K.G. Kogos, M. A. Finoshin

Detection of IP Covert Timing Channels

Key words: covert channels, timing channels, detection

Covert timing channels became widespread with the increasing popularity of packet switching networks. Detection of these channels is the only approach to counter that does not lead to a decrease of channel's capacity. Known methods of the IP covert timing channels detection were systematized. Detection methods based on the analysis of patterns in the distribution of inter-packet delays according to criteria such as alpha and beta errors, an ability of implementation were compared.

К. Г. Когос, М. А. Финошин

ОБНАРУЖЕНИЕ СКРЫТЫХ КАНАЛОВ ПО ВРЕМЕНИ В IP-СЕТЯХ

Сети пакетной передачи информации представляют возможности для реализации угроз, связанных с построением широкого класса скрытых каналов, даже в условиях шифрования трафика. Функционирование скрытых каналов по времени в IP -сетях представляет особую угрозу, так как превентивные способы противодействия, заключающиеся в ограничении пропускной способности потенциальных каналов, приводят к существенному понижению пропускной способности самого канала связи.

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

- обнаружение частного класса скрытых каналов, основанных на изменении длин межпакетных интервалов [1];
- обнаружение путем анализа закономерностей в трафике;
- обнаружение путем сравнения с «эталонной» моделью трафика (использование методов математической статистики: критерия согласия Пирсона [2] и теста Колмогорова — Смирнова [3]).

Работа методов второй группы основана на предположении, что при наличии скрытого канала трафик становится более предсказуемым. Особый интерес представляет исследование методов первой и второй групп, так как данные методы специальным образом спроектированы для обнаружения скрытых каналов по времени в сетях пакетной передачи информации. Сравнительный анализ методов обнаружения первой и второй групп представлен в таблице 1.

В таблице 1 символы имеют следующие обозначения:

- «-» — невозможность реализации метода ввиду отсутствия полиномиального алгоритма подсчета колмогоровской сложности;
- «-*» — реализация метода возможна только в случае известной и постоянной схемы кодирования;
- «-**» — реализация метода возможна при наличии «эталонной» модели трафика;
- «-***» — метод дает преимущество по сравнению с методом, основанным на анализе энтропии, только если имеются закономерности в распределении бит в передаваемом сообщении, что маловероятно, так как по скрытым каналам по времени зачастую передаются криптографические ключи, распределение бит в которых имитирует РРСП (равномерно распределенную случайную последовательность).

Таблица 1. Сравнительный анализ методов обнаружения

Метод обнаружения		Критерий сравнения		
		Ошибки 1-го рода	Ошибки 2-го рода	Возможность реализации
Первая группа методов		При построении скрытого канала с высоким уровнем шума	Отсутствуют	- *
Вторая группа методов	Анализ дисперсии [4]	При введении шума, изменении схемы кодирования	При передаче пакетов с максимальной скоростью	+
	Метод «8-близости» [4]	При введении шума		+
	Анализ колмогоровской сложности [5]	Зависят от выбора схемы подсчета колмогоровской сложности		-
	Анализ энтропии [3]	Зависят от параметров метода		**
	Анализ условной и скорректированной энтропии [3]			

В результате проведенного исследования методов обнаружения скрытых каналов по времени в IP-сетях актуальным направлением дальнейшей работы является анализ возможности построения скрытых каналов, не выявляемых при помощи существующих методов обнаружения, и получение количественных характеристик таких каналов.

СПИСОК ЛИТЕРАТУРЫ:

1.Berk V., Giani A., Cybenko G. Detection of covert channel encoding in network packet delays. Technical report TR2005-536. 2005. - 11 p.

2.Никулин М. С. О критерии хи-квадрат для непрерывных распределений // Теория вероятностей и ее применения. М., 1973. С. 675-676.

3.Walls *R. J., Kothari K., Wright M.* Liquid: A detection-resistant covert timing channel based on IPD shaping // Computer networks. 2011. Vol. 55. Issue 6. P. 1217-1228.

4.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. 2009. P. 22-59.

5.Cabuk S., Brodley C. *E., Shields* C. IP covert channel detection // ACM Transactions on Information and Systems Security. 2009. Vol. 12. № 4. P. 1-28.

REFERENCES:

1.Berk V., Giani A., Cybenko G. Detection of covert channel encoding in network packet delays. Technical report TR2005-536. 2005. - 11 p.

2.Nikulin M. S. About chi-square criterion for continuous distributions // Theory of probability and its applications. M., 1973. P. 675 -676.

3.Walls R. J., Kothari K., Wright M. Liquid: A detection-resistant covert timing channel based on IPD shaping // Computer networks. 2011. Vol. 55. Issue 6. P. 1217-1228.

4.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. 2009. P. 22-59.

5.Cabuk S., Brodley C. *E., Shields* C. IP covert channel detection // ACM Transactions on Information and Systems Security. 2009. Vol. 12. № 4. P. 1-28.