Об оценке пропускной способности скрытых информационных каналов, основанных на изменении длин передаваемых пакетов

On assessing throughput capacity of covert information channels by measuring the length of packets transmitted

Епишкина / Epishkina A.
Анна Васильевна
(avepishkina@mephi.ru)
кандидат технических наук.
ФГАОУ ВПО «Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ),
доцент кафедры «Криптология и дискретная математика»
г. Москва

Когос / Kogos K.
Константин Григорьевич
(kgkogos@mephi.ru)
НИЯУ МИФИ,
аспирант кафедры «Криптология и дискретная математика»
г. Москва

Ключевые слова: информационная безопасность – information security; сетевые скрытые каналы – covert network channels; длина пакета – packet length; пропускная способность – throughput capacity; противодействие – counteraction.

Авторами исследуются скрытые информационные каналы для решения задачи предотвращения утечки информации ограниченного доступа. Скрытые каналы, основанные на изменении длин пакетов, устойчивы к шифрованию трафика и могут быть организованы в высокоскоростных сетях пакетной передачи данных, поэтому представляют серьезную угрозу безопасности. В статье получены оценки максимальной пропускной способности указанных скрытых каналов при отсутствии противодействия и при случайном увеличении длин пакетов.

The authors review covert information channels to prevent leakage of information of limited accessibility. Covert channels based on changing packet length withstand traffic encoding and may be organized in high-rate packet switching networks, therefore they are a serious security threat. The article provides assessments of the maximum throughput capacity of such covert channels in case counteraction is absent and packet length is randomly increased.

Введение

Понятие «скрытого канала» впервые введено автором [1] в 1973 году: под скрытым каналом он понимал канал связи, который не разрабатывался и не предполагался для передачи информации. В российских нормативных документах также имеется аналогичное определение: скрытый канал – непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности [2], однако на текущий момент у регуляторов в области информационной безопасности отсутствуют требования по защите от угроз, реализуемых с использованием скрытых информационных каналов.

В настоящее время широко распространены скрытые каналы в сетях пакетной передачи данных, так как возможен негласный обмен информацией с использованием особенностей стека протоколов TCP/IP [3]. С другой стороны, традиционные способы сетевой защиты, заключающиеся в туннелировании и шифровании трафика, межсетевом экранировании, оставляют возможность построения широкого класса скрытых каналов, а повсеместное распространение высокоскоростных сетей придает масштабность проблеме утечке информации по скрытым каналам.

В российском стандарте ГОСТ Р 53113.1–2008 скрытые каналы подразделяются по механизму передачи информации на каналы по памяти, каналы по времени и статистические каналы [2]. Скрытый канал по памяти использует память, в которую отправитель записывает данные, а получатель считывает их, причем сторонний наблюдатель не знает того места в памяти, куда помещена записываемая информация. Скрытый канал по времени основан на том, что отправитель модулирует с помощи передаваемых данных процесс, изменяющийся во времени, а получатель демодулирует передаваемый сигнал, наблюдая указанный процесс во времени. Скрытый статистический канал основан на том, что получатель имеет меньшую неопределенность при определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не знающий о существовании скрытого канала.

Особую актуальность рассматриваемой угрозе придают результаты исследований А. А. Грушо, доказавшего, что если противнику известна схема контроля в системе защиты, то возможно создание невидимого для контролирующего субъекта скрытого канала как для управления программно-аппаратным агентом в компьютерной среде, так и для общения программно-аппаратных агентов в открытой среде между собой [4, 5].

Одним из способов построения скрытых каналов по памяти в IP-сетях является модуляция значений полей заголовков пакетов, например, полей TTL [6], IP ID [7], ToS [8]. Другой способ заключается в изменении длин передаваемых пакетов и будет освещен более детально далее. Скрытые каналы по времени в IP-сетях могут быть построены путем изменения длин межпакетных интервалов [9, 10], в частности с использованием технологии JitterBug [11], и при помощи изменения скорости передачи пакетов [12]. Переупорядочивание пакетов также может применяться для построения скрытых каналов по времени [13]. Скрытые каналы по времени всегда являются каналами с шумом, так как время следования пакета – случайная величина, распределение которой зависит от нагрузки на сеть [14], следовательно, пропускная способность сетевых скрытых каналов по времени значительно ниже, чем пропускная способность скрытых каналов по памяти.

В настоящей статье проанализированы существующие подходы к построению скрытых каналов, основанных на изменении длин передаваемых пакетов, и противодействию утечке информации с их использованием. Авторами предложены наилучшие схемы кодирования и посчитаны максимальные пропускные способности таких скрытых каналов при отсутствии противодействия и при случайном увеличении длин пакетов, подлежащих отправке.

Развитие методов построения и противодействия скрытым информационным каналам, основанным на изменении длин пакетов

Впервые изменять длину кадров канального уровня для скрытой передачи информации предложили авторы [15] и [16]: их работы основаны на том, что отправитель и получатель знают правило, согласно которому каждому байту скрыто передаваемого сообщения соответствует определенная длина кадра.

Многие ученые исследуют проблемы, связанные с построением скрытых каналов и разработкой способов противодействия им. Так, авторы [17] построили скрытый канал, в котором отправитель и получатель разделяют периодически обновляемую матрицу, элементы которой являются уникальными неупорядоченными длинами пакетов. Были предложены различные независимые от используемого сетевого протокола модификации такого скрытого канала [18, 19].

Авторами [20] предложен скрытый канал с высокой пропускной способностью, основанный на изменении длин и информационного наполнения пакетов. Исследование в данном направлении продолжили авторы [21], реализовав указанный скрытый канал с использованием протокола TCP. Такие скрытые каналы являются сложно обнаруживаемыми, так как распределение длин пакетов при наличии скрытого канала близко к распределению длин пакетов «нормального» трафика, то есть при отсутствии скрытого канала.

Известны и подходы к оценке пропускной способности скрытых каналов с шумом методами теории информации [22, 23].

Таким образом, важная задача заключается в превентивном ограничении пропускной способности потенциальных скрытых каналов, так как известны сложно обнаруживаемые скрытые каналы, имеющие высокую пропускную способность. Более того, существующие способы противодействия таким скрытым информационным каналам, основанные, как правило, на нормализации трафика, а именно на выравнивании длин передаваемых пакетов, зачастую бывают неэффективны, так как существенно понижают пропускную способность канала связи. При разработке методов ограничения скрытых информационных каналов необходима оценка максимальной остаточной пропускной способности скрытого канала, которая должна быть понижена до некоторого критического значения, такого что функционирование скрытых каналов с меньшей пропускной способностью считается неопасным. Например, существуют оценки данной величины, при различных условиях равные 1 бит/с и 100 бит/с [24].

В данной работе предложена оценка максимальной пропускной способности скрытого канала при отсутствии противодействия. Также разработан способ ограничения пропускной способности путем случайного увеличения длин пакетов, подлежащих отправке, оценена остаточная пропускная способность скрытого канала при введении противодействия. Отметим, что получение количественных характеристик метода крайне важно, так как он реализован авторами [25] для протокола IPSec и может быть применен на практике.

Пропускная способность скрытого канала, основанного на изменении длин пакетов

При отсутствии противодействия максимальную пропускную способность имеет скрытый канал, построенный следующим образом.

Пусть длины пакетов принимают значения на множестве $N_{l_{\text{фикс}}+L-1} \setminus N_{l_{\text{фикс}}-1}$, где N_x — множество натуральных чисел от 1 до x, $l_{\text{фикс}}$, $L \in N$, где $L-1$ – максимальный размер информационного наполнения пакета. Пропускная способность скрытого канала максимальна при следующей схеме передачи данных: для отправки символа «i» посылается пакет длины $l_{\text{фикс}} + i$, $i \in N_{n-1} \bigcup \{0\}$, где n – параметр скрытого канала. Пропускную способность скрытого канала C предлагается оценить методами теории информации, как

$$C = \max_{n}\left\{\frac{I(X,Y)}{\tau}\right\},$$

где $I(X,Y) = H(Y) - H(Y|X)$ – взаимная информация случайных величин X, Y, описывающих входные и выходные характеристики скрытого канала соответственно; энтропия случайной величины Y равна

$$H(Y) = -\sum_{i \in N_{n-1} \cup \{0\}} p_{\text{вых}}(i) \log_2 p_{\text{вых}}(i),$$

условная энтропия случайной величины Y относительно случайной величины X равна

$$H(Y|X) = -\sum_{j \in N_{n-1} \cup \{0\}} p_{\text{вх}}(j) \left(\sum_{i \in N_{n-1} \cup \{0\}} p_{\text{вых}}(i|j) \log_2 p_{\text{вых}}(i|j) \right),$$

τ – среднее время передачи пакета.

При таком способе построения скрытого канала взаимная информация случайных величин X, Y равна:

$$I(X,Y) = \log_2 n,$$

так как из-за отсутствия ошибок $H(Y|X) = 0$.

При предложенной схеме кодирования среднее время передачи пакета равно

$$\tau = \frac{2l_{\text{фикс}} + n - 1}{2\beta},$$

где β – пропускная способность канала связи.

Очевидно, что при увеличении значения n увеличиваются как средняя длина передаваемых пакетов, так и количество бит, которое несет передача одного пакета по скрытому каналу. Тогда пропускная способность скрытого канала принимает значение, равное:

$$C \approx \frac{2\left(\log_2(2l_{\text{фикс}} - 1) - \log_2\left(W\left(\frac{2l_{\text{фикс}} - 1}{e}\right)\right)\right)}{2l_{\text{фикс}} + \frac{2l_{\text{фикс}} - 1}{W\left(\frac{2l_{\text{фикс}} - 1}{e}\right)} - 1}\beta,$$

что достигается при следующем значении параметра скрытого канала:

$$n \approx \frac{2l_{\text{фикс}} - 1}{W\left(\frac{2l_{\text{фикс}} - 1}{e}\right)},$$

где $W(y)$ – функция Ламберта, определяемая как корень уравнения $xe^x = y$.

Как правило, $l_{\text{фикс}}$ определяет сумму длин заголовков сетевого и канального уровней модели взаимодействия открытых систем. Так, например, при использовании IPv4 в качестве протокола сетевого уровня сумма длин заголовков сетевого и канального уровней принимает значение не менее 34 байт, если технология канального уровня – Ethernet. Аналогичная величина при использовании протокола IPv6 равна 54 байтам. Таким образом, при использовании протокола IPv4 пропускная способность скрытого канала максимальна при $n = 138$ и достигает примерно $0{,}021\beta$, для протокола IPv6 $n = 201$, а приближенное значение максимальной пропускной способности скрытого канала равно $0{,}018\beta$.

Данные результаты подтверждают актуальность исследования методов ограничения пропускной способности скрытых каналов, так как показывают, что при пропускной способности канала связи 1 Гбит/с может быть построен скрытый канал с пропускной способностью более 10 Мбит/с.

Случайное увеличение длин пакетов как метод противодействия скрытым каналам

Авторами предложен следующий способ противодействия утечке информации по скрытым каналам: длина каждого пакета, подлежащего отправке, увеличивается на количество бит, определяемое значениями случайной величины, имеющей равномерное распределение на множестве $N_\alpha \cup \{0\}$, где α – параметр способа противодействия. Равномерное распределение представляет наибольшую неопределенность в распознавании переданного по скрытому каналу символа получателем.

Дополнительная нагрузка на канал связи заключается в отправке, в среднем, $\frac{\alpha}{2}$ фиктивных бит на пакет. С другой стороны, остаточная пропускная способность при введении данного способа противодействия равна:

$$\frac{\beta\tilde{l}}{\tilde{l} + \alpha/2},$$

где $\tilde{l}$ — средняя длина передаваемых пакетов.

Из-за случайного изменения длин пакетов применение данного способа противодействия не приводит к рассинхронизации отправителя и получателя скрытого канала, однако позволяет передавать данные лишь по таким скрытым каналам, где символам скрыто передаваемого сообщения соответствуют построенные по определенным правилам множества длин пакетов. Далее исследован скрытый канал, имеющий наибольшую пропускную способность при рассмотренном способе противодействия.

Для передачи символа «i» отправитель посылает пакет длины $l_{\text{фикс}} + i(\alpha + 1)$, $N_{n-1} \cup \{0\}$, n – параметр скрытого канала. При таком способе построения скрытого канала введение противодействия не приводит к возникновению ошибок, поэтому взаимная информация случайных величин X, Y равна:

$$I(X,Y) = \log_2 n.$$

Среднее время τ передачи пакета определяется выражением:

$$\tau = \frac{2l_{\text{фикс}} + n(\alpha + 1) - 1}{2\beta}.$$

Таблица 1

Зависимость между параметрами скрытого канали и способа противодействия

α			10	20	50	100	200	500	1000
Протокол сетевого уровня	**IPv4**	***n***	23	15	9	6	5	4	3
		$\frac{C}{\beta}\times 10^3$	11,40	9,11	6,33	4,50	3,00	1,57	0,89
	IPv6	***n***	32	20	12	8	6	4	4
		$\frac{C}{\beta}\times 10^3$	8,23	6,74	4,86	3,60	2,50	1,40	0,82

Как и ранее, при увеличении значения n увеличивается как средняя длина передаваемых пакетов, так и количество бит, которое несет передача одного пакета по скрытому каналу. Тогда пропускная способность C скрытого канала определяется следующим образом:

$$C = \frac{2\beta\left(\log_2\left(\frac{2l_{\text{фикс}}-1}{\alpha+1}\right)-\log_2 W\left(\frac{2l_{\text{фикс}}-1}{e(\alpha+1)}\right)\right)}{2l_{\text{фикс}}+\frac{2l_{\text{фикс}}-1}{W\left(\frac{2l_{\text{фикс}}-1}{e(\alpha+1)}\right)}-1},$$

что достигается при следующем значении параметра скрытого канала:

$$n = \frac{2l_{\text{фикс}}-1}{(\alpha+1)W\left(\frac{2l_{\text{фикс}}-1}{e(\alpha+1)}\right)}.$$

В таблице 1 приведены значения параметра скрытого канала n и пропускной способности скрытого канала C, а именно, $\frac{C}{\beta}\times 10^3$, при некоторых значениях параметра способа противодействия α. Указанные оценки получены для протоколов IPv4 и IPv6.

Как видно из результатов, даже небольшое увеличение длин пакетов существенно понижает пропускную способность скрытого канала по сравнению с максимальной пропускной способностью, определенной ранее.

Заключение

В работе исследована максимальная пропускная способность многосимвольных скрытых каналов, основанных на изменении длин пакетов. Показано, что для протоколов IPv4 и IPv6 пропускная способность таких скрытых каналов может достигать примерно 2% пропускной способности канала связи. Предложен способ противодействия указанному типу скрытых каналов путем случайного увеличения длин пакетов, позволяющий существенно понизить пропускную способность потенциального скрытого канала.

Перспективным направлением дальнейшей работы по данному направлению является исследование возможности совместного применения метода противодействия, основанного на увеличении длин пакетов, с иными подходами, заключающимися, например, в генерации фиктивного трафика.

Литература

1. Lampson, B. W. A Note on the Confinement Problem / B.W. Lampson // Communications of the ACM. – 1973. – P. 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. – 13 с.

3. Zander, S. A survey of covert channels and countermeasures in computer network protocols / S. Zander, G. Armitage, P. Branch // IEEE Communications surveys and tutorials. – 2007. – Vol. 9. – No. 3. – P. 44–57.

4. Грушо, А. А. Скрытые каналы и безопасность информации в компьютерных системах / А.А. Грушо // Дискретная математика. – 1998. – Т. 10. – № 1. – С. 3–9.

5. Грушо, А. А. О существовании скрытых каналов / А.А. Грушо // Дискретная математика. – 1999. – Т. 11. – № 1. – С. 24–28.

6. Zander, S. Covert channels in the IP time to live field / S. Zander, G. Armitage, P. Branch // Proc. of the 2006 Australian telecommunication networks and applications conference. – 2006. – P. 298–302.

7. Ahsan, K. Practical data hiding in TCP/IP / K. Ahsan, Kundur // Proc. of the 2002 ACM Multimedia and security workshop. – 2002.

8. Handel, T. Hiding data in the OSI network model / T. Handel, M. Sandford // Proc. of the first International workshop on information hiding. – 1996. – P. 23–38.

9. Berk, V. Detection of covert channel encoding in network packet delays / V. Berk, A. Giani, G. Cybenko. – Technical report TR2005-536. – New Hampshire: Thayer school of engineering of Dartmouth College. – 2005.

10. Sellke, S. H. Covert TCP/IP timing channels: theory to implementation / S.H. Sellke, C.-C. Wang, S. Bagchi, N. B. Shroff // Proc. of the twenty-eighth Conference on computer communications. – 2009. – P. 2204–2212.

11. Shah, G. Keyboards and covert channels / G. Shah, A. Molina, M. Blaze // Proc. of the 15th USENIX Security symposium. – 2009. – P. 59–75.

12. A study of on/off timing channel based on packet delay distribution / L. Yao [et al.] // Computers and security. – 2009. – Vol. 28. – No. 8. – P. 785–794.

13. Kundur, D. Practical Internet steganography: data hiding in IP D. Kundur, K. Ahsan // Proc. of the 2003 Texas workshop on security of information systems. – 2003.

14. Analysis of end-to-end delay measurements in Internet / C.J. Bovy [et al.] // Proc. of the 2002 ACM Conference Passive and Active Measurements. – 2002.

15. Padlipsky, M. A. Limitations of end-to-end encryption in secure computer networks / M.A. Padlipsky, D.W. Snow, P.A. Karger. – Technical report ESD-TR-78-158. – Massachusetts: The MITRE Corporation. – 1978.

16. Girling, C. G. Covert channels in LAN's / C.G. Girling // IEEE Transactions on software engineering. – 1987. – Vol. 13. – No. 2. – P. 292–296.

17. Yao, Q. Coverting channel based on packet length / Q. Yao, P. Zhang // Computer engineering. – 2008. – Vol. 34. – No. 3. – P. 183–185.

18. A novel covert channel based on length of messages / L. Ji [et al.] // Proc. of the 2009 Symposium on information engineering and electronic commerce. – 2009. – P. 551–554.

19. A normal-traffic network covert channel / L. Ji [et al.] // Proc. of the 2009 International conference on computational intelligence and security. – 2009. – P. 499–503.

20. Hussain, M. A high bandwidth covert channel in network protocol / M. Hussain // Proc. of the 2011 International conference on information and communication technologies. – 2011. – P. 1–6.

21. Edekar, S. Capacity boost with data security in network protocol covert channel / S. Edekar, R. Goudar // Computer engineering and intelligent systems. – 2013. – Vol. 4. – No. 5. – P. 55–59.

22. Millen, J. K. Covert channel capacity / J.K. Millen // Proc. of the IEEE Symposium on Security and Privacy. – 1987. – P. 60–66.

23. Venkatraman, B. R. Capacity estimation and auditability of network covert channels / B.R. Venkatraman, R.E. Newman-Wolfe// Proc. of the IEEE Symposium on Security and Privacy. – 1995. – P. 186–198.

24. Department of defense trusted computer system evaluation criteria. – Department of defense standard. – 1985.

25. Traffic flow confidentiality in IPsec: protocol and implementation / C. Kiraly [et al.] // The International federation for information processing. – 2008. – Vol. 262. – P. 311–324.