Правило 1. Инициатору запроса разрешено произвести операцию $op \in O$, если существует префикс pk слова key, такой, что $C(pk, op, pas) = Allow$, и при этом выполняется условие: если функция C определена для некоторого префикса $prefix$ слова pk, то $C(prefix, op, pas) = Pass$.

Правило 2. Инициатору запроса запрещено произвести операцию $op \in O$, если существует префикс pk слова k, такой, что $C(pk, op, pas) = Deny$, и при этом выполняется условие: если функция C определена для некоторого префикса $prefix$ слова pk, то $C(prefix, op, pas) = Pass$.

Считается, что префикс слова может совпадать с самим словом. Если условия правила 1 или правила 2 не выполняются, например, из-за того, что функция управления доступом не определена на параметрах запроса, то запрос не выполняется.

В таблице приведён простой пример задания функции управления доступом с использованием псевдокода. Для запросов с паролем «p1» разрешается выполнять любые операции над данными с ключами, которые начинаются с «a». Для запросов с ключом «ab» разрешается чтение данных всем, а запись только тем, кто знает пароль «p2».

Префиксы ключей	Псевдокод вычисления значения функции управления доступом
a	IF password = p1 return ALLOW; ELSE return PASS;

ab	IF operation = get return ALLOW;
	IF operation = set IF password = p2 return ALLOW; ELSE return DENY;

ЛИТЕРАТУРА

1. *Чернов Д. В.* О моделях логического управления доступом на основе атрибутов // Прикладная дискретная математика. Приложение. 2012. №. 5. С. 79–82.

УДК 004.62 DOI 10.17223/2226308X/8/36

THE CAPACITY OF A PACKET LENGTH COVERT CHANNEL

A. V. Epishkina, K. G. Kogos

Covert channels are used for information hiding and realize one of the most serious security threat. Widespread IP networks allow for designing such channels on the basis of special properties of packet data transfer. Packet length covert channels are resistant to traffic encryption, but some difficulties to detect them are known. It makes significant an investigation of capacity limitation methods. This work presents a technique to estimate and limit the capacity of the covert channels based on the packet length modulation by traffic padding.

Keywords: *covert channel, packet length, dummy packet, capacity limitation.*

A covert channel is a communication channel which is not intended for information transfer at all, such as the service program's effect on the system load [1]. At present the most popular covert channels are in packet networks because of some features available in the TCP/IP protocol suite. There is a number of undetectable packet length covert channels in IP networks that may be constructed even if an encryption is used at any OSI model level. This paper describes a technique to estimate and limit the capacity of such covert channels using dummy packets generation.

The design of the considered network covert channel and of a counteraction technique is as follows. Let the lengths of transferred packets have the natural values from l_{fix} to $l_{\text{fix}} + L$; $\{L_0, L_1\}$ is a partition of the set $N_{l_{\text{fix}}+L} \setminus N_L$ where $|L_0| = |L_1|$, N_a stands for the set of positive integers from 1 to a. Further, we consider a method to build a binary covert channel. In order to transfer «0» the sender communicates a packet of a length of $l \in L_0$, to transfer «1» the sender communicates a packet of the length $l \in L_1$. It is obvious that the capacity of such channel without counteraction is equal to 1 bit per packet. To build such a covert channel the sender must have the following possibilities: to modify lengths of transmitted packets, to form packets of an undefined length, to buffer packets to be sent and to transfer them at a specified moment.

The authors propose a technique to limit the capacity of covert channel based on traffic padding. After k data packets have been sent, a random length dummy packet is created where k is the parameter of a counteraction tool. Let μ be the capacity of a communication channel, then a counteraction tool decreases the capacity of a communication channel to $k\mu/(k+1)$.

After dummy packet receiving, the mismatch between the hidden sender and the hidden receiver takes place. To negotiate this fact SOF packets [2] are utilized after $T-1$ packets transferring within the covert channel. The receiver fixes $T-1$ packets gained after SOF packet and waits for the next SOF packet. Thus T is the covert channel parameter which estimates the synchronization frequency. As the identification of bits received after the mismatch happened is wrong, in order to build the covert channel the inequality $T < k+1$ is required. The corresponding choice of parameters is explained in Fig. 1.

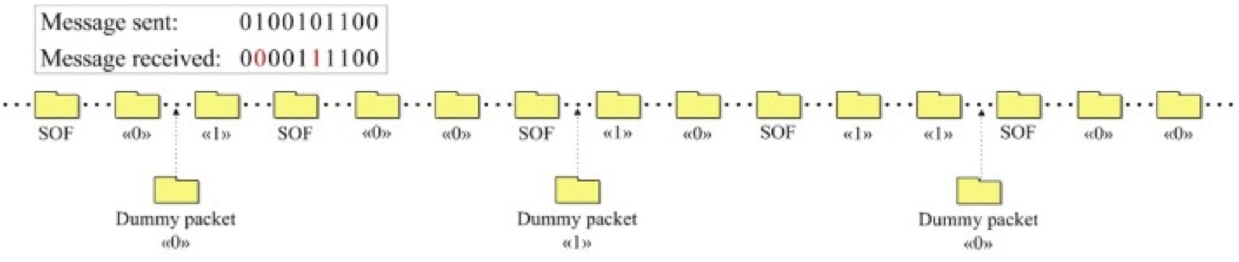

Fig. 1. The scheme of data transfer in the covert channel ($T = 3$, $k = 5$).

The capacity C of the investigated covert channel is $C = \max\limits_X I(X,Y)$ where $I(X,Y)$ is the mutual information of random variables X and Y describing respectively the input and output data of the channel properly. Since each T-th packet sent via the covert channel is not a data packet but is a synchronization one, the mutual information can be calculated using the following formula:

$$I(X,Y) = \frac{T-1}{T} I^*(X,Y),$$

where $I^*(X,Y) = H(Y) - H(Y|X)$ is a mutual information of random variables describing the input and output data of the covert channel without synchronization.

The sizes of sets L_0 and L_1 are equal and lengths of dummy packets passing through the covert channel are chosen randomly and equiprobable. Therefore, $H(Y) = 1$. Since the values of conditional probabilities $p(y|x)$ for $x, y \in \{0,1\}$ depend on the number of packets sent via a covert channel from the moment of synchronization to the moment of a dummy packet receiving, the mutual information $I^*(X,Y)$ can be found using the following formula:

$$I^*(X,Y) = \frac{k-(T-1)+\sum\limits_{i=0}^{T-2}\Big(1-H_i(Y|X)\Big)}{k},$$

where $H_i(Y|X)$ is the conditional entropy of Y compared to X evaluated when i packets are received between the synchronization and dummy packet arrival moments.

Then the approximate value of the mutual information for X and Y is

$$I(X,Y) \approx \frac{T-1}{T} - \frac{(T-1)^2}{kT} + \frac{(2T-3)(T-1)}{2kT}\log_2\frac{2T-3}{T-1} - \frac{(T-2)(T-1)}{2kT\ln 2}.$$

Note, that if k is a continuous variable, $k \in [T;+\infty)$, then $I(X,Y) \approx A(T)/k + B(T)$ is a hyperbola as a function of k where

$$A(T) = \frac{(T-1)^2}{T} + \frac{(2T-3)(T-1)}{2T}\log_2\frac{2T-3}{T-1} - \frac{(T-2)(T-1)}{2T\ln 2}$$

is negative strictly decreasing, $B(T) = (T-1)/T$ is positive strictly increasing, and they are functions of T. To build a covert channel the parameter T is chosen to maximize $I(X,Y)$. For example when $k \in \{2,3,4\}$ the parameter T should be equal to 2, when $k \in \{5,6,7,8\}$ the parameter T should be equal to 3 and when $k \in \{9,10,11,12,13,14\}$ the parameter T should be equal to 4. Graphs for function $I(X,Y)$ of k and $T = 2,3,4,5$ are illustrated in Fig. 2.

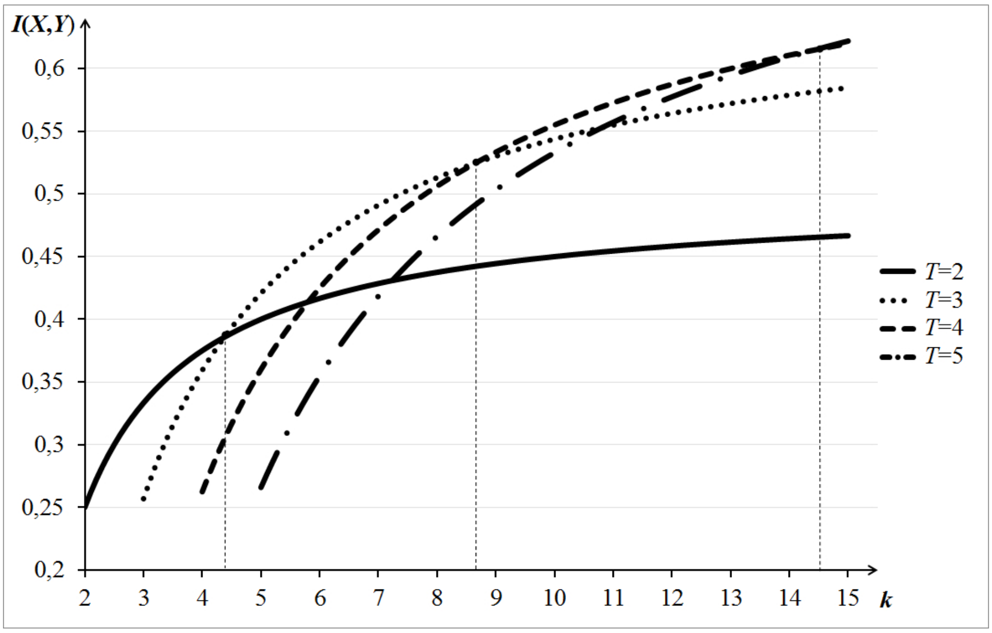

Fig. 2. Graphs for $I(X,Y)$ as the function of k and $T = 2,3,4,5$.

Let $v_{\max}$ be the value of the covert channel capacity such that the functioning of the covert channel with a capacity less than $v_{\max}$ has no influence upon security. Then a value T_0 can be defined satisfying the following inequalities:

$$\begin{cases} v_{\max} - C_{\min}(T_0) > 0, \\ C_{\min}(T_0) > C_{\min}(T), \end{cases}$$

for every $T \geqslant 2$, $T \neq T_0$ where $C_{\min}(T)$ is the capacity of the covert channel when the value k is taken the smallest for each fixed value T.

In fact, the parameter of counteraction tool k can be computed as $k = \left\lfloor \dfrac{B(T_0)}{v_{\max} - A(T_0)} \right\rfloor$.

The results of the work are useful for constructing secure IP networks. The authors have suggested a technique to select the parameter of the counteraction tool when an allowable covert channel capacity is given. The novelty of the method is that the capacity of the covert channel is limited in contrast to the other approaches which detect and destroy the active covert channels. The topic of the further work is to research the techniques to limit the packet length covert channel capacity by random increasing the lengths of packets before sending them.

BIBLIOGRAPHY

1. *Lampson B. W.* A note on the confinement problem // Comm. ACM. 1973. No. 16. P. 613–615.
2. *Cabuk S., Brodley C. E., and Shields C.* IP covert timing channels: design and detection // Proc. CCS'04, October 25–29, 2004, Washington, DC, USA. P. 178–187.