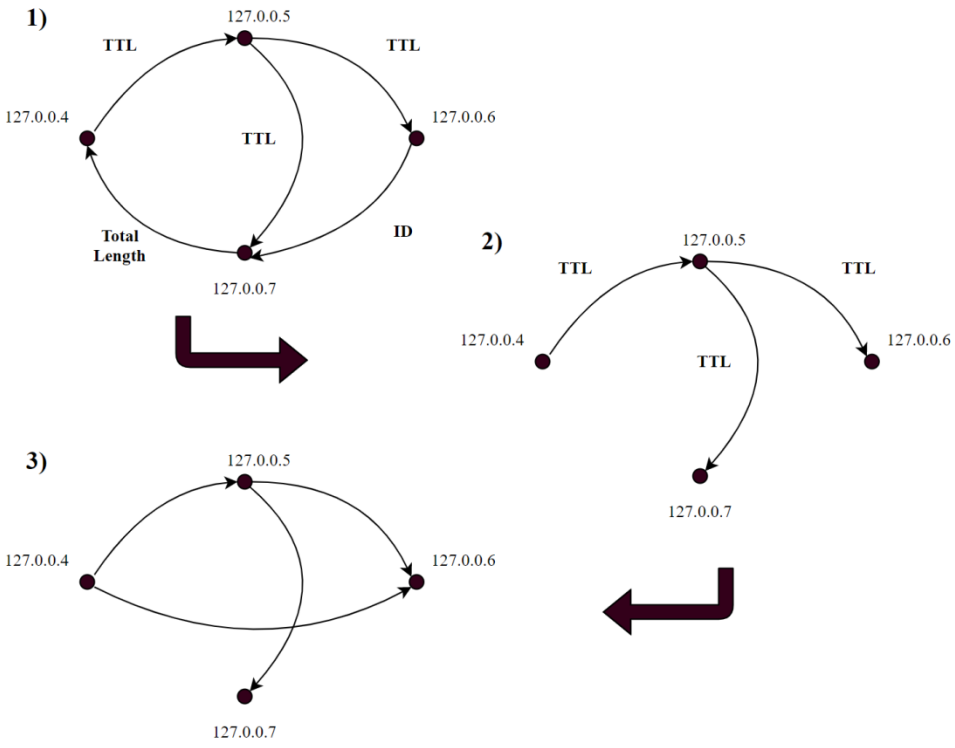

Рис. 2. Процесс идентификации скрытых каналов в одноранговой сети при использовании разработанного метода идентификации сетевых скрытых каналов

Fig. 2. The process of identifying hidden channels in a peer-to-peer network when using the developed method of identifying network hidden channels

Первый граф описывает скрытые информационные потоки построенной одноранговой сети, где метками дуг являются те атрибуты, которые используются для создания скрытого канала. Второй граф показывает скрытые информационные потоки в рамках третьего этапа метода идентификации, которые получены в результате применения разработанного программного средства. На четвертом этапе проводится выбор атрибутов, в рамках которых будет рассматриваться наличие скрытого канала в сети и выделяется подграф. В данной работе выбран атрибут «TTL», а так как программное средство идентификации разработано для скрытых каналов, основанных на изменении атрибута «TTL», то выделенный подграф совпадает с графом скрытых информационных потоков одноранговой сети, построенным при использовании разработанного программного средства (ни одна дуга не удалена).

На пятом этапе строится транзитивное замыкание подграфа, выделенного на предыдущем этапе. В данном случае транзитивным замыканием является третий граф на рис. 2, представляющий собой все скрытые информационные потоки в сети, определенные разработанным методом.

При сравнении результата применения разработанного метода идентификации (третий граф) с графом скрытых информационных потоков созданной сети (первый граф) можно убедиться, что третий граф является транзитивным замыканием первого графа в рамках атрибута «TTL». Следовательно, применение разработанного метода позволило идентифицировать все скрытые информационные потоки в рамках атрибута «TTL».

В данной работе представлено тестирование разработанного метода идентификации для скрытых каналов, основанных на изменении атрибута «TTL». Однако разработанный метод может быть применен и для идентификации других видов сетевых скрытых каналов по памяти.

Заключение

В работе приведено описание разработанного метода идентификации сетевых скрытых каналов. Преимущество данного метода перед известными в том, что он может быть легко автоматизирован для практических задач идентификации скрытых каналов в IP-сетях на основе изменения полей заголовков пакетов.

СПИСОК ЛИТЕРАТУРЫ:

1. Lampson B.W. A note on the confinement problem. Communications of the ACM. 1973. Vol. 16, no. 10. P. 613–615.
2. Тимонина Е.Е. Скрытые каналы (обзор). Jet info. 2002. Т. 14. №. 114. С. 3–11. URL: https://www.jetinfo.ru/Sites/portal/Uploads/2002_11.DF9C812FFBD9496BAE9694E27F2D9D1D.pdf (дата обращения: 20.04.21).
3. Kogos K., Sokolov A. Methods of IPD normalization to counteract IP timing covert channels. CEUR Workshop Proceedings. 2017. P. 118–126. URL: http://ceur-ws.org/Vol-1901/paper20.pdf (дата обращения: 20.04.21).
4. Zander S., Armitage G., Branch P. An empirical evaluation of IP Time To Live covert channels. 2007 15th IEEE International Conference on Networks. IEEE, 2007. P. 42–47. DOI: http://dx.doi.org/10.1109/ICON.2007.4444059.
5. Zander S., Armitage G., Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys & Tutorials. 2007. Vol. 9, no. 3. P. 44–57. DOI: http://dx.doi.org/10.1109/COMST.2007.4317620.
6. Rowland C.H. Covert channels in the TCP/IP protocol suite. 1997. URL: https://firstmonday.org/ojs/index.php/fm/article/download/528/449?inline=1 (дата обращения: 20.04.21).

7. Ahsan K., Kundur D. Practical data hiding in TCP/IP. Proc. Workshop on Multimedia Security at ACM Multimedia. 2002. Vol. 2, no. 7. P. 1–8. URL: https://www.comm.toronto.edu/~dkundur/pub_pdfs/AhsKunMMSec02.pdf (дата обращения: 20.04.21).
8. Yao Q., Zhang P. Coverting channel based on packet length. Computer engineering. 2008. Vol. 34, no. 3. P. 183–185. URL: https://en.cnki.com.cn/Article_en/CJFDTotal-JSJC200803064.htm (дата обращения: 20.04.21).
9. Ji L., Jiang W., Dai B. and Niu X. A novel covert channel based on length of messages. 2009 International Symposium on Information Engineering and Electronic Commerce. IEEE, 2009. P. 551–554. DOI: http://dx.doi.org/10.1109/IEEC.2009.122.
10. Ji L., Liang H., Song Y. and Niu X. A normal-traffic network covert channel. 2009 International Conference on Computational Intelligence and Security. IEEE, 2009. P. 499–503. DOI: http://dx.doi.org/10.1109/CIS.2009.156.
11. Kemmerer R.A. Shared resource matrix methodology: An approach to identifying storage and timing channels. ACM Transactions on Computer Systems (TOCS). 1983. Vol. 1, no. 3. P. 256–277. DOI: https://doi.org/10.1145/357369.357374.
12. Porras P.A. and Kemmerer R.A. Covert flow trees: a technique for identifying and analyzing covert storage channels, Proceedings. IEEE Computer Society Symposium on Research in Security and Privacy, 1991. P. 36–51. DOI: https://doi.org/10.1109/RISP.1991.130770.
13. Song X.M., Ju S.G. Covert Flow Graph Approach to Identifying Covert Channels. Journal of Networks. 2011. Vol. 6, no. 12. P. 1740–1746. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.658.385&rep=rep1&type=pdf#page=88 (дата обращения: 20.04.21).
14. Socket: Linux Programmer's Manual. URL: https://www.man7.org/linux/man-pages/man2/socket.2.html (дата обращения: 12.05.2020).
15. RFC 791: Internet Protocol – Data Internet Program – Protocol Specification. 1981. URL: https://datatracker.ietf.org/doc/html/rfc791 (дата обращения: 20.04.21).
16. Ss: Linux man page. URL: https://linux.die.net/man/8/ss (дата обращения: 19.03.2021).
17. Software for identifying network covert channels page. URL: https://github.com/HayrapetyanSV/network_cc_identification/blob/master/program.py (дата обращения: 20.04.21).

REFERENCES:

[1] Lampson B.W. A note on the confinement problem. Communications of the ACM. 1973. Vol. 16, no. 10. P. 613–615.
[2] Timonina E.E. Skrytye kanaly (obzor). Jet info. 2002. T. 14, no. 114. S. 3–11. URL: https://www.jetinfo.ru/Sites/portal/Uploads/2002_11.DF9C812FFBD9496BAE9694E27F2D9D1D.pdf (accessed: 20.04.21) (in Russian).
[3] Kogos K., Sokolov A. Methods of IPD normalization to counteract IP timing covert channels. CEUR Workshop Proceedings. 2017. P. 118–126. URL: http://ceur-ws.org/Vol-1901/paper20.pdf (accessed: 20.04.21).
[4] Zander S., Armitage G., Branch P. An empirical evaluation of IP Time To Live covert channels //2007 15th IEEE International Conference on Networks. IEEE, 2007. P. 42–47. DOI: http://dx.doi.org/10.1109/ICON.2007.4444059.
[5] Zander S., Armitage G., Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys & Tutorials. 2007. Vol. 9, no. 3. P. 44–57. DOI: http://dx.doi.org/10.1109/COMST.2007.4317620.
[6] Rowland C. H. Covert channels in the TCP/IP protocol suite. 1997. URL: https://firstmonday.org/ojs/index.php/fm/article/download/528/449?inline=1 (accessed: 20.04.21).
[7] Ahsan K., Kundur D. Practical data hiding in TCP/IP. Proc. Workshop on Multimedia Security at ACM Multimedia. 2002. Vol. 2, no. 7. P. 1–8. URL: https://www.comm.toronto.edu/~dkundur/pub_pdfs/AhsKunMMSec02.pdf (accessed: 20.04.21).
[8] Yao Q., Zhang P. Coverting channel based on packet length. Computer engineering. 2008. Vol. 34, no. 3. P. 183–185. URL: https://en.cnki.com.cn/Article_en/CJFDTotal-JSJC200803064.htm (accessed: 20.04.21).

[9] Ji L., Jiang W., Dai B. and Niu X. A novel covert channel based on length of messages. 2009 International Symposium on Information Engineering and Electronic Commerce. IEEE, 2009. P. 551–554. DOI: http://dx.doi.org/10.1109/IEEC.2009.122.

[10] Ji L., Liang H., Song Y. and Niu X. A normal-traffic network covert channel. 2009 International Conference on Computational Intelligence and Security. IEEE, 2009. P. 499–503. DOI: http://dx.doi.org/10.1109/CIS.2009.156.

[11] Kemmerer R.A. Shared resource matrix methodology: An approach to identifying storage and timing channels. ACM Transactions on Computer Systems (TOCS). 1983. Vol. 1, no. 3. P. 256–277. DOI: https://doi.org/10.1145/357369.357374.

[12] Porras P.A. and Kemmerer R.A. Covert flow trees: a technique for identifying and analyzing covert storage channels, Proceedings. IEEE Computer Society Symposium on Research in Security and Privacy, 1991. P. 36–51. DOI: https://doi.org/10.1109/RISP.1991.130770.

[13] Song X.M., Ju S.G. Covert Flow Graph Approach to Identifying Covert Channels. Journal of Networks. 2011. – Vol. 6, no. 12. P. 1740–1746. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.658.385&rep=rep1&type=pdf#page=88 (accessed: 20.04.21).

[14] Socket: Linux Programmer's Manual. URL: https://www.man7.org/linux/man-pages/man2/socket.2.html (accessed: 12.05.2020).

[15] RFC 791: Internet Protocol – Data Internet Program – Protocol Specification. 1981. URL: https://datatracker.ietf.org/doc/html/rfc791 (accessed: 20.04.21).

[16] Ss: Linux man page. URL: https://linux.die.net/man/8/ss (accessed: 19.03.2021).

[17] Software for identifying network covert channels page. URL: https://github.com/HayrapetyanSV/network_cc_identification/blob/master/program.py (accessed: 20.04.21).

Поступила в редакцию – 20 апреля 2021 г. Окончательный вариант – 19 августа 2021г.
Received – April 20, 2021. The final version – August 19, 2021.