An Analysis of Security Systems for Electronic Information for Establishing Secure Internet

Muneer Sameer Gheni Mansoor[a], Mohammed Qasim Dhahir[b], Hasanain Abdalridha Abed Alshadoodee[c], [a]Mobile Communications and Computing Engineering, University of Information Technology and Communications, The Iraqi Ministry of Higher Education and Scientific Research, Republic of Iraq, [b]English Language, University of Kufa, The Iraqi Ministry of Higher Education and Scientific Research, Republic of Iraq, [c]Computer Labs in Geographic, University of Kufa, The Iraqi Ministry of Higher Education and Scientific Research, Republic of Iraq, E-mail: muneer.m@uoitc.edu.iq, mohammedq.dhahir@uokufa.edu.iq, hasanain.allawi@uokufa.edu.iq

The modern integrated world is built on billions of web-servers that support the operation of information systems providing various functions from trading operations to e-government support. This set of systems contains not only personal data but financial information that needs to be secured during its storage, transfer and transformation. The transfer of financial flows from the banking sector and introduction of various payment systems and trading operations, which are concluded remotely, has expanded the circle of potential intruders infringing on these objects. Recent years have been marked by an increase in the number of attacks that target web-servers. Crime in this area has become more organized and has shifted from the actions of hackers, affirmed at the expense of such doubtful success to quite meaningful actions of mass password gathering and financial information theft.

Key words: *The Internet, information security, web sites security, virus attacks, network level, information scanning, system level.*

Introduction

Computer system attack is the action taken by the attacker, which consists of the search and use of a particular vulnerability. Thus, an attack is a threat implementation. It is of note, that such interpretation of an attack (involving a person with malicious intent) excludes the element of chance in the definition of threat, but experience has shown that it is often impossible to distinguish between intentional and accidental actions, and a good security system must respond to any of them properly. Researchers usually identify three basic types of security threats which are threats of disclosure, integrity and denial of service. The threat of disclosure is that information becomes known to someone who should not know it. In terms of computer security the threat of disclosure is whenever the access is made to some confidential information stored in a computer system or transferred from one system to another. Sometimes the terms “theft” or “leakage” are used instead of “disclosure”. The threat of integrity is any intentional change (modification or even deletion) of data, stored in computer systems or transferred from one system to another. It is generally believed that government institutions are subject to the threat of disclosure to a greater extent, whereas business and commercial structures are subject to the threat of integrity. The threat of denial of service occurs whenever the access to some resource of the computing system is blocked as a result of some actions. In reality the blocking can be permanent, so that the requested resource is never received, or it can only cause a delay in the requested resource, long enough for it to become useless. In such cases we say that the resource is depleted.

Typical threats in the Internet are (Network component has failed, Information scanning, Inappropriate use of information is the use of information for purposes other than the authorized ones, Unauthorized deletion, Modification, Penetration and Masquerading)
Proceeding from the above, the objective of this work within the field of “Information Security in the Internet” is as follows: To reveal the essence of actions representing real threats in the computer network in order to develop an independent strategy and security tactics that prevent virus attacks.

To achieve the objective the following tasks are considered:

1. To show the systems for detecting virus attacks and their advantages.
2. To set the statistics of virus attacks.
3. To find security methods to prevent remote attacks on the Internet.
4. To develop recommendations on information storage and control on the Internet.

Attack Detection

Historically, the technology used to build systems for detecting attacks has conventionally been divided into two categories: anomaly detection and misuse detection. However, in practice, another classification is used, which takes into account the principles of practical implementation of such systems: network-based detection of attacks and host-based detection of attacks. The former systems analyze the network traffic, while the latter analyze the logs of the operating or application system. Each of the classes has its advantages and disadvantages, but more on that later. It should be noted, that only some systems of attack detection can be unambiguously assigned to one of the named classes. Typically they include the capabilities of several categories. Nevertheless, this classification reflects the key capabilities that distinguish one system of attack detection from another.

At present the technology for anomaly detection is not widely used, and it is not used in any commercially distributed system. This is due to the fact that this technology sounds nice in theory, but it is very difficult to implement in practice. However, there is a gradual return to it (especially in Russia and China), and we can believe that in the near future users will be able to see the first commercial systems of attack detection using this technology. Another approach to detecting attacks is the detection of misuse, which consists in describing an attack in the form of a pattern or signature and searching for this pattern in the controlled space (network traffic or log). Antivirus systems are an excellent example of an attack detection system using this technology.

As noted above, there are two classes of systems, detecting attacks on network and operation levels. The principal advantage of network-based systems of attack detection is in the fact that they identify attacks before they reach the attacked node. These systems are easier to deploy in large networks, because they do not require installation on various platforms used in the company. In in Iraq the most common operation systems are MS-DOS, Windows 95, NetWare and Windows NT. Different dialects of UNIX are not as widespread as abroad. Moreover, network-based attack detection systems practically do not reduce network performance.

Host-based attack detection systems are created for operation under the control of a specific operating system, which imposes certain restrictions on them. For example, we are not familiar with any system of this class, running under MS-DOS or Windows for Workgroups (however, these operating systems are still quite common in Iraq). Using the knowledge of how the operating system should “behave”, the tools built with this approach can sometimes detect intrusions, which are missed by network attack detectors. However, this is often achieved at a high cost, because the constant registration required to perform this kind of detection significantly reduces the performance of the secured host. Such systems heavily load the processor and require large amounts of disk space for storing logs and are not applicable for high-critical systems operating in real time mode (for example, «Operation Bank Day» system or monitoring system).

However, in spite of this, both of these approaches can be used to protect your company. If you want to protect one or more hosts, then host-based attack detection systems can be a good choice. However, if the aim is to protect most of the company's network hosts, then network-based attack detection systems are likely to be the best choice, since the increase in the number of hosts in the network will not affect the level of security achieved with attack detection systems. It will be able to protect additional host without additional configuration, while in the case of the system running at the host level it will be necessary to install and configure it for every protected host. An ideal solution would be an attack detection system combining both of these approaches [1]. The commercial Intrusion Detection Systems, IDS existing on the market use either a network or system approach to detect and repel attacks. In any case these products are searching for ***attack signatures,*** specific templates, which usually indicate hostile or suspicious actions. If these patterns are found in network traffic, the IDS operates at the ***network level.*** If the IDS looks for attack signatures in the operating system or application logs, then it is the ***system level.*** Each approach has its advantages and disadvantages, but they complement each other. The most effective is the intrusion detection system which uses both technologies in its work. This article discusses differences in methods for attack detection at the network and system levels to demonstrate their strengths and weaknesses. There are also options for using each of the methods for the most effective attack detection.

Network-Based Attack Detection

Network-based intrusion detection systems use raw network packets as a source of data for analysis. Typically, network-based IDS use a network adapter, operating in promiscuous mode, and analyzes the traffic in real time as it passes through the network segment. The attack detection module uses four widely known methods to detect attack signatures:

o Traffic matching to a pattern (signature), expression or a bytecode, characterizing an attack or a suspicious action;
o Monitoring the frequency of events or exceeding the threshold value;
o Correlation of several events with low priority;

- Detection of statistical anomalies.

Once an attack is detected, the response module provides a wide range of notification options, issuing an alarm and implementing countermeasures in response to an attack. These options vary from system to system but usually include: notifying the administrator through the console or by an e-mail, ending the connection to the attacking node and/or recording the session for later analysis and collecting evidence.

Advantages of network-based intrusion detection systems

Network-based IDS have a lot of advantages, which are not found in the host-based intrusion detection systems. In fact, many customers use network-based IDS due to its low cost and timely response. The main reasons, which show network-based IDS as an important component of effective implementation of security policy, are given below.

1. ***Low cost of operation.*** Network-based IDS must be installed in the most important locations of the network to control traffic circulating between multiple systems. Network-based systems do not require that the software of intrusion detection systems be installed on every host. Since to monitor the entire network the number of places where IDS is installed is small, the cost of their operation in the company network is lower than the cost of operation of host-based IDS.

2. ***Detection of attacks, which are missed at the system level.*** Network-based IDS learn the headers of network packets for suspicious or hostile activity. Host-based IDS do not work with the headers of packets; therefore, they cannot detect these types of attacks. For example, many "denial-of-service" and TearDrop network attacks can only be identified by analyzing packet headers as they pass through the network. This type of attacks can be quickly identified by a network-based IDS, which looks at traffic in real time. Network-based IDS can examine the content of the packet data by searching for commands or a specific syntax used in specific attacks. For example, when a hacker is trying to use the Back Orifice on systems, which are not affected by it, then this fact can be detected by examining the contents of the packet data body. As mentioned above, host-based systems do not work at the network level, and therefore are not able to detect such attacks.

3. ***It is more difficult for a hacker to remove the traces of his presence.*** Network-based IDS use "live" traffic when real-time attacks are detected. Thus, a hacker cannot remove the traces of his presence. Analyzed data include not only information about the attack method but also information which can help to identify the attacker and to prove in a court. Since many hackers are familiar with logs, they know how to manipulate these files to hide their traces reducing the efficiency of the system-level systems, which require this information to detect attacks.

4. ***Real time detection and response.*** Network-based IDS detect suspicious and hostile attacks AS FAST AS THEY HAPPEN, and so provide much faster notification and response than IDS of a system-level. For example, a hacker initiating a denial-of-service network attack based on TCP protocol can be stopped by a network-based IDS, sending the set reset flag in the header of TCP-packet to terminate the connection with the attacking host before the attack causes damage to the attacked node. As a rule, host-

based IDS do not detect attacks until the corresponding log entry and take response actions after the record has been made. By this time the most important systems or resources can already be compromised or the performance of the system, which runs host-based IDS, can be disrupted. The real time notification helps to quickly respond in accordance with predefined parameters. The range of these reactions varies from penetration permission in the surveillance mode in order to gather information about the attack and an attacker before the immediate end of the attack.

5. ***Detection of failed attacks or suspicious intentions.*** A network-based IDS installed on the outside of the firewall can detect attacks targeting resources beyond the firewall even though firewall may reflect these attempts. System-level systems do not see repelled attacks which do not reach the host behind the firewall. This lost information can be the most important in assessing and improving the security policy.

6. ***Independence from the OS.*** Network-based IDS do not depend on the operating systems installed in the corporate network. Host-based IDS require specific operating systems to function properly and generate the required results.

Advantages of host-based intrusion detection systems

And while system-level intrusion detection systems are not as fast as their network-based counterparts, they offer advantages that the latter do not. These advantages include more rigorous analysis, close attention to event data on a particular host and lower implementation costs.

1. ***Confirm the success or failure of the attack.*** As host-based IDS use logs with information about events that actually took place, then the IDS of this class may determine whether the attack was successful or not with high accuracy. In this respect the host-based IDS provide an excellent complement to network-based intrusion detection systems. This combination provides early warning with the network component and the “success” of the attack using the system component.

2. ***It controls the activity of a specific node.*** The host-based IDS monitor user activity, file access, changes in file permission, attempts to install new programs and/or attempts to access privileged services. For example, host-based IDS may control all logon- and logoff-activity of the user, as well as the actions, that every user performs when connecting the network. For a network-based system it is very difficult to provide such a level of specification of events. The technology for detecting attacks on a system level may also monitor activities that are usually conducted by the administrator. Operating systems record any event, which adds, deletes and changes user accounts. Host-based

IDS are able to detect the corresponding changes as soon as they happen. IDS of a system level can also audit changes in security policy, which affect how systems monitor in their logs, etc.

3. ***Detection of attacks which are missed by network-based systems.*** IDS of a system-level can detect attacks which cannot be detected by network-based systems. For example, attacks made from the target server cannot be detected by network-based intrusion detection systems.

4. ***Well suited for networks with encryption and switching.*** As a host-based IDS is installed on different hosts of the company network, it may overcome some problems at the operation of network-based systems in the networks with encryption and switching. Switching helps to manage large-scale networks and several small network segments. As a result it is difficult to determine the best place to install a network-based IDS. Sometimes managed ports and mirror ports, span ports can be helpful on the switches but these methods are not always applicable. Attack detection at the system level provide more efficient operation in switched networks, as it helps to place IDS only on the nodes which need it. Certain encryption types also present problems for network-based intrusion detection systems. Depending on where encryption is performed (channel or subscriber), a network-based IDS may remain “blind” to certain attacks. Host-based IDS do not have this limitation. Moreover the OS, and, hence, a host-based IDS analyzes the decrypted incoming traffic.

5. ***Detection and response in near real time.*** Although the detection of attacks on the system level does not provide a response in real-time, it can be implemented in near real-time if implemented properly. Unlike legacy systems which check the status and the contents of the logs at predefined intervals, many modern host-based IDS get an OS interrupt once a new entry in the log appears. This new record can be processed immediately, greatly reducing the time between attack detection and response to it. There is a delay between the time the operating system records the event to the log and the time it was detected by intrusion detection system, but in many cases the attacker can be detected and stopped before doing any damage.

6. ***Do not require additional hardware.*** Host-based intrusion detection systems are installed on the existing network infrastructure, including file servers, Web-servers and other resources used. This capability can make a host-based IDS very cost effective, because they do not require another node on the network that needs attention, maintenance and monitoring.

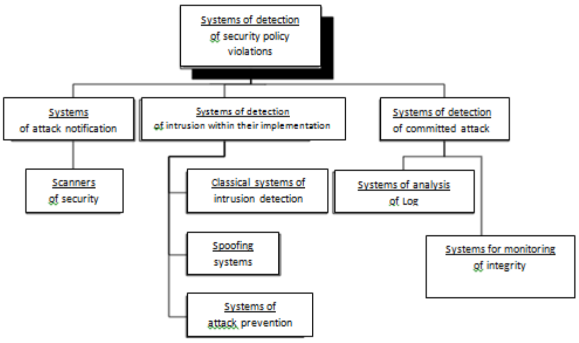
7. ***Low cost.*** Despite the fact that network-based intrusion detection systems provide traffic analysis of the entire network, very often they are quite expensive. The cost of

one system for detecting attacks may exceed $10,000. On the other hand, host-based intrusion detection systems cost hundreds of dollars for one agent and can be purchased by a customer if it is necessary to control only some of the nodes of the company without monitoring network attacks.

The need for both network-based and host-based intrusion detection systems

Both solutions: network-based and host-based IDS have their advantages and strengths, which effectively complement each other. Thus, the next generation of IDS should include integrated system and network components. Combination of these two technologies will greatly improve the network's reluctance to attacks and abuse, help to toughen the security policy and improve flexibility in the operation of network resources. The figure below demonstrates how the methods of network-based and host-based attack detection interact when creating a more efficient system of network protection. Some events are detected only with network systems. Other events are detected only with the system ones. Some require the use of both types for reliable attack detection.

Fig.1. Interaction of methods for network-based and host-based attack detection


Systems of detection of security policy violations
Systems of attack notification
Systems of detection of intrusion within their implementation
Systems of detection of committed attack
Scanners of security
Classical systems of intrusion detection
Systems of analysis of Log
Spoofing systems
Systems for monitoring of integrity
Systems of attack prevention

The Whole World Is Full With Attacks

Two strategies can be applied to protect against various attacks. The first strategy is to acquire the most praised (though not always the best) systems of protection against various types of attacks. This method is very simple but requires a huge amount of money. No home user or even the head of the company will do it. Therefore, the second strategy is usually used, which consists of preliminary analysis of possible threats and the subsequent choice of means of protection against them [2].

Threat analysis or risk analysis is also made via two methods. A complex but more effective method is that before choosing the most likely threats, the analysis of the information system, information processed in it, hardware and software used are analyzed. This will significantly reduce the range of potential attacks and, thus, increase the efficiency of investing money in the acquired means of protection. However, such an analysis takes time, money and, most importantly, high qualification of specialists, who conduct an inventory of the analyzed network. Few companies, except home users, can afford to go this way. Choice of means of protection is made based on the so-called standard threats, that is, those that are most widespread. In spite of the fact that some of the threats inherent in the protected system can be ignored, most of them will fall into the outlined framework. This article is devoted to discovering the most common types of threats and attacks. For the data to be more accurate, statistics used are obtained from various sources.

Who most often commits computer crimes and various attacks? Which are the most common threats? The data obtained by the most authoritative source in this field — Computer Security Institute (CSI) is used with regard to the group of computer attacks identified by the FBI office in San Francisco. This data were published in March 2000 in the annual report “2000 CSI/FBI Computer Crime and Security Survey”. According to the data 90% of respondents (large corporations and state organizations) recorded various attacks on their information resources; 70% of respondents recorded serious violations of security policy, for example, viruses, “denial of service” attacks, abuse by employees, etc.; and 74% of respondents suffered considerable financial losses due to these violations.

In recent years the volume of losses due to violations in security policy has been also increased. If in 1997 the amount of losses was 100 million dollars, in 1999 - 124 million dollars, then in 2000 this figure increased to 266 million dollars. The size of losses from denial of service attacks reached 8.2 million dollars. Other interesting data include sources of attacks, types of common attacks and the amounts of losses from them. Another authoritative source, the CERT coordination center, also confirms these data. Moreover, according to the data obtained by them, the increase in the number of security incidents coincides with the spread of the Internet.

The attention to e-commerce will help to strengthen this growth in subsequent years. There is another tendency. In the 80s through to the beginning of the 90s, external attackers attacked the Internet nodes out of curiosity or to demonstrate their skills. Now the attacks more often pursue financial or political goals. According to many analysts the number of successful intrusions to information systems doubled in 1999 compared to the previous year (from 12 to 23%) and in 2000 through 2001 this tendency continued, there are no statistics for cybercrime in Iraq.

How Can We Protect From Remote Attacks In The Internet?

At present the peculiarity of the Internet is that 99% of information resources of the network are public. Remote access to these resources can be made anonymously by any unauthorized network user. An example of such unauthorized access to public resources is the connection to

WWW- or FTP-servers, provided such access is allowed. In determining which Internet resources a user intends to access, it is necessary to answer the following question: is the user going to allow remote access from the network to his resources? If not, then it makes sense to use a "pure client" OS a network OS (for example, Windows'95 or NT Workstation), which does not contain remote server software, and, therefore, remote access to this system *is basically impossible*, as it does not provide software (for example, OC Windows'95 or NT, but it is true for: under the data of the system there are no FTP, TELNET, WWW servers, but it is crucial not to forget the built-in ability to provide remote access to the file system, the so-called *share* of resources. And remembering the strange position of Microsoft company, with respect to the security of its systems, much deliberation is necessary before choosing the products of this company. As a final example: on the Internet there is a program which provides the attacker unauthorized remote access to the file system of OS Windows NT 4.0!). The choice of the client operating system solves the problems of security for this user (you cannot access the resource which simply does not exist!). However, in this case the functionality of the system is degraded. It is timely to formulate the basic security axiom:

Security axiom. The principles of accessibility, convenience, speed and functionality of the computing system are antagonistic to the principles of its security.

Basically this axiom is obvious: the more accessible, convenient, faster and multifunctional computer system, the less secure it is. There are many examples. For example, the DNS service: it is convenient but insecure. The user's choice of the client network OS is one of the most sensible steps leading to the network policy of isolationism. This network policy of security is to implement as complete isolation of its computing system from the outside world as possible. Also this is one of the steps to secure this policy is the use of Firewall systems, which helps to create a dedicated secured segment (for example, a private network), separated from the global network. By all means, there is nothing to stop this policy of network isolationism to the point of absurdity by simply pulingl out the network cable (complete isolation from the world!) which ultimately is the solution of all the problems with remote attacks and network security (due to complete absence of them).

Now, let the user of the Internet decide to use only the client network OS to access the network and use unauthorized access with it. Are the problems with security solved? There are not! It would be a good thing if it was not so bad. For the "Denial of service" attack it does not matter what type of access is used by the user and the type of the network OS are (though the client OS is preferable from the viewpoint of protection from attacks). This attack using fundamental gaps in the security of protocols and infrastructure of the Internet hits the network OS on the user's host with one single goal that is to disrupt its performance. For an attack connected with the imposition of a false route with the help of ICMP protocol, which aims at denial of service, OS Windows'95 and Windows NT are the most desirable targets. In this case the user is left to hope that his modest host does not present any interest for the attacker, who can disrupt its performance for the desire to simply play mean tricks.

Administrative methods of security against remote attacks in the Internet

The most correct step in this area is to ask an information security specialist to solve the entire complex of tasks together with you to ensure the required level of security for your distributed computing system. This is a rather complex integrated problem for the solution of which it is necessary to determine, what (the list of controlled objects and resources of CS), from what (analysis of the possible threats for CS) and how (developing requirements, defining a security policy and administrative and hardware software measures to ensure the developed security policy in practice) to secure. Administrative methods of security against information-destroying actions are perhaps the most simple and cheapest ones.

How can we protect from network traffic analysis?

There is an attack which helps the hacker to listen to any information exchanged by remote users using software listening of the message channel, if only unencrypted messages are transmitted on the channel. It can also be shown, that basic application protocols of the remote access TELNET and FTP do not provide for elementary cryptographic protection of even identifiers (names) and authenticators (passwords) of users. Therefore, network administrators can be advised not to allow the use of these basic protocols to provide remote *authorized* access to the resources of the systems and consider the analysis of the network traffic to be a constantly present threat which is impossible to be eliminated, but it can be made meaningless using strong crypto-algorithms to secure IP-flow.

How to protect against a false ARP-server

In the case if the network OS does not have information on the correspondence between IP- and Ethernet-addresses of hosts within the same segment of the IP-network, this protocol helps to send an ARP broadcast request to find the necessary Ethernet-address, to which the attacker can send a false response and in the future all traffic will be intercepted by the attacker at the data link level and will pass through a false ARP-server. It is obvious, that to eliminate this attack it is necessary to eliminate the reason why it is possible to implement it. The main reason for the success of this remote attack is the absence of the necessary information from the OS of every host on the corresponding IP- and Ethernet-addresses of all other hosts within this segment of the network. Thus, the simplest solution is the creation of the static ARP-table in the form of a file by a network administrator (it is usually /etc/ethers on OS UNIX), where it is necessary to enter the corresponding information on addresses. This file is installed on every host within a segment and, therefore, the network OS does not need to use the remote ARP-search.

How to protect against a false DNS-server

Using the Internet DNS service in its current form may allow a cracker to gain global control over the connections by imposing a false route through the host of the cracker – a false DNS-server. The implementation of this remote attack based on potential DNS vulnerabilities may lead to disastrous consequences for a great number of the Internet users and become a reason of mass destruction of information security of this global network. The following two paragraphs give possible administrative methods to prevent or hinder this remote attack for administrators and users of the network as well as for administrators of DNS-servers.

How can a network administrator be secured from a false DNS-server?

If you answer this question briefly then the answer is he cannot. Neither administratively nor from SW base can one can be secured from the attack on the existing version of DNS service. The best solution from the security viewpoint is to refuse using DNS service in your protected segment at all! By all means, it is very uncomfortable to completely refuse using names when accessing hosts for users. Therefore, we can offer the following compromise solution: to use names, but to abandon the mechanism of the remote DNS-search. You have guessed right that this is the return to the scheme used before the appearance of DNS service with dedicated DNS-servers. Then on every machine in the network there was a *hosts* file, which contained information on the corresponding names and IP-addresses of all hosts in the network. It is obvious, that at present an administrator can make information on the frequently visited servers of the network by the users of this segment in the file. Therefore, the use of this solution is extremely difficult in practice and, apparently, unrealistic (for example, what can be done with browsers which use URL with names?). To make it difficult to implement this remote attack we can ask administrators to use TCP protocol instead of the default UDP protocol for DNS service (though it is not clear how to change it from the documentation). This makes it much difficult for an attacker to transfer a false DNS response to the host without receiving a DNS request.

The general disappointing conclusion is that: on the Internet when using the *existing* version of the DNS service *there is no* acceptable solution for protecting against a false DNS-server (you will not refuse as in the case of ARP, but to use it insecure)!

How can a DNS-server administrator be secured from a false DNS-server?

If you answer this question briefly then the answer is he cannot. The only way to complicate the implementation of this remote attack is to use TCP protocol but not UDP to communicate with hosts and other DNS-servers. Nevertheless, this only makes it difficult to perform the attack- do not forget about the possible interception of DNS-query, and about the possibility of mathematical prediction of the initial value of the TCP-identifier ISN.

In conclusion we can recommend for the entire Internet to quickly move to either new or more secure versions of DNS service or to adopt a single standard for a secure protocol. To make this transition despite enormous costs is a necessity, otherwise the Internet can simply be brought to its knees before the ever-growing successful attempts to violate its security with the help of this service!

Hardware and software security methods from the remote attacks in the Internet

The hardware and software means for information security of communication equipment in computer networks are:

- hardware encoders of network traffic;
- Firewall technique, implemented on the basis of software and hardware;
- secure network cryptographic protocols;
- software-hardware analyzers of network traffic; and
- secure network OS.

There are a huge number of references devoted to these security means intended for use on the Internet (for the past two years almost every issue of any computer magazine has an article on this topic). Further, if possible briefly not to repeat the well-known information we will describe these security means used on the Internet. At the same time we pursue the following objectives: firstly, we will return once again to the myth of the “absolute security” which the Firewall systems supposedly provide, evidently thanks to the efforts of their sellers; secondly, we will compare the existing versions of cryptographic protocols used on the Internet, and, in fact, give an estimate to the *critical* situation in this area; and, thirdly, we will introduce to the readers the possibility of security with the help network security monitoring, designed to perform dynamic control of the situations that appear in the protected segment of the IP-network, indicating the implementation of one of the remote attacks described in Chapter 4.

The Firewall method as the main hardware and software solution of a network security policy in a dedicated IP network segment

In general the Firewall method performs the following three main functions:

Multilevel filtering of network traffic.

Filtering is usually performed on three levels of OSI:
network (IP);
transport (TCP, UDP);
application (FTP, TELNET, HTTP, SMTP, etc.).
Network traffic filtering is the main function of the Firewall system, it helps the network security administrator to centrally implement the necessary network security policy in a dedicated IP network segment, that is, by configuring the Firewall appropriately, we can allow or deny user access from the external network to the corresponding host services or to host located in the protected segment, and access of users from the internal network to the corresponding resources of the external network. It is possible to draw an analogy with the administrator of the local OS, who on order to implement security policy in the system, appropriately assigns the relationships between subjects (users) and objects of the system (for example, files), which helps to distinguish access of system subjects to their objects in accordance with the access rights given by the administrator. The same reasoning is applied to the Firewall-filtering: the IP addresses of the user hosts will act as subjects of interaction, and the IP addresses of hosts, transport protocols and remote access services are used as objects to be distinguished.

We have proposed a security tree for data security using Trusted Third Party (TTP). A TTP is a government or reputed organizations which ensures complete security of the entire cycle. A TTP develops, updates and audits security services for clients but there is no direct contact with user data. An exciting feature of TTP is its binary tree structure in which all of the security features are represented by nodes.

Proxy-scheme with additional identification and authentication of users on the Firewall-host.

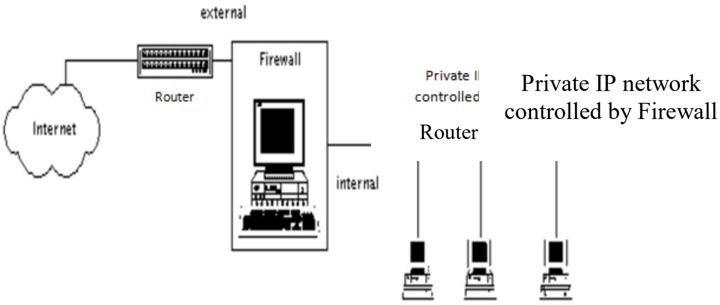
Firstly, proxy-scheme helps to perform additional identification and authentication of the remote user when accessing a protected Firewall network segment, secondly it is a basis of creation of private networks with virtual IP-addresses. The meaning of the proxy-scheme is to create a connection with the final destination through an intermediate proxy-server (proxy – “authorized”, Eng.) on the Firewall host. On this proxy-server additional subscriber identification can be performed.

Creation of Private Virtual Network – PVN with “virtual” IP-addresses (NAT - Network Address Translation).

In case the network security administrator considers it appropriate to hide the true topology of the internal IP-network, he can be recommended using the Firewall systems to create a private network (PVN). Hosts in the PVN are any “virtual” IP-addresses. For addressing to an external network (through Firewall) it is necessary either to use above-mentioned proxy-servers on the Firewall host, or to use special systems of routing, through which external addressing is possible. This is due to the fact that the virtual IP-address used in the internal PVN-network is obviously not suitable for external addressing (external addressing is an addressing to the subscribers outside the PVN network). Therefore, a proxy-server or a routing tool must communicate with subscribers from an external network from its real IP-address. Moreover, this scheme is convenient if you have not enough IP addresses to create IP-network (in the IPv4 standard this happens very often, therefore to create a full-fledged IP-network with the use of a proxy-scheme you need only one dedicated IP-address for a proxy-server).

So, any device which implements at least one of these functions of the Firewall-technique is a Firewall-device. For example, nothing prevents you from using a computer with an ordinary OS FreeBSD or Linux as a Firewall-host, which must properly compile the kernel of the OS. A firewall of this type will provide multilevel filtering of IP-traffic. Another thing, the powerful Firewall-complexes on the market, made on the basis of computers or mini-computers usually implement all the functions of the Firewall-technique and are full-featured Firewall systems. The following figure shows a network segment separated from the external network by a fully-functional Firewall-host.

Fig. 2. A generalized scheme for a fully-functional Firewall host.



However, IP network administrators, yielding to the advertising of the Firewall system, should not be mistaken in that the Firewall is a guarantee of complete security from remote attacks on the Internet. A Firewall is not so much a security tool as an ability to centrally implement a network policy to differentiate remote access to the available resources of your network. No doubt, in case if remote TELNET-access is prohibited to this host, the Firewall will definitely prevent the possibility of this access. The fact is that the most remote attacks have completely different purposes (it’s pointless to try to get a certain type of access if it is prohibited by the Firewall system).

Which of the considered remote attacks can a Firewall prevent? Is it an analysis of network traffic? Obviously it is not! Is it false ARP-server? Yes and no (for security it is not necessary to use a Firewall). Is it a false DNS-server? Unfortunately, it's not. Firewall does not help you here. Is it imposing a false route using an ICMP protocol? Yes, this attack of a Firewall will easily reflect by filtering ICMP-messages (although a filtering router will be enough, for example Cisco). Is it a substitution of one of the subjects of TCP-connection? The answer is negative; Firewall has absolutely nothing to do with it. Is it disruption of the host by creating a direct storm of false requests or request overflow? In this case the use of a Firewall will only worsen the whole thing. In order to disable (cut off from the outside world) all hosts inside a segment protected by the Firewall system an attacker needs to attack only one Firewall, not several hosts (it is easily explained by the fact that the connection of internal hosts to the outside world is possible only through the Firewall).

From all the above mentioned it does not follow that the use of the Firewall systems is completely meaningless. However, at this time there is no alternative to this technique and its main purpose must be clearly understand and remembered. It seems to us that the use of the Firewall technique to ensure network security is a necessary but *not sufficient* condition and we must not consider that having installed the Firewall we will have solved the problems with network security and deleted all possible remote attacks from the Internet. Dying, from the security point of view the Internet network, cannot be prevented by any single Firewall!

Software security methods used on the Internet

Software security methods on the Internet are primarily security cryptographic protocols, with the use of which there is a possibility of reliable protection of the connection. In the next section we will speak on current approaches in the Internet and main already developed cryptographic protocols. Another class of software security methods which prevent remote attacks are programs, the main purpose of which is to analyze network traffic for the presence of one of the known active remote effects.

SKIP-technology and SSL, S-HTTP cryptographic protocols as the primary means of connection and transmitted data security on the Internet

One of the main reasons for the success of remote attacks on distributes CS is the use of network communication protocols, which cannot identify remote objects reliably, protect the connection and the data transferred. Therefore, it is quite natural that in the process of Internet functioning various secure network protocols have been created using cryptography both with private and public keys. Traditional cryptography with symmetric cryptographic algorithms assumes that the transmitting and receiving sides have symmetric (identical) keys for encrypting and decrypting messages. These keys are supposed to be distributed in advance between a finite number of subscribers which in cryptography is called the standard problem of static key distribution. It is obvious, that the use of traditional cryptography with symmetric keys is possible only on a limited set of objects. In the Internet for all its users to solve the problem of static key distribution is not possible. However, Kerberos protocol was one of the first secure exchange protocols on the Internet, it was based on static key distribution for a finite number of subscribers. Using traditional symmetric cryptography our special services are forced to go this way, they develop their secure cryptographic protocols for the Internet. This is due to the fact, that for some reason there is still no guest cryptographic algorithm with a public key. Everywhere in the world such standards of encryption have long been accepted and certified, and we are apparently going another way!

So, it is clear that in order to protect all the Internet users and not a limited subset of them it is necessary to use dynamically generated keys in the process of creating a virtual connection when using public key cryptography. Next we will consider the current approaches and protocols ensuring security for the connection. **SKIP** (Secure Key Internet Protocol) technology is the IP-packet encapsulation standard which helps to ensure security of the connection and transmitted data in the existing network-based standard IPv4. It is achieved in the following way: SKIP-packet is a typical IP-packet, data field of which is a SKIP-header defined by a format specification and a cryptogram (encrypted data). This structure of a SKIP-packet helps to easily route it to any host on the Internet (the internetworking takes place via the usual IP-header in the SKIP-packet). According to the predetermined algorithm by the developers the final recipient of the SKIP-packet decrypts the cryptogram and forms a typical TCP- or UDP-packet, which transmits to the corresponding conventional module (TCP or UDP) the kernel of the operating system. In principle, nothing prevents the developer from forming his original header different from a SKIP-header according to this scheme.

S-HTTP (Secure HTTP) is the secure HTTP-protocol developed by Enterprise Integration Technologies (EIT) specifically for the Web. S-HTTP protocol helps to ensure reliable crypto-security only for HTTP-documents of the Web-server and operates on the application layer of the OSI model. This feature of the S-HTTP protocol makes it an absolutely specialized means of connection security and, hence, impossible application for the security of all other application protocols (FTP, TELNET, SMTP, etc). Moreover, none of the current basic Web-browsers (neither Netscape Navigator 3.0, nor Microsoft Explorer 3.0) support this protocol.

SSL (Secure Socket Layer) is the development of the Netscape Company, a universal protocol of the connection security, operating at the OSI session level. In our viewpoint nowadays this protocol, using cryptography with a public key is the only universal means helping to dynamically secure any connection with the use of any application protocol (DNS, FTP, TELNET, SMTP, etc.). It is connected with the fact that SSL, unlike S-HTTP, operates at the intermediate OSI session level (between transport - TCP, UDP, - and application - FTP, TELNET, etc.). At the same time, the process of creation of virtual SSL-connection is carried out according to Diffie-Hellman scheme (section 6.2), which helps to develop a crypto-resistant session key used by subscribers of the SSL-connection for encryption of the transmitted messages. Today SSL protocol is practically formed as an official standard of security of HTTP connection, that is, for the security of Web-servers. It is maintained by Netscape Navigator 3.0 and oddly enough by Microsoft Explorer 3.0 (remember the fierce conflict between the browsers of Netscape and Microsoft). By all means, to establish SSL-connection with the Web-server it is necessary to have the Web-server, which supports SSL. Such versions of the Web-servers have already existed (for example, SSL-Apache).

In conclusion SSL protocol, until recently, the US laws prohibited the export of the cryptosystems with a key length of more than 40 bits (it has been increase up to 56 bits). Therefore, existing versions of browsers use 40-bits keys. Experimentally cryptoanalysts found out that in the existing version of the SSL protocol encryption using 40-bits key is not a reliable protection for the transmitted messages because by simply combining (2^{40} combinations) this key is selected in time from 1.5 (on a supercomputer Silicon Graphics) up to 7 days (120 workstations and several minicomputers were used during calculation). It is obvious that the widespread use of these security exchange protocols, especially SSL (with a key length of more than 40 bits), will put a reliable shield to all sorts of remote attacks and seriously complicate the life of crackers from all over the world. *However, all the tragedy of today's security situation on the Internet is that none of the existing cryptographic protocols (there are a lot of them) has been formed as a single standard of connection security so far, which would be supported by all manufacturers of the network OS OC!*

The SSL protocol, available today, suits perfectly. If it were supported by all network OS, it would not be necessary to create specific application SSL-compatible servers (DNS, FTP, TELNET, WWW, etc.). If we do not agree on the adoption of a single standard for a secure session-level protocol, then many standards for protection of each individual application service will be required. For example, an experimental Secure DNS protocol, which is not supported by anyone, has already been developed. Moreover, there are experimental SSL-compatible Secure FTP- and TELNET-servers. However without a single standard for a secure protocol supported by all manufacturers all this does not make any sense at all. Today the manufacturers of the network OS cannot agree on a single view on this topic and, thus, shift the solution of these problems directly to Internet users and suggest them solving ***their*** problems with information security in the way they want!

Security network monitor IP Alert-1

Practical and theoretical research of the authors in the area connected with the analysis of the security of distributed CS, including the Internet (two polar research directions: violation and ensuring information security), has brought an idea: on the Internet, as in other networks (for example, Novell NetWare, Windows NT), there is a serious shortage of security software, performing ***integrated*** control (monitoring) at the link level over the entire flow of information transmitted over the network to detect all types of remote actions described in chapter 4. The research of the Internet security software market has revealed the fact that we do not have such integrated remote attack detection tools, and those that are available are designed to detect an attack of one particular type (for example, ICMP Redirect or ARP). Therefore, the development of a control tool for the segment of an IP-network, intended for the use on the Internet has been started and it is named security network monitor **IP Alert-1**. The main task of this tool, which analyzes software network traffic in the transmission channel, is not to reflect remote attacks on the communication channel but to detect them, and log (maintaining an audit file with logging in a form convenient for subsequent visual analysis of all events related to remote attacks on this segment of the network) and promptly signaling to the security administrator if a remote attack is detected. *The main task of* security network monitor **IP Alert-1** is *to monitor* the security of the corresponding segment of the Internet.

Security network monitor **IP Alert-1** has the following functionality and helps to detect remote attacks to the controlled segment of the Internet using network analysis.

Functionality of security network monitor IP Alert-1

1. ***Monitoring of the correspondence of IP- and Ethernet-addresses in packets transmitted by hosts within the monitored network segment.***

On the IP Alert-1 host the security administrator create a static ARP-table, which records information on the corresponding IP- and Ethernet-addresses of hosts within the monitored network segment. This function helps to detect an unauthorized change of IP-address or its spoofing (IP Spoofing).

2. *Monitoring of the correct use of the mechanism of remote ARP-search.*
This function helps to detect a remote attack “False ARP server” using a static ARP-table.
3. *Monitoring of the correct use of the mechanism of remote DNS-search.*
This function helps to detect all possible types of remote attacks on the DNS service.
4. *Monitoring of the presence of ICMP Redirect messages.*
This function notifies about the detection of ICMP Redirect messages and a corresponding remote attack.
5. *Monitoring of the correct remote connection attempts by analyzing the transmitted requests.*

Firstly, this function helps to detect an attempt to investigate the law of changing the initial value of TCP-connection identifier - ISN, secondly, a remote attack “denial of service” by overflowing the connection requests, and, thirdly, a “storm” of false connection requests (both TCP and UDP), leading to a denial of service.

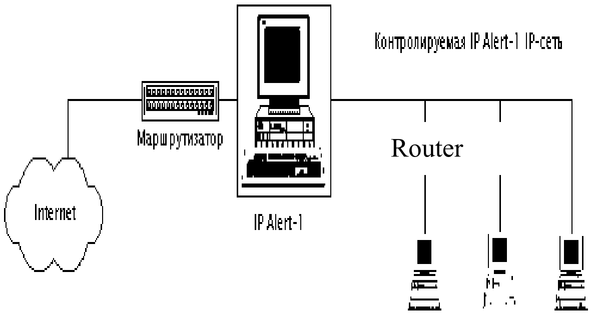
Thus, security network monitor **IP Alert-1** helps to detect, notify and record all types of remote attacks described in chapter 4! However, this program is not a competitor to the Firewall systems. Using described and systematized in chapter 4 features of remote attacks on the Internet **IP Alert-1** is a necessary addition, which is cheaper, to the Firewall systems. Without a security monitor most attempts to implement remote attacks on your network segment will remain hidden from your eyes.

None of the firewalls known to the authors are engaged in this kind of intelligent analysis of messages passing through the network for the detection of various types of remote attacks, limited to logging which records information on the attempts to select passwords to TELNET and FTP, port scanning and network scanning using the famous remote search program of known vulnerabilities of the network OS - SATAN.

Therefore, if an IP-network administrator does not want to remain indifferent and be satisfied with the role of an ordinary observer of remote attacks on his network, then it is desirable to use a security network monitor **IP Alert-1**. By the way we will recall that Tsutomu Shimomura was able to record an attack by Kevin Mitnick, apparently, thanks to tcpdump program- the simplest analyzer of IP-traffic.

IP network controlled by IP Alert-1

Fig. 3. Security network monitor IP Alert-1.



Conclusion

There are many users who are interested in the Internet as a system with categorized information and authority of users subject to the established security policy. However, after a while the most vivid creations of the human mind begin to live independent life developing and going beyond the initial intentions of the creators. Therefore, the weak security of the network has become a problem to its users over time. In our opinion there should not be information on the web, the disclosure of which will lead to serious consequences. On the contrary, it is necessary to post information on the web, distribution of which is desirable to its owner. It is always necessary to take into account the fact that at any time this information can be intercepted, distorted or may become unavailable. Therefore, it should not be about the security of the Internet but about ensuring sufficiency of information security of the Web.

By all means, this does not negate the need to familiarize users with a rich and constantly growing range of software and hardware to ensure information security of the network. Nevertheless, we note that they are not able to turn the Internet into a protected environment which would mean a change in its nature. Is the Internet secure? The development of the Internet security can be in conflict with its purpose and distort the very idea of the Network. It is more legitimate to raise a question of the creation of the world specialized security information sphere, designed to manage global production, transport, geopolitics. The progress seems to lead to the necessity of creation such a unified system. This communication environment will have security architecture and guarantee the integrity and confidentiality of information. It is obvious that the designers of this system should ensure compliance with political and economic interests of world's subjects, since the multiple ownership of this system means control over the world.

It is clear that the Internet in today's form cannot be such an environment. In our opinion the main thing is to resist to the desire to bring the present Internet closer to such a world control environment. The Internet is good in the form in which it is. What is the perspective of information system security in the era of integration of the information processing environment? In our opinion the way out of this situation is through a clear delineation of information that is of vital interest to the subjects (users) and the creation of specialized systems of its processing. Such systems should be able to integrate into the global network while ensuring their unilateral information isolation.

REFERENCES

1. Ahmed, U., Zin, M. L. M., & Majid, A. H. A. (2016). Impact of Intention and Technology Awareness on Transport Industry's E-service: Evidence from an Emerging Economy. *산경연구논집 (IJIDB)*, *7*(3), 13-18.
2. A.V. Babash. Information Security. Laboratory Course: a Textbook / A.V. Babash, E.K. Baranova, Y.N. Melnikov. — M.: KnoRus, 2013. — 136 p.
3. V.V. Gafner. Information Security: a Textbook / V.V. Gafner. — Rostov-on-Don: Fenix, 2010. — 324 p.
4. Y.Y. Gromov. Information Security and Information Protection: a Textbook / Y.Y. Gromov, V.O. Drachev, O.G. Ivanova. — Stary Oskol: TNT, 2010. — 384 p.

5. L.L. Efimova. Information Security of Children. Russian and Foreign Experience: Monograph / L.L. Efimova, S.A. Kocherga… — M.: UNITY-DANA, 2013. — 239 p.
6. L.L. Efimova. Information Security of Children. Russian and Foreign Experience. Monograph. Code of training center “Professional Textbook”. Code of R&D Institute of Education and Science. / L.L. Efimova, S.A. Kocherga. — M.: UNITY, 2013. — 239 p.
7. S.V. Zapechnikov. Information Security of Open Systems. In 2 vol. Vol.1 — Threats, Vulnerabilities, Attacks and Approaches to Security / S.V. Zapechnikov, N.G. Miloslavskaya. — M.: GLT, 2006. — 536 p.
8. S.V. Zapechnikov. Information Security of Open Systems. In 2 vol. Vol.2 — Security Means in Networks / S.V. Zapechnikov, N.G. Miloslavskaya, A.I. Tolstoy, D.V. Ushakov. — M.: GLT, 2008. — 558 p.
9. Chris Mitchell. Artyom Konev. Web-sites Security. // Australia: SophosLabs. [E-source]. URL: http://help.yandex.ru/webmaster/protecting-sites/contents.xml
10. S.N. Smirnov. Database System Security – M.: Gelios ARV, 2007.-352p., ill.
11. A.A. Biryukov. Information Security: Defense and Attack – M.:DMK Press, 2012.-474.: ill.
12. K.S. Sumkin, I.A. Ivanova, V.V. Nikonov, I.V. Terekhin. Fuzzy Hybrid Systems in the Tasks of Security, Analysis and Control of Access Rights Differentiation in Computer Networks// Topical Issues of the Humanities and Natural Science. 2014. No.6-1. P. 145-150.
13. A.A. Mayuk. Information Security: Conceptual and Methodological Basis of Information Security / A.A. Malyuk. — M.: GLT, 2004. — 280 p.
14. T.L. Partyka. Information Security: a Textbook / T.L. Partyka, I.I. Poppov. — M.: Forum, 2012. — 432 p.
15. S.V. Petrov. Information Security: a Textbook / S.V. Petrov, I.P. Slinkova, V.V. Gafner. — M.: ARTA, 2012. — 296 p.
16. A.F. Chipiga Information Security of Automatic Systems / A.F. Chipiga. — M.: Helios APB, 2010. — 336 p.
17. V.F. Shangin. Information Security of Computer Systems and Networks: a Textbook / V.F. Shangin. — M.: PH FORUM, RDC INFRA-M, 2013. — 416 p.
18. V.F. Shangin. Information Security and Information Protection / V.F. Shangin. — M.: DMK, 2014. — 702 p.
19. V.I. Yarochkin. Information Security: a Textbook / V.I. Yarochkin. — M.: Academic Project, 2008. — 544 p.
20. S. Renu,S.H.Krishna Veni ‘ 2018. An enhanced security tree to secure cloud data. International Journal of Engineering & Technology, 7 (1.1) 64-70.