COVERT CHANNELS OF INFORMATION TRANSFER

Alekseev, Viktor M., *Russian University of Transport (MIIT), Moscow, Russia.*

ABSTRACT

The article deals with the organization of hidden channels of information transfer with the help of embedded agents in operating systems. The current state of research in this field of science, comparison with the world level, shows that there are no theoretical developments of hidden channel analyzers, as well as software and hardware implementation of their models. The author offers his approach to creating covert channel analyzers based on methods of self-organization, as well as an algorithm for network operations that allows to perform the functions of entanglement of packets in order to destroy the process of transmitting information over hidden channels.

Keywords: information channels, corporate network, hidden channel, analyzer, secret agent, packet, perceptron.

Background. *The review of publications on the hidden transfer of information showed that the problem of research in this field is relevant. Hidden agents, supplied in modern operating systems (OS), perform various tasks to collect data from computers through seemingly innocuous applications. The amount of memory occupied by operating systems is growing significantly, and the functions practically remain the same. This proves indirectly that within the operating systems on the basis of applications there are secret agents-organizers, hidden agents for the transfer of information. Applications are a necessary tool for gathering information legally installed on personal computers, communicators, servers and other computing facilities [1–3, 6, 7]. And with the update of the operating system at the same time, secret agents are updated.*

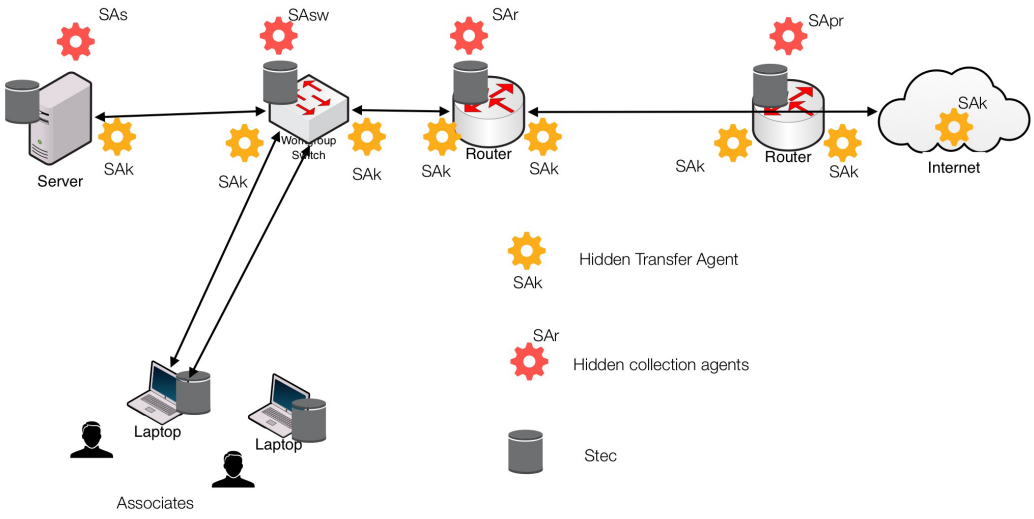
Objective. *The objective of the author is to consider hidden channels of information transfer.*

Methods. *The author uses general scientific methods, comparative analysis, evaluation approach, scientific description.*

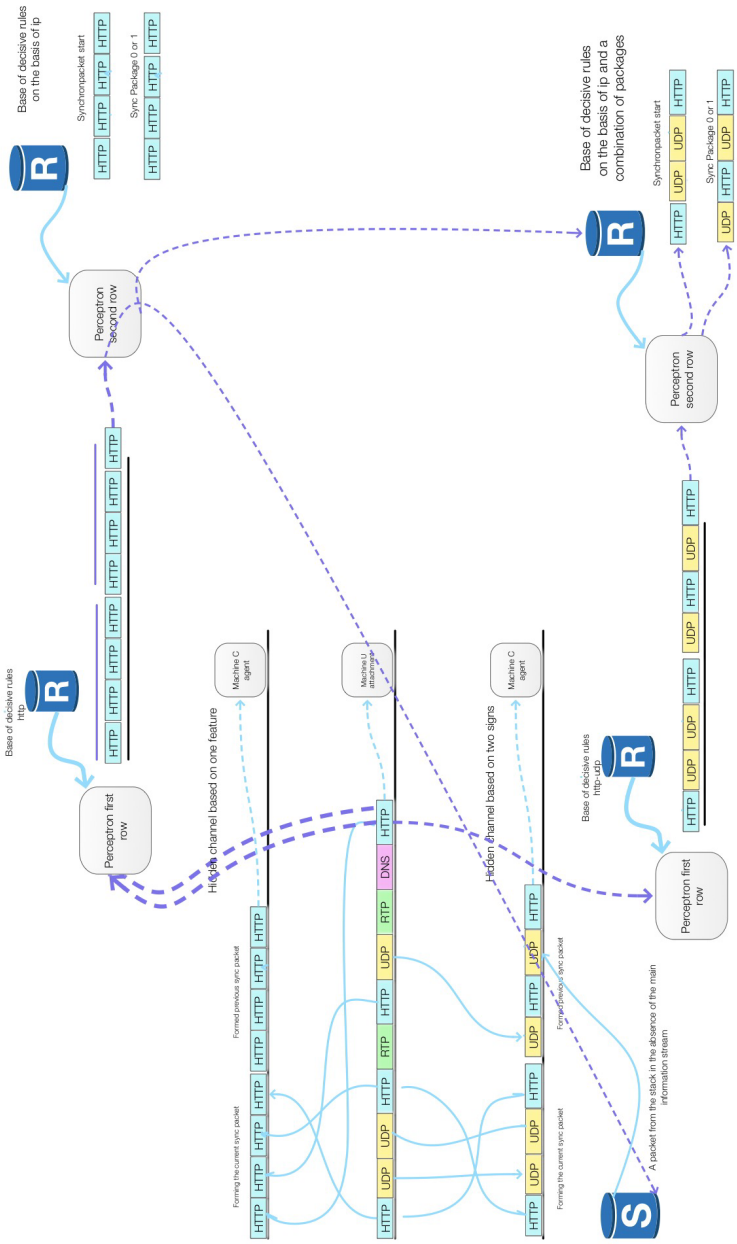
Results. *The technology of hidden channels is based on the following principle. The hidden software (agents) does not allow itself to be controlled, since it is directly located in the kernel of the operating system. The secret agent starts to act from the command from the outside, and therefore, the hidden delivery channels of the management command must be organized in the system. The agent-organizers are engaged in this. The transfer and reception of their information is carried out through the same channels that the corporate network also uses. The process first goes through the equipment of the local network: access points, switches, protective screens, routers. The transfer of information over the hidden channels occurs further through the equipment of the communication operator, where the main links are the servers and routers.*

In other words, through the communication channel from an external source to an illegal agent information must be transferred, the volume of which depends on the type of tasks being solved. But if such an operation is noticed, then the «bookmark» can be immediately destroyed. It is clear that the transfer of information to the automated device of such an agent is carried out through the same input sequence as information to the computer system (CS). The CS is monitored by a U subject which does not see the hidden management of the agent and has some information about the current state of the CS and the task submitted to the input.

The subject U does not see in the state s the hidden channel $X \to Y$ then and only then $I_s(X, Y) \to Is(X, Y|Z)$ [3, 5, 8]. This conclusion is interpreted as



Pic. 1. Structured scheme of the formation of hidden channels: SAs, sw, r, pr – hidden agents responsible for data collection from network devices and formation of the volume of transmitted information; SA_k –hidden information transfer agent for one of the features or a combination thereof.



Pic. 2. Formation of the information flow according to the features.

follows. If C receives a message $z \in Z$ and does not want this fact to be seen by the subject U, then the information stream from X to Y should remain the same as in the case when there is simply no hidden transfer through the channel $X \to Z$.

In the formation of a hidden channel illegal agents of servers, switches, routers are involved. The most rational way to control the appearance of hidden channels of information transfer can be applied for equipment with large queues: switches and routers, the mandatory attribute of which is the presence of a stec of packets, where they are sent and where the missing packets can be extracted in the absence of them in the information flow. This is how the sequence of the hidden channel is formed from the current information flow and the stec of packets (Pic. 1).

The work of the information-flow analyzer based on perceptron [4] is based on the analysis of the situation according to the formed decision rules in the space of given characteristics. The peculiarity of the analyzer is that it is required to recognize a combination of existing parameters. To implement a hidden channel, it is possible to use synchronization sequences that denote the beginning and the end of the transfer of the information flow (respectively, the sync packets of the beginning and the end are used). The organizer of any transfer is a secret agent-intermediary. The repeatability of some combinations is a sign that there is a hidden transfer.

A single-row perceptron, in the case of applying one feature to transfer information over a hidden channel, contains possible combinations of packets

arranged in accordance with a certain feature, for example, via a protocol. In the variant of applying two characteristics, the decision functions will contain two characteristics, etc. (Pic. 2).

The formation of a hidden channel using two signs occurs as follows. A predefined sequence of i_p-addresses for certain protocols (HTTP-UDP or any other pair, for example, HTTP-RTCP) can be used as a sign. It should be noted that the creation of a hidden sequence can be based on the order of the packets. Therefore, the perceptron must contain a combination of the location of the packets in the base of the decision rules, as in the following example: UDP and HTTP.

The sequence of packets is divided into flows by protocols, and a hidden channel can be formed in each flow. In the case of a sequence of two, the sync flow is generated from the packet sequences of two protocols.

Pic. 2 shows two cases of forming hidden channels on packets of one protocol and packets on two protocols. In the second case, the decision rules should take into account the fact that the combination of packet allocation can also be used for the formation of synchronous packets of hidden channels.

If you try to generate a sequence from a common flow on attribute X_1, then the subject U does not succeed, since the packets are confused. The first series of perceptron with two signs will have decision functions:

$$R_j = \left(x_1^* - x_1\right)_j^2 + \left(x_2^* - x_2\right)_j^2,$$

where x^*_1 and x^*_2 – central values of the attributes when training the perceptron (it takes a numerical value corresponding to the type of the packet DNS – 1, DHCP – 2, HTTP – 3, etc.).

The use of the perceptron allows the creation of analyzers of hidden channels that operate on several characteristics, and the perceptron must be multi-row.

The assignment of the second series of the perceptron-based analyzer is the analysis of combinations of protocol packets that «bear» certain characteristics on the basis of which the information should be transferred. The transfer is synchronized with the initial and final combinations formed from the protocol packets in a strictly defined sequence (the transfer agents agree in advance). The model of the second perceptron series using one «carrier» protocol will include (for example, if there are two ip-addresses: ip_1 – logical zero, ip_2 – logical unit) possible combinations indicating the beginning or the end of the information transfer. For example, if you use a combination of eight packets, the model contains 256 options for implementing the start and end timing signals.

In order to speed up the flow of information, the data block between the beginning and the end of the process is transferred by logical zeros and units, which can be, as indicated earlier, ip-addresses. At the output of the second row of the percetron, we have the following sequence at time instants $[t_k]$:
$R^{ник}{}_j[t_k]$, $\{R^b_{i+1}[t_{k+1}],\ldots, R^b_{i+1}[t_{k+1}],\ldots,\}R^{ник}{}_m[t_{k+p}]$,
where $R^{ник}{}_j[t_k]$ – analyzer output, trained for sync packet «beginning of transfer»;

$R^{ник}{}_m[t_{k+p}]$ – analyzer output, trained for sync packet «end of transfer»;

$R^b_{i+1}[t_{k+1}],\ldots, R^b_{i+1}[t_{k+j}]$ – analyzer outputs trained to fix a logical unit and zero; are formed in a block of transmitted data.

The resulting sequence represents data traveling along a hidden channel. It should be noted that their transfer should be carried out in a limited time interval, so as not to be recognized. And besides, to reveal the probability of the existence of a hidden channel without using adequate task of analyzers is almost impossible.

Conclusion. *The information received from the hidden channel analyzer is necessary to apply methods that prevent the possibility of continuing the process with the participation of «illegal» agents. To implement such a task, it is proposed to investigate the methods of packet entanglement. Technically, this requires considerable data processing speeds, which predetermines the use of optical interfaces connecting the entanglement server and buffer storage, where packets are temporarily placed. Moreover, the algorithm should allow certain packets to be passed unchecked, which cannot be confused, otherwise the network devices will malfunction.*

Thus, the implementation of the perceptron-based analyzer for recognizing hidden channels allows to significantly increase the effectiveness of the control over them in the corporate segment of networks.

REFERENCES

1. Info Jett. [Electronic resource]: http://www.jetinfo.ru/jetinfo_arhiv/raspredelennye-ataki-na-raspredelennye-sistemy/o-kanalakh-skrytykh-potajnykh-pobochnykh-i-ne-tolko/2006. Last accessed 10.01.2017.

2. Internet-technology. [Electronic resource]: http://www.internet-technologies.ru/articles/article_2826.html. Last accessed 10.01.2017.

3. Grushko, A. A. Hidden channels and information security in computer systems [*Skrytye kanaly i bezopasnost' informacii v komp'juternyh sistemah*]. *Diskretnaja matematika*, 1998, Iss. 1, pp. 3–9.

4. Alekseev, V. M. Monitoring system of information security for high-speed transport [*Sistema monitoringa informacionnoj bezopasnosti dlja vysokoskorostnogo transporta*]. *Nauka i tehnika transporta*, 2016, Iss. 4, pp. 71–79.

5. Alcaraz Cristina, Lopez Javier, Kim-Kwang, Choob Raymond. Resilient interconnection in cyber-physical control systems: Computers & Security, Vol. 71, October 2017, pp. 2–14.

6. Osborn Emma, Simpson Andrew. On small-scale IT user's system architectures and cyber security: A UK case study: Computers & Security, Vol. 70, September 2017, pp. 27–50.

7. Lei Ding, Jun Liu, Tao Qin, Haifei Li. Internet traffic classification based on expanding vector of flow Computer Networks, October 2017, pp. 178–192.

8. Hongtao Sun, Chen Peng, Taicheng Yang, Hao Zhang, Wangli He. Resilient control of networked control systems with stochastic denial of service attacks, Neurocomputing, October 2017, pp. 170–177.

Information about the author:
Alekseev, Viktor M. – D.Sc. (Eng), professor of the department of Management and Information Protection, Russian University of Transport (MIIT), Moscow, Russia, alekseevvm@ramber.ru.

Article received 14.07.2017, revised 02.10.2017, accepted 05.10.2017.