D11-2002-292

P. M. Vasiliev[1], V. V. Ivanov[2,3], V. V. Korenkov[2],
Y. A. Kryukov[1], S. I. Kuptsov[1]

MAIN CONCEPT OF LOCAL AREA NETWORK PROTECTION ON THE BASIS OF THE SAAM «TRAFFIC»

[1]Department of Informatics, «Dubna» International University
of Nature, Society and Human, 141980, Dubna, Russia
[2]Laboratory of Information Technologies, Joint Institute
for Nuclear Research, 141980, Dubna, Russia
[3]International Solvay Institutes for Physics and Chemistry, CP-231,
ULB, Bd. du Triomphe, 1050, Brussels, Belgium

Introduction

We live in the dynamically developing world. It seemed the main concepts of safety in the interstate policy were defined not long ago. However, at the moment we are realizing a necessity of cardinal changes. The day of September 11, 2001, has forced the political figures worldwide think of main threats for all the states today.

Similar processes take place in telecommunication technologies, too. The present-day global network Internet was designed in conditions of possibility of a nuclear impact taking into account a provision of maximal reliability of the communications by introducing extra links and network nodes. The provision of maximal reliability of physical lines and network devices was caused by the threat that was actual at that moment. The application in network devices of integrated circuits with a high density of units has allowed one to increase considerably the reliability of the electronic devices used. This base has provided lately a stable operation of the communication links and hosts in the Network.

What is the greatest threat to million users of corporate systems and telecommunication services at present?

Like it occurs in the present-day politics, the greatest threat to the normal operation of information systems is caused by small groups of people (often single ones), irrespective of place of their residence and with absolutely inadequate (from the viewpoint of the majority of the population) ideas and purposes. To the same groups can be referred those who, utilizing telecommunication technologies, tries to solve their own financial problems. All of them can be called telecommunication terrorists.

The market competition between organisations, companies and banks makes them provide a wide access of users to their information databases, tools, services, and, accordingly, integrate the corporate systems in the common use global networks.

The cost of the confidential information stored on electronic carriers and transmitted via data links can be estimated, for example, by calculating the losses in case of usage by its competitors [1]. Apparently, the sizes of such losses can be compatible with the cost of the fix goods of the enterprise. There should not be underrated incorporeal losses of citizens, companies, countries in case of distribution or distortion of confidential information.

Well, one should not think that the information systems providing the operation of critical objects (military objects, atomic plants, airports, etc.) provide similar possibilities for unauthorized access to confidential information and management. Such systems usually operate in the framework of local networks not having physical links with common use networks. Besides, they, as a rule, apply nonstandard operating systems and data transfer protocols. However, even in this case the problems of information safety should be under stationary control of experts in view of possibility of unauthorized access "within" the systems from the serving staff.

Thus, the problems of provision of information safety of the Network gradually become the top-priority ones in the research on creating informationally safe automized systems and data transfer protocols, application of network nodes adequately reacting to various network messages, etc.

In [2] a system for acquisition, analysis and management of a network traffic (SAAM "Traffic") for a segment of the JINR local area computer network (JINR LAN) - the local area network of the university "Dubna" (University LAN) was presented. This system is located on the entry gateway LAN server and allows one to conduct a continuous monitoring of parameters of the network traffic. It provides visualization of results of the analysis of the traffic and helps the network manager make decisions on LAN managing.

The purpose of this paper is a classification of network attacks for the operating detection of undesirable events in the LAN of JINR and the university "Dubna" and working out the guidelines on modernization of the network devices and the LAN topology for decreasing the probability of implementation of threats to the computer networks and systems.

The first chapter will discuss the main concepts of the theory of computer protection and main types of remote attacks on computer complexes. The second chapter considers the structures of the network traffic in course of execution of main types of remote attacks in the framework of protocol TCP/IP. The third chapter discusses the main problems and structure of a LAN protection on the basis of the SAAM "Traffic".

1. Main principles of the network protection

The modern theory of computer safety deals with three main definitions [3]:

- *Threat* - any undesirable event in operating hard- and software of hosts, network devices, communication links resulting in an inadequate operation of the whole system. The undesirable event cannot by all means be caused by a hacker, it can occur due to erratic operations of a system manager (for example, random deleting of the database table) or machine failures (for example, in case of a hard disk failure).
- *Technological possibility (vulnerability)* - a consequence of unsuccessful, from the viewpoint of safety, engineering decisions in the field of implementation of algorithms and a program code of operating systems, data transfer protocols potentially permitting the hacker to implement the undesirable event.
- *Attack* - a targeted activity of the hacker applying known technological possibilities for implementation of an undesirable event.

Let us consider the first group of undesirable events [3], the so-called "threat".

- *Threat of disclosure* - disclosure of confidential information resulting in the heaviest consequences, as the fact of the disclosure cannot always be discovered in time.
- *Threat to integrity* - change or substitution of true information by false one is usually accompanied by disclosure of information. The threat to integrity can be minimized by applying nonstandard monitoring systems of information reliability.
- *Threat of refusal in service* leads to a temporal inaccessibility of one or several network operational lifes resulting in loss of service capability of the whole automized system. This is the most widespread type of attacks as it can be easy implemented.

Prevention of the probability of implementation of the mentioned three types of undesirable events can be done by "rapid analysis" of the network traffic on the basis of the SAAM "Traffic" [2]. However, further classification of possible types of attacks and systematization of the features of the network traffic on an example of the known scripts of executing remote attacks on network devices and hosts are required for carrying out such an analysis.

The main types of the network attacks on LAN can be classified [3]:

- Of the character of the effect on *active* and *passive* attacks. *The active attack* is aimed at changing the algorithms of operating the system's components and, accordingly, the whole system. The change of algorithms is reached, for example, by reconfigurating the system, the logic of operating the network connections and tools, failing separate parts of the system. *The passive attack* implements threat of disclosure by listening to data links and thus does not render the functioning of the system.
- Of location of the source on internal, network and internetwork attacks. At internal attack the source is placed in one domain of collisions with the attacked object and has a possibility to listen to absolutely all network packages of the object. During the network attack the source is located in one IP-network with the attacked object, but the network can be segmented by a switch, so the attacking person can listen only to the broadcast packages of the object. In case of an internetwork attack, the source and the object are located in different IP-networks divided either by a router or by an internetwork Firewall screen.
- Of a condition of beginning the execution on conventional and unconditional attacks. In the first case, the attacking person expects from the object a generation of inquiry of a particular type (for example, generation of DNS-inquiry to the DNS-server), or occuring an expected event in the work of the object (for example, turn off the computer of a legal user without the LOGOUT command). The unconditional attack implies an active effect on the object, despite the state of the system attacked. The example is the generation by the attacking person of a great number of packages of discovery of sessions for implementation of the threat of refusal in service.
- Of presence of feedback on attacks that require obtaining by the hacker the answer packages from the object, and attacks not requiring feedbacks.
- Of the OSI model level, where the attack is undertaken. At a *physical level,* for example, a direct connection to the wires of communication links for listening to a line or actual breakaway of the communications for neutralizing one of the subjects of attack is possible. At a channel level, a capture of packages from a uniform, distributed environment is possible. At a network level, the object under attack becomes transmission of IP-packages without confirmation. At a transport level, the objects under effect are algorithms of protocols TCP and UDP, at a session level, for example, attack with substitution of one of the subjects of TCP-connection, on a representation level - attack with substitution of ports and sockets is possible. The attack at an application level effects the algorithms of functioning a particular application.

Each of the known types of attacks is characterized by its own typical script of exchanging of network packages and thus there exists a potential possibility of formalising the scripts of the network traffic for attacks of a particular type. In this case, there is an opportunity without development of complex intellectual systems (and, accordingly, without enormous temporal expenditure) on the basis of a set of standard features (patterns) to fix the fact of carrying out a network attack of a particular type.

The scheme of the LAN protection proposed is very similar to quite effective systems of the anti-virus software, where for detection of virus some sets of standard texts with fragments of codes of programs - viruses will be utilized. Such an approach allows one to utilize typical schemes of the network traffic for LAN protection as well as to develop quickly some effective algorithms of protection from new scripts of the network attacks.

2. Traffic analysis for some scripts of network attacks

As it has been already mentioned, one of the most dangerous threats is the threat of disclosure - a disclosure of confidential information. As a rule, the computer networks at a level of workgroups of big enterprises and small offices use one of the popular LAN standards (more often Ethernet) representing a uniform data transfer environment devided in time by all computers. Such an approach makes the LAN creation much cheaper at the expense of minimization of expenses on equipment and cable laying, but at the same time it provides access of each computer absolutely to all the network packages transferred within of this network.

2.1 Listening to the data link

It is the broadcast aspect in operation of most LANs that contains a potential danger for implementation of different type attacks, and, as we shall demonstrate below, the listening to the data link is one of the basic conditions for making the most attacks.

As a result of listening to data links, the hacker can receive all the necessary information on LAN, namely: the network architecture, used services and tools, addresses of hosts and servers, names, and sometimes keywords of users, router information, temporal schedules of node operation, etc.

Thus, the urgent detection of facts of listening to the computer communication links is one of the important conditions of the successful struggle against external and internal attacks.

Listening to the channel is a passive attack. It does not leave any tracks in the total volume of the network traffic. It is impossible to struggle against passive attacks by a passive watching out the behaviour of the network traffic. Active periodic actions directed at the detection of a network packages capture program - a sniff program - are needed.

The problem of detecting such programs can be realized with the help of the SAAM "Traffic" that actively affects the sniff programs based on the known fact of independent work of program modules operating at various levels of the OSI model.

In a regular mode of operating the network adapter begins receiving any package transferred via the network by recording the obtained data in its receiving buffer. As soon as the obtained bits are enough for analysis of the address field of the receiver of the package, the network adapter decides on necessity of further reception of the package (when the address of the receiver coincides with the home address of the network adapter) or on termination of reception and cleaning the receiving buffer (if the address does not coincide). The check-up procedure is assigned to the channel level of model OSI (the network adapter devices).

With the help of commands of the NDIS specification, it is possible to change the mode of the normal operation of the channel level of the network adapter assigned by the Ethernet standard, on the capture of all network packages. Thus the operation of the program modules of the protocol TCP/IP does not change, and the stack of the protocol fulfills its functions. Therefore, the following algorithm of detecting the operating sniff computer is possible.

The SAAM "Traffic" system forms a "wrong" package containing not existing in LAN MAC-address, but having in the IP-header an actual (responding to the checked-up PC) IP-address. Aware of the idea of capture of all the packages translated on the network, the channel level of the sniff computer will take the "wrong" package (not discard it as required by the Ethernet standard) and transmit it for analysis to the program module implementing the network level of the model (the IP-protocol). The network level will receive a "pure" IP-package with a remote header and end of the frame of the channel level so it does not get a possibility to test the correctness of its processing by the channel level of the network adapter.

If the package in the data field contains, for example, a command of the protocol ICMP, intended for check-up of the service capability of IP-networks (the PING command), then the subroutine of implementation of protocol ICMP in the IP unit can only process the command in a standard way that will result in the creation of an answer package informing on the service capability of the systems addressed to the source.

The reception of such a package allows one to fix the fact of listening to the information in LAN by a particular user. Otherwise, when the channel level of the computer under study works in a regular mode, the forming of the answer package will not happen.

Besides, some present-day network adapters, realizing a pipeline processing of coming packages, allow one to separate the dataflows, one part of which is routed on processing to the standard stack of protocols, and another - to the simultaneously operating sniff program. In this case, in order to obtain the answer package, it is necessary to make so that the standard algorithms of the network adapter will not be able to unambiguously identify an accessory of the package to one of the protocols and routed "the disputable package" to both directions. The used in this case MAC-address of the receiver can have, for example, the following view: FF-00-00-00-00-00.

It should be noted that the routed by the SAAM"Traffic" packages - researchers are the address ones at an IP-level (instead of broadcasting). Therefore, in order to detect the fact of listening to the network, it is necessary to investigate all possible addresses of this IP-network including even IP-addresses not involved at the moment. In case of the university "Dubna" LAN, the SAAM "Traffic" has to generate 512 packages of the researchers, each with a unique IP-address of the researched computer in the LAN. The package with the PING command of the protocol ICMP has a minimal size: 64 bytes without a preamble. Taking into account that a 10 MB/s Ethernet network produces up to 14800 minimal size packages per second, the generated auxiliary traffic will not limit the capacity of the whole network even during small time intervals.

The periodic sniff-scanning of the network traffic with the help of the SAAM "Traffic", for example, every 10 minutes, does not provide a way for the hacker neither to listen to a segment of the network nor to utilize this subnetwork as a foothold for realization of other types of remote attacks.

The important element of monitoring LAN with the help of the SAAM "Traffic" is the test of the correspondence of MAC-addresses of the PC network adapters in LAN to the IP-addresses produced at registration, and of the absence of computers with nonauthorized IP-addresses. As it is impossible to apply the program of listening to the network, it would be tempting to utilize nonself MAC-address, IP-address or the NETBIOS of the computer.

The SAAM "Traffic" maintains the database on the equipment of computers in the LAN [2] and on the basis of protocol ICMP (for example, with the help of the NBTSTAT.EXE code) provides a possibility of control over the correspondence of these three addresses to the addresses registered in the database. Such extra control increases the auxiliary traffic in LAN a little, however, it is the extremely effective tool in the LAN protection.

2.2. Technological especial features of operating the ARP - server in TCP/IP networks

Unfortunately, the address of the network adapter (MAC-address) does not allow one to create big distributed networks, as it does not provide a possibility (a parameter) for grouping computers together in a territorial manner to create subnets. On the other hand, it unambiguously and automatically identifies the computer in the framework of a particular segment of the network. Besides, in order to identify a particular computer in LAN, different addresses at different levels OSI are applied: at a channel level - a MAC-address, at a network one - IP-address, character addresses are used as well. It can be one of the reasons of the technological vulnerability used for implementation of network attacks.

The application of several identifiers leads to a necessity of building-up systems permitting one to determine a correspondence of one of the names to the remaining ones. In particular, while network searching the server by the name of TIGGER (by the net view tigger command), the correspondence of the name TIGGER to the IP-address of this server is determined, for example, 159.93.167.50 and further - correspondence of the IP-address to the MAC-address of its network adapter, for example, 00-01-1A-16-B8-CA.

The task of search of the MAC-address on the IP-address is fulfilled by the protocol of the network level ARP (Address Resolution Protocol). Let us consider a scheme of addressing the packages in the Internet and the safety problems arising. The base protocol of exchange in the Internet is the protocol IP permitting transfer of the IP-package to any point of the global network. The search of a target by intermediate network devices is performed on the basis of analysis of the IP-address. After delivery of the IP-package in the subnetwork of the receiver, the local router should deliver the package with the data transfer technology used by the network adapter of the target. Here a number of necessary operations should be done, too, as the router can access to an addressed host for the first time and does not have appropriate names in its base.

Let us consider a scheme of the protocol ARP operation:

- the router sends a broadcast inquiry where it mentions its MAC-address and asks to answer the computer having the indicated IP-address;

- the broadcast inquiry will be received by all the computers of the network segment, but only that PC will answer, for which the requested name coincides with its own name. Moreover, the IP- and MAC-addresses of the router obtained from the inquiry before sending the answer, will enter the ARP-table of correspondence of addresses at the requested computer;
- having received the answer, the router brings the data to the ARP-table and sends a message to the target using the MAC-address obtained.

Protocol ARP works in the framework of a particular segment of the network and therefore has a local character. The analysis of protocol ARP shows that on its basis there is a possibility of carrying out an attack with implantation in the network of a false object. As a result of such an attack, it is possible to change the packages route and, accordingly, to assign the hacker's computer traffic from the network host he is interested in. For the concentrators' based LAN such an attack losesits significance as the hacker can easy get access to the traffic of any network computer by using a sniff program.

Another situation takes place for the networks broken down into segments with possible the help of switches. In this case the attack based on the protocol ARP looks most.

Let us consider a possible script of such an attack. Let it be necessary for a hacker to receive unauthorized access to information about exams stored on the remote education server of the university "Dubna". The university LAN is well segmented and does not submitive a hacker access to this server's traffic. Besides, the sniff program available on its computer will be captured by the SAAM "Traffic" immediately.

In such conditions the following script of implantation of the false ARP-server is possible (Fig. 1):

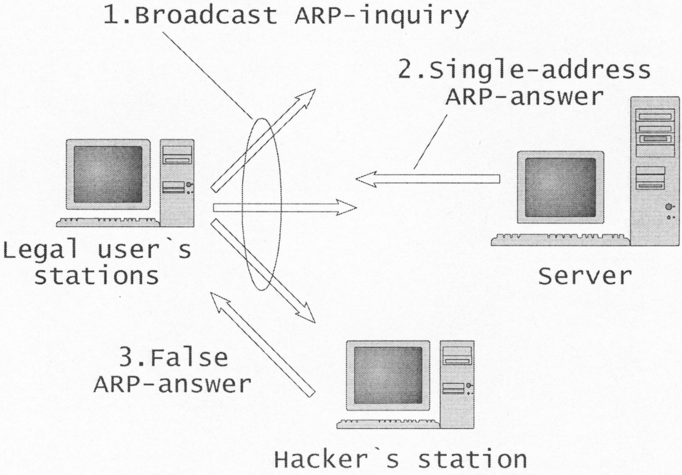

Fig.1. A script of implantation of a false ARP-server

- Waiting a broadcast ARP-inquiry from the PC of one of legal users of the remote training system possessing all the necessary privileges; this inquiry identifies the user intended to work with the server;
- Upon obtaining the inquiry, a false ARP-response is transferred to the asking host, where the MAC-address of the attacking server and the IP-address of the demanded remote training server is mentioned.

Thus it should be noted that, for example, the OS Windows changes its ARP-table at the moment of arriving the ARP-response, even if the computer did not dispatch inquiry. Therefore, the hacker does not have even to hurry up with sending a false response. Such a response can be transmitted immediately after the ARP-response of the server since in the ARP-table of the attacked computer - client there is only a correspondence of IP- and MAC-addresses of the last response.

Then a legal user will attempt to register in the system under his name and keyword. However, beginning from this moment, all packages will be routed to the hacker's computer and then they will be re-routed on the exact path (Fig.2).

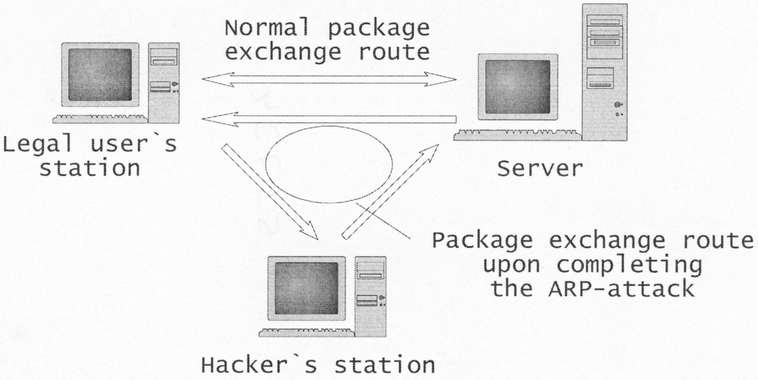
Normal package exchange route
Legal user`s station
Server
Package exchange route upon completing the ARP-attack
Hacker`s station

Fig.2. A rerouting of the package exchange upon completion of ARP-attack.

All transmitted packages with responses are one-addressed and they are routed by switches to the "target" by optimal paths, therefore, the SAAM "Traffic" can not fix such an attack only on the basis of analysis of the traffic.

At a first glance, it can seem that it is impossible to apply the system of the analysis of network attacks placed on the external gateway server to detect such intersegment operations. However, it is not the case as we have missed a small detail. The point is that the reception of packages from the flamed network server by a hacker will be impossible without changing over the network adapter in a sniff mode or else without changing the IP-address, as the packages will come with a correct MAC-address and contain the IP-address of the remote training server. Therefore, in this case the packages will be discarded not only at a channel level (i.e. by the network adapter) but also by the IP-protocol unit, so the attack will not reach its purpose.

2.3 To make the technological possibilities of the attack serve DHCP

Using several types of addresses on hosts operating under the protocol TCP/IP leads to a necessity of the manual configurating of computers by network managers. This process is rather routine and laborious as it is necessary practically to detect manually all movings of computers in LAN, modernization of network equipment, installation of new PC, etc. The size of such operations sharply increases in large LANs containing hundred and thousand computers.

In order to accelerate this procedure, a dynamic protocol of configurating the DHCP host in LAN will be utilized. The DHCP tools centralize debugging the protocol TCP/IP, control selection of the configurational information, automatically assign IP-addresses to the LAN computers. Having installed the DHCP- server, one ceases to configurate the network manually as the installation of network services of the operating system on a new computer debugs the protocol TCP/IP by default for the automatic obtaining of required parameters [4]:

- IP - address of the computer;
- Mask of a subnet,

as well as additional parameters:

- IP- address of the gateway server by default;
- IP- address of the DNS- server;
- IP- address of the WINS- server.

When starting the new computer, the stack of protocol TCP/IP does not have necessary information for organization of its interaction with other hosts in the network. The obtaining of the necessary debugs occurs as a result of exchange of the client and the DHCP server by the following four packages [4]:

- DHCP Discover - inquiry on obtaining customizations from the DHCP server. The client does not know layout of the DHCP-server so the frame is a broadcasting one both at the MAC-address level and at the IP-address level.
- DHCP Offer - proposal of the DHCP server containing the suggested for usage IP-address. The server can not directly address to the inquiring computer because it has not got an address yet.
- DHCP Request - choice of the address, it is sent off by the client after making decision whether the suggested address suits him. It is sent off also by a broadcasting package (since the address is not assigned the client yet).
- DHCP ACK - confirmation of the server about final fixing the suggested IP-address for the client and transmission of the list of all additional parameters installed at the DHCP-server.

The operational analysis of this protocol for safety shows its complete vulnerability. First, all frames used by the protocol are the broadcasting ones thus it takes out the necessity of using by the hacker a sniff program and does not require to troubleshoot segmentation of the traffic by switches. Secondly, utilized is not a deutogram UDP protocol identifying the connection. In addition, there is a possibility for adjusting translation of the broadcasting DHCP-inquiries by the routers in the adjacent subnets (to decrease the total number of the DHCP-servers in the network) that multiplies the number of potential objects of the attack.

In frames of such practically an unguarded network service it is possible to implement a lot of variants of unauthorized LAN usage.

Let us consider one of possible scripts. The hacker implements a scheme of a broadcasting search by the client of the DHCP-server and realizes a "false object introduction" scheme. Having received, like all the LAN computers, a DHCP-inquiry, the hacker generates a standard DHCP-suggestion and points his IP-address as a message source. Thus the attack can not be accompanied by suppression of operation of the real DHCP-server (in large networks several DHCP-servers can be used), the client is content with obtaining a response that came first and discards the remaining(Fig.3).

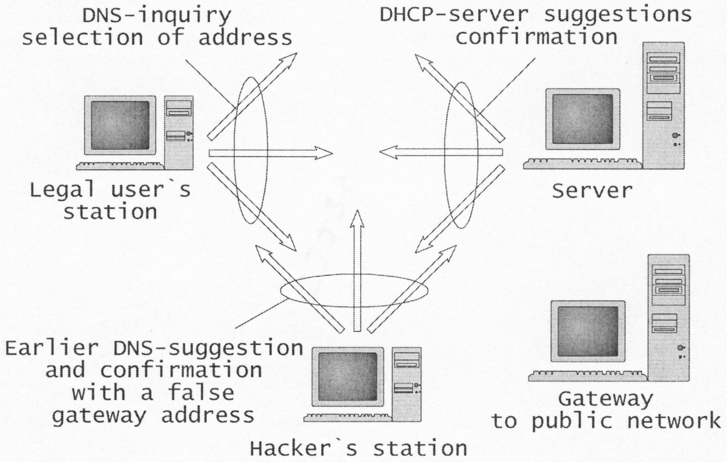

Fig.3. Implementation of the scheme realizing a "false object" with the help of the DHCP-suggestions with a false address of the gateway server

Further on, the "output" process of the IP-address goes on in a usual manner, however, here a legal networker will receive false padding addresses (the address of the gateway server by default, WINS- and DNS-address of servers), and all his traffic will be controlled by the attacking person (will be transitted through his computer). Thus, the threat of disclosure will be implemented.

One should also take into consideration that the inquiries about obtaining addresses are generated in a mass order at the moment of morning switching on the computers by the users (for example, about 9 a.m.). At this moment tens and hundreds PC can be attacked the traffic of which can be used by the hacker in a similar way (Fig.4).

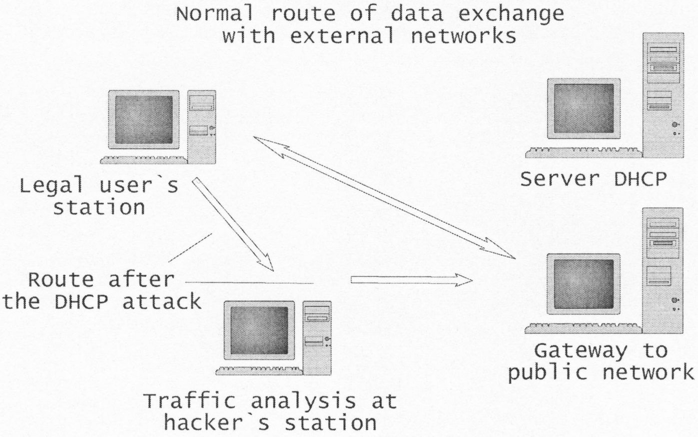
Normal route of data exchange
with external networks
Server DHCP
Legal user`s station
Route after the DHCP attack
Gateway to public network
Traffic analysis at hacker`s station

Fig.4. A rerouting of traffic after implementation of DHCP-attack

Another purpose of such an attack can be a provoking of threat of refusal in service. In this case the hacker can simple distribute wrong information on customizations of the protocol, thus it will be impossible to perform network operations by a user (Fig.5).

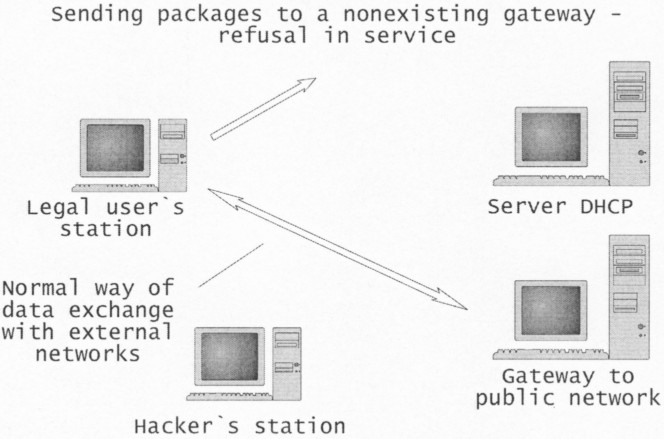
Sending packages to a nonexisting gateway -
refusal in service
Server DHCP
Legal user`s station
Normal way of data exchange with external networks
Gateway to public network
Hacker`s station

Fig.5. Implementation of threat of refusal in service with the help of DHCP-attack

A possible solution of the problem of protection of the DHCP service on the basis of the SAAM «Traffic» consists in the following. The broadcasting of the DHCP-traffic allows one by a passive listening to detect a presence of a nonregistered PC in LAN that generates a DHCP-traffic and then, if necessary, to suppress its activity by a mini-storm of inquiries on TCP-connection (having in mind the supposition about out of operation of a large number of corporate PCs) and to inform the system manager about the current events.

2.4 To make the technological possibilities of attack serve the DNS

As it is known, the hosts in the Internet are addressed not only with the help of the MAC- and IP-addresses. As a matter of convenience of storing host names, the padding addressing is applied. It is not connected with the data transfer protocol and implies composite character addresses of servers which are unambiguously connected to the IP-address. An example of such a name is the address: WWW.UNI--DUBNA.RU. Access to the WWW-server in the Internet through a browser is possible via the IP-address and with the help of a character name.

DNS (Domain Name System) service is responsible for the support of correspondence of the IP-address and the character name. The DNS-service is constructed as a hierarchy scheme on the basis of the DNS servers, each being responsible for its service area. The server supports operation of a database of correspondence of host names to IP-addresses, the data entry being performed manually by a network manager. If the network has no DHCP service, any workstation, connected on-line to Internet, is configurated manually, where the IP-address and the DNS-server serving this zone are mentioned.

The DNS-data exchange, performed within the transaction, between a workstation and a DNS-server consists of an inquiry and a response. The inquiry on permission of a name is dispatched by the client as a small frame whose size is determined by the length of the name requested. The frames of inquiries DNS are one-addressed and are routed directly to the DNS-server. It should be noted that the used UDP-protocol (53-rd port) is a deutogram one, and it does not require identification of the user with the help of a connection procedure.

Having received the inquiry, the DNS-server checks a record in the database appropriate to the name asked. The answer frame contains section "DNS Answer", where both the asked name and its IP-address are located. If the name does not exist, the server either will return the message "Name does not exist" to the client or (in the mode of recursion) will transmit the inquiry to another server. If the first recursive DNS-server has no data on the asked name, it transmits the recursive inquiry to the DNS-server following on hierarchy. The size of the frame thus does not vary, and the address of assignment and source is adjusted only. If the higher DNS-server has necessary information, it transmits it to a first server which in turn transfers the answer (Fig.6) to the client.

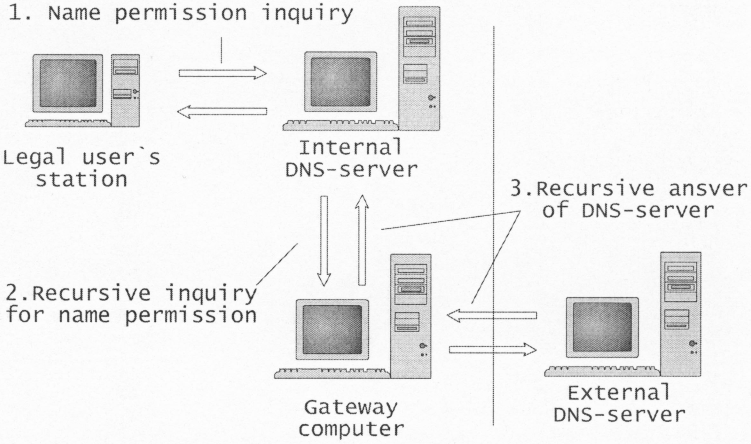
1. Name permission inquiry
Legal user`s station
Internal DNS-server
3.Recursive ansver of DNS-server
2.Recursive inquiry for name permission
Gateway computer
External DNS-server

Fig.6. A scheme of data exchange between a workstation and a DNS-server if asked on permission of a name

The use of such tools provides the hacker with some ways for carrying out attack on the DNS-service.

First, there can be two purposes of such an attack:

- Input of a false object for rerouting the paths of packages at interaction of hosts in the network;
- Change of the host name or its IP-address with the purpose of enforcing the legal networkers for obtaining extraneous information when calling the known network resources.

Secondly, the attack can be directed at a network station (a particular user will be suffered then) or at a DNS-server of a particular level of hierarchy. In the latter case not only users working with this server will be under attack, but also other LAN users, as the information on the false path will be in due course doubled in the cache of other DNS-servers committing recursive inquiries.

Let us note that the attacks on the DNS-service, as against attacks on the ARP protocol, can be both internal, network and internetwork ones, when the attacking computer can be at a huge distance from the object under attack. Thus the input of the false path will allow one "to throw" the LAN traffic, for example, to another continent, and after analysis to bring it back. In this case, the attacked object will experience only increasing a system's response time that, basically, can be caused by other reasons, too.

Let us consider some scripts of carrying out attacks of the mentioned type.

2.4.1 Interception of DNS- inquiry

In case of an internal attack, the interception of a DNS-inquiry by the computer with a sniff program is possible. In case of a network attack, the interception of one-addressed DNS - inquiry is possible after a successful ARP-attack. The interception entails a false answer of the port of the remailer in the UDP-package and the inquiry identifier (ID) are indicated in the intercepted inquiry. The false answer can contain the IP-address of the attacking computer or the IP-address of an extraneous site. Further the hacker obtaining a first information package from a flamed host for saving and analysis, then the information package is routed on the actual address of assignment (Fig.7), or else the attacked PC gets information of extraneous contents (Fig. 8).

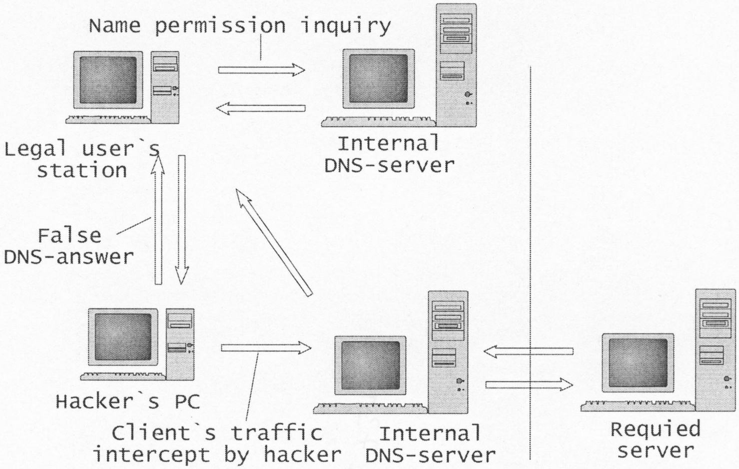

Fig.7. Attack "interception of DNS-inquiry" with the purpose of a vending the traffic of the attacked PC to the attacking server

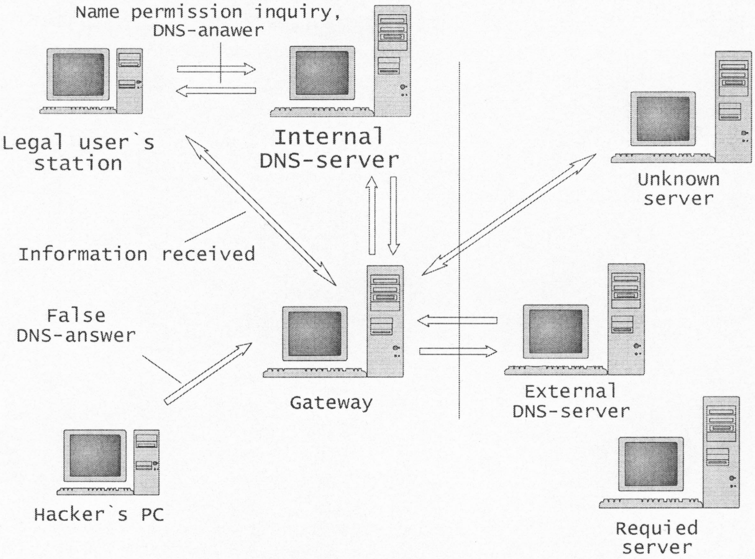

Fig.8. Attack "interception of DNS-inquiry" with the purpose of substituting the IP-address asked by a legal user

The LAN protection from the internal or network attacks is easily solved with the help of the SAAM "Traffic" in frames of an anti-sniff program.

2.4.2 Directional storm of the DNS-answers

An intersegment attack can be much more dangerous. In this case the hacker fails to receive a one-addressed DNS-inquiry in his network. Moreover, in order to organize a successful attack, it is necessary to know the address of the server whose name can be asked by the object.

In this case the hacker will go by way of search of legal clients of the resource of interest. The search can be implemented not only by technological means, but also by conversation on correspondence, from various printed sources, etc.

Having figured out that a networker is connected to the required resource, the hacker can organize the attack based on transmission of a great number of DNS answers directed at the IP-address of the object that will indicate the IP-address of the attacking PC as a required address. The hacker cannot know the time of appearance of the required inquiry, therefore he should realize a storm of the DNS-answers during a long period of time.

One should take into account that the attacking person does not know the number of the UDP-port, from which the DNS-inquiry and two-byte identifier of DNS-inquiry (ID) will be transmitted. However, it is known that the port's number has a restricted range of numbers beginning from 1023. The exhaustive search of all possible numbers of the UDP-port in the DNS-answers can reach the purpose of the attack if to take into account a possibility "to slow down" with the answer the real DNS-server. The attack permitting to sharply reduce the performance of the server, will be considered in section " Directional storm of TCP- inquiries on creation of connection". The two-byte identifier of the ID inquiry usually is not a problem at all, as in the DNS-inquiries of the majority browsers this identifier is set equate to unity.

Thus, the analysis of this type attack shows that quite a particular script of the traffic behaviour takes place at the moment of beginning the attack - a sequence of the network packages coming on the external gateway server, with the identifier of the DNS-answer having quite a particular periodicity per unit of time and containing exhaustive search of the number of the remailer's UDP-port. Such type traffic can be easily identified in a common stream of packages passing the SAAM "Traffic" and blocked on the basis of using a time filter.

2.4.3 Directional storm of recursive DNS - answers on the DNS- server

The DNS-server regularly gets inquiries from its clients the solution of which is impossible due to absence of appropriate information in its database. In this case the DNS-server itself appears in the role of a generator of DNS-inquiry, accessing for permission of a character name to a DNS-server of a more high level and then transfers the obtained information to the asked host. It is seen from this scheme that the hacker can apply the described above scheme of attack (interception of inquiry and storm of DNS-answers) to input in fallacy the DNS-server. Thus it is necessary to take into account that in case of a successful attack, the false IP-address in due course will be directed to a great number of the hosts - clients using the DNS-tools of this server. Besides, the answer obtained from a higher level server will be stored in memory of the DNS-server, usually, not so long (60 minutes by default). Therefore, the addresses even frequently used by corporate computers, will be for certain updated by recursive inquiries of the server every morning, and this considerably simplifies the task of the hacker.

Such an attack can be aimed at vending the information flow to a false object for the analysis of the intercepted traffic or else it can be directed at implementation of threat to integrity - for example, replacement of access of a user to the information he needs by access to sites of "doubtful contents" (Fig.9).

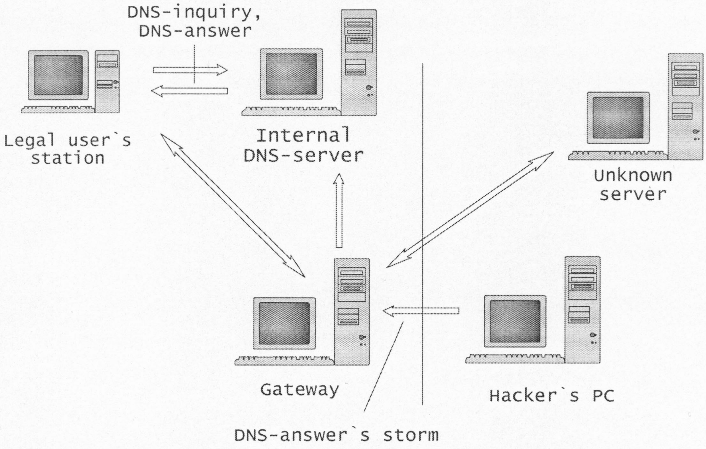

Fig.9. Substitution of access of a user to a required information by demonstrating a "doubtful contents" site.

When implementing the attack, the interception of the inquiry is rather problematic as these packages are intended usually for DNS-servers being in other subnetworks, and they are transmitted through the trunk communications, the connection to which is not provided for ordinary users.

Therefore, a storm of the DNS-answers is necessary for realization of the attack. As against a similar DNS-attack on a host, the DNS-server at generation of inquiries actively uses a two-byte identifier ID in the header of inquiry. The number is increases at each new inquiry by unity. It is possible to determine a provisional current number, for example, by generation of standard DNS-inquiries by a hacker with a subsequent analysis of the average speed of changing the identifiers ID from the headers of DNS-answers. Otherwise, the hacker can attempt to solve the problem "in forehead", i.e. by simple exhaustive search of all possible numbers. Exhaustive search is quite a long process (in a limiting case it is necessary to transmit 65536 variants of inquiries). One can also try to take the DNS-server out of operation, for example, by applying one of the circumscribed below ways, with the purpose to achieve a reboot of the server OS, that will approach the ID number to unity.

For both variants of attacks there is a clearly expressed storm of DNS - answers, only with exhaustive search of the number ID in the package headers. In order to provide the LAN protection from such type attacks on the base of the possible scripts of remote attacks of the SAAM "Traffic", it is necessary to have a number of templates to make the attack identification on the DNS-service of the server.

2.5 Attack on the basis of technological features of the TCP protocol.

One of main protocols in networks TCP/IP on delivery of data from one PC of the network to another is a TCP protocol (Transmission Control Protocol). Until data transfer starts on the basis of this protocol, it is necessary to install a virtual connection between these computers (simple data transfer can be implemented without usage of the TCP protocol). As soon as the virtual connection is installed, there is a possibility to allocate the packages of the virtual connection in the common stream of coming packages on the basis of numbering the packages transmitted by the source computer, beginning from the first one, as well as to inspect by packages of confirmation a successful delivery to a target of the next (numbered) package.

An additional task of the protocol is the protection from substitution of one of the subjects of the TCP-connection. For identification of the package, except the IP-addresses of the remailer, a counter of sent packages, called here the Sequence Number (Number of sequence) is used as well as Acknowledgment Number (Number of confirmation). While creating the virtual TCP-connection, the numbers of sequence and confirmation start not from unity but from some almost random number (each of numbers has 32 bits in the TCP-header). In addition to this, for transmission 6 controlling bits are used:

- URG - field of the urgent pointer;
- ACK - meaning of the confirmation field;
- PSH - function of promoting;
- RST - to restore connection;
- SYN- to clock the numbers of sequence;
- FIN - end of data transfer.

A somewhat simplified diagram of creating the TCP-connection presented below (Fig.10):

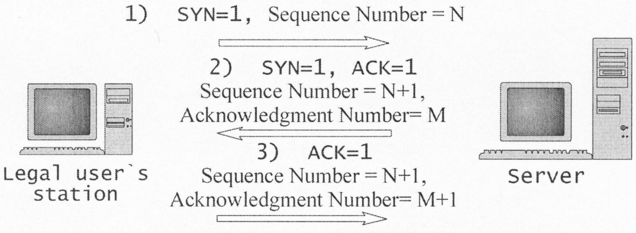

Fig.10. A simplified diagram of TCP-connection

- The initiator of TCP-connection transmits a frame - inquiry on creating the connection in which the flag SYN (SYN = 1) is lifted and installs the initial number of sequence;
- The target responds by a frame of confirmation of availability to install connection with lifted flags SYN and ACK and offers its initial number of sequence; thus the number of confirmation contains a number from the field of sequence of the first package increased by unity;
- The initiator ends the installation procedure by a third frame, with the lifted flag ACK and the numbers of sequence and confirmation increased by unity.

After the virtual connection is installed, the message transfer between transmitting and receiving computers is fulfilled.

2.5.1 Substitution of a subject of TCP-connection

Clearly, the process of installing the connection identifying the source of the received package in the framework of the TCP-connection on three fields (IP-address, numbers of sequence and confirmation) provides a way for interaction from a false name. The following situation looks quite tempting for a hacker. There is a possibility to wait for a moment, when one of legal users - system administrators, by creating the TCP-connection, performs identification and autification on the server and slightly loiter. There are no hindrances, by capturing previous packages with necessary numbers, to prolong work with the server on behalf and from the IP-address of the legal user - manager. As at the moment of restoration of operation of the manager his packages will be disallowed in the framework of the installed TCP-connection because the numbers saved on the computer of the client will become "outdated" (work of the hacker with the system leads to increasing the numbers of sequence and confirmation), and the manager should install a new connection.

Such a script can be implemented only if the attacking person has a possibility to capture network packages for analysis of numbers of sequence and confirmation with the help of a sniff program (utilizing internal or network attacks). In this case, the application of the anti-sniff subsystem of the SAAM "Traffic" can provide protection of LAN from this type attacks.

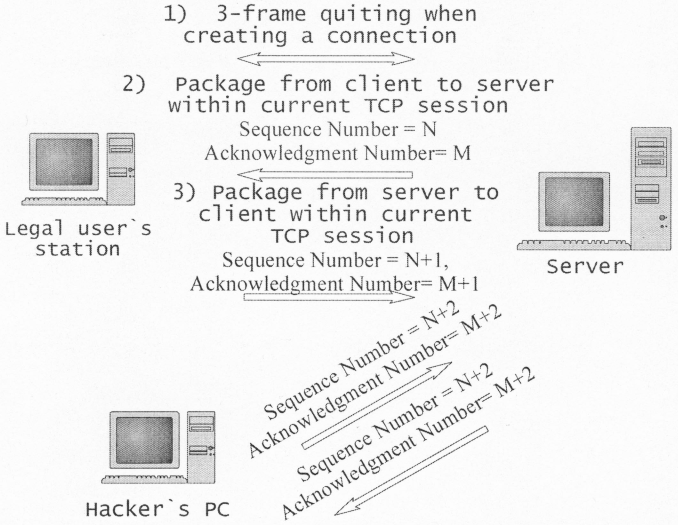
1) 3-frame quiting when creating a connection
2) Package from client to server within current TCP session
Sequence Number = N
Acknowledgment Number= M
3) Package from server to client within current TCP session
Sequence Number = N+1,
Acknowledgment Number= M+1
Legal user`s station
Server
Sequence Number = N+2
Acknowledgment Number= M+2
Sequence Number = N+2
Acknowledgment Number= M+2
Hacker`s PC

Fig.11. A scheme of attack with replacement of a subject of TCP-connection

2.5.2 Directional storm of TCP- inquiries on creating a connection

There are a great number of scripts of remote network attacks directed at provoking threat of refusal in service by violating the service capability of network computers.

Let us consider the simplest scripts.

Directional storm of TCP-inquiries on creating a connection - one of the mentioned scripts.

Clearly, the server, intended for interaction simultaneously with many clients, has a possibility to install more than one session of a TCP-connection. Thus the connection is not installed immediately but during some time required for generation of packages of a three-frame quiting procedure. In case of obtaining several packages in sequence with inquiry of creating a connection, the server can not answer all clients at once. Therefore, it should save these inquiries in its memory and to process them sequentially, by enqueueing on processing due to the course of arrival.

In this situation the attack based on transmission of a great number of inquiries about creation of the TCP-connection (Fig.12) is possible. Here the server's processor is obliged to generate for each inquiry a number of confirmation and to form an answer package. The procedure takes some time. In case of using high-speed trunk links, such quantity of inquiries on connection can be transmitted that even the most high-performance server will spend 100 % of CPU time to generate answers. As a result, the server either ceases to respond legal inquiries (refusal in service), or completely "hangs up".

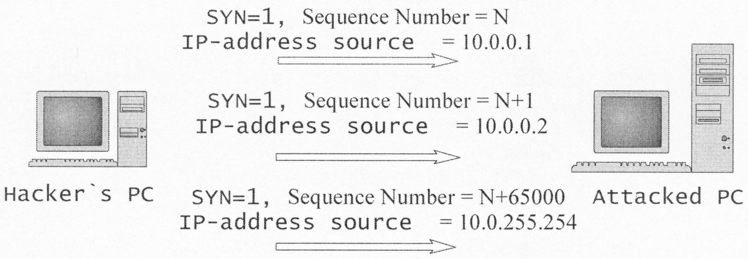
SYN=1, Sequence Number = N
IP-address source = 10.0.0.1
SYN=1, Sequence Number = N+1
IP-address source = 10.0.0.2
Hacker`s PC
SYN=1, Sequence Number = N+65000
IP-address source = 10.0.255.254
Attacked PC

Fig.12. Directional storm of TCP-inquiries on creating connection

The situation becomes more complicated because the fourth TCP/IP version does not allow one to detect the package routes from remote subnetworks. That is why the attempts of implementation of protocol TCP/IP of some manufacturers of the network operation systems with limiting the quantity of open TCP- sessions with one IP-address will not lead to protection against such type attacks. Nothing hinders to generate the storm of TCP-inquiries with exhaustive search of any IP-addresses as the hacker does not expect any answer from them.

The protection against the attacks of the mentioned type can be implemented by the system SAAM "Traffic". The layout of the system on the LAN external gateway server allows one to substantially limit the quantity of inquiries on creation of a TCP-connection with a particular IP- address of the package receiver.

2.6 Attack with usage of errors in the units of network services

Clearly, the most hackers are not the experts in the area of telecommunication technologies and they hardly can realize the attack that requires carrying out a network traffic analysis. Their main objective is the implementation of threat of refusal in service with application of available programs using known errors in the units of network services. The manufacturers of network operation systems certainly know about the existence of such vulnerable areas, but it is not always possible to remove the error locally, without a cardinal processing of the core of the system.

2.6.1 Attack with usage of incorrect data in header

One of possible ways is the attack with usage of the package, where the IP-address of the source in the header coincides with the IP-address of the receiver, and in the TCP-header the port of destination coincides with the source's port (Fig.13). Experiments show that many operation systems inadequately take the obtaining of such a package. The server can spend 100 % of its CPU time during several tens of seconds for processing the received information refusing in service to legal users. Thus, it is possible "to slow down" the server operation for a more long period of time periodically sending incorrect data to it.

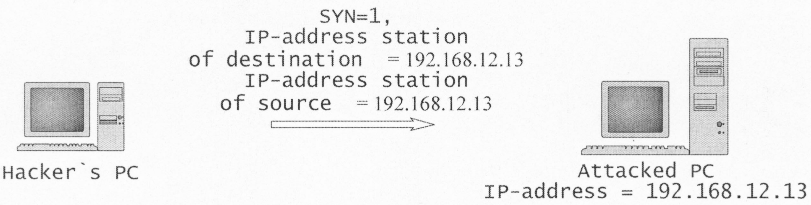
SYN=1,
IP-address station
of destination = 192.168.12.13
IP-address station
of source = 192.168.12.13
Hacker`s PC
Attacked PC
IP-address = 192.168.12.13

Fig.13. Attack with usage of an incorrect address in the package header.

The analysis of the address part of coming packages in the SAAM "Traffic" allows one to prevent implementation of such an attack.

2.6.2 Attack with usage of an error in the unit of assembly of fragmented packages

One of the conceptual advantages of the TCP/IP-protocol is a possibility of fragmentation of packages at data transfer in the networks using various technologies. Indeed, the Internet is a set of local networks conjugated by gateway servers. The local network can be constructed with the help of various technologies. For example, for data transfer from one Ethernet network (the size of the package varies from 64 up to 1518 bytes) to another Ethernet network, a transit transmission through the network of the ATM standard (the package size - 53 bytes) is required. Such a transmission would not be possible without separating the large Ethernet package into fragments for transmission through ATM.

Unfortunately, the fragmentation procedure is not free of errors. The developers of network protocols have tried to provide various nonstandard situations originating during the assembly - disassembly of packages. In particular, there can be a situation, when the beginning of the next fragment is responded by the address hitting not at the end but in the middle of the previous one. In this case, it is necessary to align the fragments and to put data on correct places. The algorithm of alignment leads to a negative shift value, if the length of the coming fragment is less than the size of the overlap. The hacker can take the advantage. As the shift shows a current address in the computer RAM, its negative value leads to the record of the fragment on a random address, and it, in turn, can cause refusal in the operation of the operation system's programs.

Attacks of this type can be identified with the help of SAAM "Traffic" by analysis of the lengths of the fragment and shift.

2.7 Remote scanning of ports on the attack's objects

At the initial stage of organization of a remote attack, the hacker has to spot potential possibilities for its realization. For this purpose, he needs to collect information on the services and tools of the object. Each of such programs is a server application responding the inquiries of clients. The call to a required tool takes place after identification of the appropriate port's number of the protocol TCP. Each calling client, before starting the interaction with the server, is obliged to install a virtual TCP-connection, irrespectively of the service of interest.

That is, at the initial stage all calls are of the same form, the number of the port of destination only varies. The hacker only has to generate TCP-inquiries with exhaustive search of possible TCP-ports. The obtaining of confirmation with the lifted flags SYN and ACK for the sent inquiry allows him to detect the operating server program.

The scanning of TCP-ports can be revealed with the help of SAAM "Traffic" on the regular arrival at the particular IP-address of packages with the inquiries containing a sequential search of the ports of destination.

3. Basic problems of the of LAN protection subsystem

The attempts to create systems for an effective LAN protection from network attacks have been undertaken for a long time. In particular, the software products of the Firewall family are aimed at the solving of the task. They provide LAN protection by inclusion in the process of routing the procedures of various filters thus essentially limiting the spectrum of applications realized in the network. In the market of commercial products there are also more developed systems of bucking to network attacks, some of which will be represented below.

3.1. The ICEcap Security Suite system for intrusion detection

The ICEcap Security Suite is a hybrid security system that comprises some components. ICECAP Manager installs, controls and maintains the software products of three types: BlackICE Agents, BlackICE Sentries and BlackICE Guards, on all the network computers.

The BlackICE Agents system is scanned on each server, workstations and user's remote terminal and provides protection of both the whole LAN and its units. The BlackICE Agents maintain a wide kit of tools protecting the network. BlackICE Agents are implemented for OS Solaris, Linux and Windows and are compatible with VPN-clients.

BlackICE Guards are aimed at detection and neutralization of network attacks before they reach a result.

BlackICE Sentries provide detection of intrusion on Gigabit- and Fast Ethernet-segments of the network without use of expensive hardware.

With the help of these components the manager collects information on various nonstandard situations in the network, records the network traffic for documenting the process of network activity and for accepting administrative actions. The joint work of the components allows one to detect undesirable events over all the segments of the network.

3.2. The intrusion detection system "Dragon"

Dragon (Enterasys) is a hybrid system that includes Dragon Sensors, Dragon Squire and Dragon Server.

Dragon Sensors system is a real time sensor that works directly with a channel level traffic. In case of the intrusion detection, Dragon Sensors can send an e-mail message to the network manager to organize suppression of the network attack and records in the Log-file for a subsequent analysis.

Dragon Squire is a sensor inspecting the network activity traffic of the network adapter of the server or host. It views Log-files with the purpose of finding a fact of malicious or nonstandard activity of applications. Dragon Squire can also analyze firewall Log-files, processes on routers and other network components that can apply protocol SNMP or provide Syslog.

Dragon Server controls all components Dragon Sensors and Dragon Squire, records nonstandard events in the main database. Dragon Server includes different messages and tools for analysis E-mail, SNMP- or Syslog-messages.

3.3. The intrusion detection Cisco Secure system

Cisco Secure is a system of detecting network attacks by controlling the network traffic. It includes a system of Sensors and Managers.

The Cisco Secure Sensor is a network device used for analysis of enormous sizes of IP-traffic in the network and Syslog-information from Cisco routers. The attacks are translated into significant cases of safety which are transmitted to Cisco Secure to Manager. The sensor can also register data of the Log-file of safety, decrease TCP-sessions and dynamically control the router tables.

The Cisco Secure Manager has a centralized graphic interface to control the distributed network safety. It also controls the traffic with the help of applications of indirect manufacturers, realizes access to the database of the network safety, provides remote control over Sensors, sends e-mails to the system manager. The manager inspects on-line the activity of the Sensors located in the networks with various networking standards.

3.4. The intrusion detection RealSecure system

One of the most highly developing software products is a network safety monitor RealSecure 3.0 produced by the Internet Security Systems company.

RealSecure is a hybrid system consisting of network sensors, OS-sensors and a manager. The network sensors analyze the network traffic for detection of known scripts of attacks, violations in operation of various protocols and repeated attempts of access. The OS-sensors analyze operation of the OS core, view Log-files with the purpose of detecting and preventing an unauthorized activity in a real-time mode.

RealSecure also provides LAN protection from network attacks with the help of an internetwork screen and a router controlling the network traffic filtering rules.

3.5. Tasks of the LAN protection subsystem

The analysis of the existing protection systems shows that the available commercial systems of detecting attacks are not able to provide an effective LAN protection [5]. There is a set of unsolved problems that constrain the intensive development and mass implantation of the systems intended for intrusion detection.

Some of them are as follows:

- From a theoretical viewpoint, only the systems based on the idea of identification of abnormal events ("self - nonself" principle) in LAN can detect new and unknowns types of attacks; unfortunately, in the existing systems the level of failures is too high, an it shifts the main part of operation in the analysis of disputable fragments of network traffic to the network manager and makes application of such systems inefficient;
- The systems of safety of various manufacturers use different protocols of messaging and controlling information, since there are no unified international standards for the network resources protection systems;
- The intrusion detection systems on the basis of high-speed hardware sensors are extremely expensive (a great variety of sensors made to order and with a necessity of configuration of each sensor separately is required);
- The systems on the basis of databases contain a wide set of known attacks, however, it requires their regular modification - organizational measures on inducing upgrade of the bases providing by a wide circle of interested corporations and organizations are needed;
- Many commercial solutions in the field of systems of intrusion detection are aimed at recording the Log-files of the traffic of detected network attacks with the purpose of further analysis, however, the main problem of the systems should be concentrated on protection of intrusion;
- There is a tendency in the development of such systems with a great number of sensors and agents for installation "inside" local networks, however, the high complexity of the connections in global networks, increase in network sizes do underline that the development of the systems operating on the boundaries of networks looks promising [5];
- The commercial systems being completely closed for the users, do not allow one to add the own scripts to struggle against new types of attacks and thus strongly limit their possibilities.

In view of the mentioned above, as a first stage in the development of a subsystem for the LAN protection in the environment of the SAAM "Traffic" we plan

- to create a database with the scripts of behaviour of the network traffic (templates base) for the set of standard attacks described above;
- to develop a system of caching the network traffic with a subsequent analysis on the templates of network attacks;
- to develop the methods of bucking to network attacks in a real-time mode based on the "self - nonself" concept.

Conclusion

In the framework of this paper we have tried to mirror the known scripts of network attacks and to suggest some protection methods based on the SAAM "Traffic". An open subsystem with a stackable base of scripts of network attacks is under development now. First of all, it will play a role of a polygon for improvement of various approaches to the LAN protection. Besides, such a polygon will allow one to study the possibilities of detecting the fact of attack at a channel level, with no attracting for this purpose the data of the network, session and applied levels of the OSI model. This approach should essentially speed up the process of identification of the network attack realized.

At the first step of the development of the LAN protection subsystem, main attention should be focussed on the solving of the following tasks:

- Creation of a templates base with representation of different in nature types of attacks;
- Optimization of the structure of the templates base for fast template search adequate to the script of the expected attack to provide a way for a real time monitoring of the network traffic;
- Development of a simplest structure of the database for its filling by a wide circle of interested experts;
- Development of software for generating simulated network attacks which are included in the templates base; such software is required, in particular, for the development of algorithms of identification of abnormal events at the analysis of the network traffic directly at a channel level;
- Preparation of a detailed description of both the structure of the template base and each template separately; preparation of appropriate descriptions for their publication.

To summing up, it is necessary to underline the following important feature of the approach developed. In spite of the fact that the LAN protection system is installed on a computer - router, i.e. on the boundary between subnetworks, it is not an analogue of the firewall so it does not hinder the operation of distributed network applications. Thus there is a possibility of applying this approach in the GRID-technologies, where the protection on the basis of firewall cannot be used at all.

Acknowledgements

This work has been partly supported by the European Commission in the frame of the International Society Technologies program, the IMCOMP (IST-2000-26016) project.

REFERENCES

[1] Lukatsky A.V.. Detection of attacks. St-Petersburg, 2001

[2] Vasiliyev P.M., Ivanov V.V., Korenkov V.V., Kriukov Yu.A., Kuptsov S.I. System of Acquisition, Analysis and Management of Network Traffic for Segment of the JINR Computer Network - Local Network LAN of the University "Dubna", Communication of the JINR, D11-2001-266, Dubna, 2001.

[3] Medvedovsky I.D., Semyanov P.V., Leonov D.G.. Attack on the Internet. M., 1999.

[4] Corporate technologies of Microsoft Windows NT Server 4.0. Educational course. Transl from English. - Moscow: Publishing Department "Russian Edition" TOO "Channel Nrading Ltd", 1998.

[5] North Atlantic Treaty Organisation, Research and Technology Organisation, RTO Technical Report 49, Intrusion Detection: Generics and State-of-the-Art. Copyright RTO/NATO, 2002.

[6] Web-site materials http: // www.microsoft.com

[7] Web-site materials http: // www.hackzone.ru/

[8] Lukatsky A.V., Adaptive safety of the network. "ComputerPress". No. 8, 1999.

[9] Microsoft Corporation. Microsoft System Management Server 2.0. Educational course: Official manual. "Russian edition", 2000.

[10] Vekhov V.B. Computer crimes: ways of fulfilment and disclosure. Moscow: Right and Law, 1996.

[11] Olifer V.G., Olifer N.A. Computer networks. Concepts, technologies, protocols. "Peter", 1999, 672 p.

[12] Galatenko A.V. Application of methods of the probability theory for the solving of problem of information safety. Problems of cybernetics. Moscow: 1999, RAS, NIISI.

[13] Guiding document. Protection against unauthorized access. Part 1. Software of resources of information protection. Classification on the level of controlling the absence of not declared possibilities. State tech. Committee of Russia, 1999.

[14] Drozhzhyn V.V. Logical resources for analysis of the program systems security. Theses of interregional conference "Information safety of Russia regions", 1999.

[15] Erkhov E. The scripts of attacking banking systems in the Internet. "Analytical banking magazine". No.7, 1998.

[16] Peter Capell. Analysis of Courses in Information Management and Network System Security & Survivability. December 1998. SPECIAL REPORT, CMU/SEI-99-SR-006.

[17] Configuration of the protection system of operation system Windows ® NT 4.0 for using the RealSecure system. Protection of a Windows NT node at the attack detection. Internet Security Systems. Transl. From English by A.V.Lukatsky and Yu.Yu.Tsaplev. March 26, 1998.

Received on December 27, 2002.

Васильев П. М. и др. Д11-2002-292
Основные принципы обеспечения безопасности локальной
компьютерной сети на основе ССАУ «Трафик»

Ранее нами была создана система сбора, анализа и управления сетевым трафиком (ССАУ «Трафик») для сегмента компьютерной сети ОИЯИ. В настоящей работе рассмотрены наиболее известные сценарии сетевых атак и предложены методы борьбы с ними на основе ССАУ «Трафик». Несмотря на то, что система защиты локальной сети устанавливается на компьютере-маршрутизаторе, она не является аналогом «firewall» и не препятствует функционированию распределенных сетевых приложений. В связи с этим появляется возможность применения такого подхода в GRID-технологиях, в которых защита сети на основе «firewall» в принципе не может быть использована.

Работа выполнена в Лаборатории информационных технологий ОИЯИ.

Сообщение Объединенного института ядерных исследований. Дубна, 2002

Vasiliev P. M. et al. D11-2002-292
Main Concept of Local Area Network Protection
on the Basis of the SAAM «Traffic»

In our previous paper we developed a system for acquisition, analysis and management of the network traffic (SAAM «Traffic») for a segment of the JINR local area computer network (JINR LAN). In our present work we consider well-known scenarios of attacks on local area networks and propose protection methods based on the SAAM «Traffic». Although the system for LAN protection is installed on a router computer, it is not analogues to the firewall scheme and, thus, it does not hinder the performance of distributed network applications. This provides a possibility to apply such an approach to GRID-technologies, where network protection on the firewall basis cannot be basically used.

The investigation has been performed at the Laboratory of Information Technologies, JINR.

Communication of the Joint Institute for Nuclear Research. Dubna, 2002

Макет *Т. Е. Попеко*

Подписано в печать 30.01.2003.
Формат 60 × 90/16. Бумага офсетная. Печать офсетная.
Усл. печ. л. 1,93. Уч.-изд. л. 3,16. Тираж 170 экз. Заказ № 53734.

Издательский отдел Объединенного института ядерных исследований
141980, г. Дубна, Московская обл., ул. Жолио-Кюри, 6.
E-mail: publish@pds.jinr.ru
www.jinr.ru/publish/