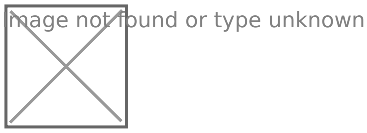
Содержание:



1. Introduction

The Internet is a global computer network spanning the whole world. Today, the Internet has about 15 million subscribers in more than 150 countries. Monthly network size increases by 7-10%. The Internet forms, as it were, the core that provides the connection of various information networks belonging to various institutions around the world, one with the other.

If previously the network was used exclusively as a medium for transferring files and e-mail messages, today more complex tasks of distributed access to resources are being solved. About two years ago, shells were created that support the functions of network search and access to distributed information resources and electronic archives.

The Internet , which once served exclusively as research and educational groups whose interests extended right up to access to supercomputers, is becoming increasingly popular in the business world.

Companies are tempted by speed, cheap global communication, convenience for joint work, affordable programs, and a unique Internet database . They view the global network as a complement to their own local area networks.

In fact, the Internet consists of many local and global networks belonging to different companies and enterprises, interconnected by various communication lines. The Internet can be imagined as a mosaic composed of small networks of various sizes that actively interact with each other, sending files, messages, etc.

At a low cost of services (often this is only a fixed monthly fee for the lines or telephone used), users can access commercial and non-commercial information services in the USA, Canada, Australia and many European countries. In archives of free access to the Internet, you can find information on almost all spheres of human activity, from new scientific discoveries to tomorrow’s weather forecast.

In addition, the Internet provides unique opportunities for cheap, reliable and confidential global communications around the world. It turns out to be very convenient for firms with branches around the world, multinational corporations and management structures. Usually, using the Internet infrastructure for international communications is much cheaper than direct computer communications via satellite or telephone.

Email is the most common Internet service . Currently, approximately 20 million people have an email address. Sending a letter by e-mail is much cheaper than sending a regular letter. In addition, a message sent by e-mail will reach the addressee in a few hours, while a regular letter can reach the addressee for several days, or even weeks.

The Internet is currently experiencing a boom, thanks in large part to the active support of European governments and the United States. About US $ 1-2 million is allocated annually in the United States to create a new network infrastructure. Network communications research is also funded by the governments of Great Britain, Sweden, Finland, and Germany.

However, state funding is only a small part of the incoming funds, as The "commercialization" of the network is becoming more noticeable (80-90% of the funds come from the private sector).

2. Problems of information security

The Internet and information security are incompatible by the very nature of the Internet . It was born as a purely corporate network, however, at present, using a single protocol stack TCP / IP and a single address space, it unites not only corporate and departmental networks (educational, state, commercial, military, etc.), which, by definition , networks with limited access, but also ordinary users who have the opportunity to directly access the Internet from their home computers using modems and a public telephone network.

As you know, the easier the access to the Network, the worse its information security, therefore, we can justifiably say that the initial simplicity of access to the Internet is worse than theft, since the user may not even know that files and programs were copied from him. , not to mention the possibility of their damage and adjustment.

The rapid growth of the Internet, along with a significant set of new features and services, brings a number of new problems, the most unpleasant of which, of course, is the security problem. Even a cursory analysis of the computer press shows that the problem of security and safety of information posted on the Internet or in internal corporate Intranet systems is quite acute. Therefore, it is not surprising that all Internet software companies are introducing increasingly sophisticated information protection tools into their products.

What determines the rapid growth of the Internet , characterized by an annual doubling of the number of users? The answer is simple - a "freebie", that is, the cheapness of the software (TCP / IP), which is currently included in Windows 95, the ease and cheapness of access to the Internet (either using an IP address or using a provider) and to all world information resources.

The fee for using the Internet is a general decrease in information security, therefore, to prevent unauthorized access to their computers, all corporate and departmental networks, as well as enterprises using intranet technology , put fire-walls between the internal network and the Internet , which actually means leaving the Internet single address space. Even greater security will be provided by the departure from the TCP / IP protocol.

This transition can be carried out simultaneously with the process of building a global public information network, based on the use of network computers, which using a 10Base-T network card and cable modem provide high-speed access (10 Mbps) to the local Web server via a cable television network.

Data security is a major concern on the Internet . There are more and more scary stories about how computer crackers, using increasingly sophisticated techniques, penetrate other people's databases. Of course, all this does not contribute to the popularity of the Internet in business circles. The mere thought that some hooligans or, worse, competitors will be able to access archives of commercial data, makes corporate executives refuse to use open information systems. Experts argue that such fears are unfounded, as companies that have access to both public and private networks have almost equal chances of becoming victims of computer terror.

What can happen to your information if you do not care about its security?

The first is the loss of privacy.

Your personal information may remain intact, but will no longer be confidential, for example, someone on the Internet will receive your credit card number.

Secondly, this is Modification.

Your information will be modified, for example, your order in the on-line store or your resume.

Thirdly, the substitution of information, which can be of 2 types.

1) WWW server can impersonate another, which it is not.

2) WWW server can really exist under this name and claim, for example, that it is an online store, but in reality never send any goods, but only collect credit card numbers.

An attack on information can be accomplished in several ways.

Firstly, it is an attack on the client system from the server side.

A hacker who has his own WWW server can try using Java incorrect applets and JavaScript applications embedded in an HTML document to disable the user system, or obtain information about it that will allow him to crack the user's machine.

Secondly, the attack on the server from the client.

A hacker can try to disable a user system or www server through a www client , or gain access to information that he does not have access to. To do this, he can use security holes in CGI applications, poor server configuration, try to replace the CGI application.

Finally, information may be stolen by a third party upon transmission.

Every organization dealing with any values, sooner or later faces an encroachment on them. Prudent begin to plan the defense in advance, prudent - after the first major “puncture”. One way or another, the question is what, how and from whom to protect.

Usually, the first reaction to a threat is the desire to hide values in an inaccessible place and put protection on them. This is relatively uncomplicated when it comes to values that you won’t need for a long time: removed and forgotten. Much more difficult if you need to constantly work with them. Each call to the store for your values will require a special procedure, take time and create additional inconvenience. This is the security dilemma: you have to make a choice between the security of your property and its availability for you, and therefore the possibility of useful use.

All this is true with respect to information. For example, a database containing confidential information is only then completely protected from encroachment when it is located on disks removed from a computer and put into a protected place. As soon as you have installed these disks in the computer and started using it, several channels appear along which the attacker, in principle, has the opportunity to gain access to your secrets without your knowledge. In other words, your information is either inaccessible to everyone, including you, or is not one hundred percent protected.

It may seem that there is no way out of this situation, but information security is akin to navigation safety: both of these are possible only taking into account some allowable degree of risk.

In the field of information, the security dilemma is formulated as follows: you must choose between the security of the system and its openness. It is more correct, however, to speak not about choice, but about balance, since a system that does not have the property of openness cannot be used.

3. PROTECTION OF WEB SERVERS

An organization's Web server provides its presence on the Internet . However, the data distributed by this server may contain private information that is not intended for others. Unfortunately, Web servers are tidbits for cybercriminals. Cases of an "attack" on the servers of the Ministry of Justice and even the CIA were widely publicized: attackers replaced the home pages of these organizations with obscene cartoons. Animal rights advocates infiltrated the Kriegsman Furs server and replaced the home page with a link to sites dedicated to protecting our smaller brothers. A similar fate befell the servers of the Ministry of Justice of the United States, the CIA, Yahoo ! and fox . Dan Farmer , one of the creators of the program SATAN, to find gaps in the protection of networks used has not yet completed his official version of the scanner to probe the Web - Server Internet and found that nearly two-thirds of them have serious flaws in the defense.

Obviously, Web servers are far less secure than we would like. In some simple cases, it's all about inconspicuous but unsafe flaws in the CGI scripts. In other situations, the threat is the inadequate protection of the host operating system.

The easiest way to strengthen the security of a Web server is to place it behind a firewall. However, acting in this way, the user as it were transfers security problems to the internal corporate network, and this is not the most successful solution. As long as the Web server is located “on the other side” of the firewall, the internal network is protected, but the server is not. A side effect of this step is the complexity of administering the Web server .

A better solution would be a compromise: hosting a Web server on its own network, banning external connections, or restricting access to internal servers.

Along with ensuring the security of the software environment, the most important issue will be the delimitation of access to Web service objects . To resolve this issue, it is necessary to understand what the object is, how subjects are identified, and which access control model - forced or arbitrary - is used.

The Web -Server access objects are the universal resource locator (the URL - Uniform (Universal) the Resource Locator). Various entities can stand behind these locators - HTML files, CGI procedures, etc.

Typically, access subjects are identified by IP addresses and / or names of computers and management areas. In addition, password authentication of users or more complex schemes based on cryptographic technologies can be used.

In most Web servers, rights are delimited to the extent of directories (directories) using arbitrary access control. Permissions may be granted for reading HTML files, executing CGI procedures, etc.

For early detection of attempts to illegally enter the Web server, regular analysis of registration information is important.

Of course, the protection of the system on which the Web server operates must follow universal recommendations, the main of which is the maximum simplification. All unnecessary services, files, devices must be deleted. The number of users who have direct access to the server should be minimized, and their privileges should be ordered in accordance with their official duties.

Another general principle is to minimize the amount of server information that users can receive. Many servers, if accessed by the name of the directory and the absence of the index.HTML file in it, produce an HTML version of the directory contents. This table of contents may contain file names with the source code of CGI procedures or with other confidential information. It is advisable to turn off such “additional features”, since excess knowledge (of an attacker) multiplies sorrows (of the server owner).

3.1. Access restrictions in WWW servers

Consider two of them:

- Limit access by IP addresses of client machines;

- enter the recipient ID with a password for this type of document.

The introduction of restrictions of this kind began to be used quite often, because many seek the Internet to use its communications to deliver their information to consumers. Using this kind of mechanisms for delimiting access rights, it is convenient to self- distribute information for the receipt of which there is a contract.

IP address restrictions

Access to private documents can be allowed, or vice versa denied using the IP addresses of specific machines or networks, for example:

123.456.78.9

123.456.79.

In this case, access will be allowed (or denied depending on the context) for the machine with the IP address 123.456.78.9 and for all subnet machines 123.456.79.

Recipient ID restrictions

Access to private documents can be allowed, or vice versa can be denied using the assigned name and password to a specific user, and the password is not stored explicitly anywhere.

3.2 World wide web servers and information security problem

Among WWW servers, Netscape servers, WN and apache are notable for the lack of known security problems .

WN server.

It is a freeware server available for many UNIX platforms. Its main goals were safety and flexibility. WN server contains in each directory a small database (list) of documents contained in it. If the document is not listed in the database, the client cannot receive it. Databases are either automatically generated by a special program for all files in the directory tree, or are created from other text descriptions by another program manually. In addition to listing documents, you can embed HTML text in these files, because this is an analogue of index.html in this server.

The web site administrator does not need to understand the generated files, but in principle they are similar. cache gopher files . The server itself has a form for simultaneously processing gopher and http requests for the same documents.

The security of executing CGI applications is ensured by setting uid / gid for the required file of this database. Without any programming and special settings, the WN server provides 8 search options within documents, has an interface to the WAIS server. You can include some documents inside others on the server side (for example, standard messages at the beginning and at the end of a document) You can apply filters to any document to obtain the necessary document at the output (for example, word substitution). To access the document, you can use a URL like < http : // host / dir / foo; lines = 20-30 to get lines 20 to 30. The server documentation is very good, it is installed quickly, detected errors are fixed within a few days .

Apache server is a freely distributed WWW server for various UNIX platforms and Windows NT, one of the most popular in the world. Now apache runs on 36 percent of the total number of all HTTP servers in the world. It is a fast and stable server. You can embed the SSL protocol into the server , which is described below using the Netscape server as an example .

Netscape Enterprise Server.

Netscape Enterprise Server is a high-performance, secure World Wide Web server for creating, distributing, publishing information on the Internet and running Internet-based Internet applications using tools based on Java and JavaScript .

Netscape FastTrack Server.

Netscape FastTrack server is a solution for those who are not satisfied with the price and complexity of the Netscape Enterprise server. It is easy to use, designed to allow beginners to create and administer a WWW server.

Netscape servers have built-in security for commercial information and communications. Flexible user authorization controls access to individual files and directories using user name and password, domain name, machine name, IP address, client-side certificates , named groups. Additional security features are provided by Secure Socket Layer 3.0 (SSL 3.0) protocol and public key mechanism.

SSL 3.0 is the latest version of the widespread Internet standard developed by Netscape Communications corporation .

SSL protocol ensures confidentiality, integrity and authenticity of information.

Confidentiality and integrity of information is ensured through public key encryption. Authentication is provided through digital certificates that are almost impossible to fake. The certificate must be obtained from a third party that both parties trust.

SSL protocol is a low level encryption scheme used to encrypt transactions in high level protocols such as HTTP, NNTP and FTP. The SSL protocol contains methods for identifying the server for the client, encrypting data during transmission, and additionally, verifying the client for the server. From commercial SSL systems, the protocol is now implemented in Netscape navigators and Netscape servers. (Implemented data encryption and server authorization, no client authorization).

There is also a freely available version of SSL called SSLeay . It contains C source code that can be embedded in applications such as Telnet and FTP. The freely distributed Unix Web servers Apache and NCSA httpd and several Web clients, including Mosaic, are also supported . This package can be used free of charge for commercial and non-commercial applications.

The public key mechanism provides encryption of data using a public key (public key). In traditional encryption systems, the same key was used for encryption and decryption. In a new open or asymmetric encryption system, keys go in pairs: one key is used for encoding, the other for decoding. One of these keys, called the public key, is freely available and is used to encode messages. Another key, called a private key, is secret and is used to decode an incoming message. In this system, a user sending a message to a second user can encrypt the message with the public key of the second user.

The message can be decrypted by the owner of the secret private key of the second user. This system can be used to create fake digital signatures. In Netscape Enterprise Server, administrators can dynamically change keys for a server, allowing you to quickly change authorization policies.

Netscape servers and navigators encrypt using either a 40-bit key or a 128-bit key. In principle, you can crack a 40-bit key by sorting through every possible combination (a total of 2 ^ 40) until you find that the message is decrypted. Hacking a 128-bit key is almost impossible.

3.3.Java, JavaScript and a security issue

Java and JavaScript - this is the section of Web security that does not concern administrators and creators of Web servers, but users and administrators of user networks.

Despite the similarities in the names of Java and JavaScript, these are two different products. Java is a programming language developed by SunSoft . Java programs are precompiled in a compact form and stored on the server. HTML documents can reference mini - applications called Java applets . WWW clients that support Java applets download compiled Java applications and run them on the client machine. JavaScript is a set of HTML extensions interpreted by the WWW client. In principle, despite the fact that JavaScript has a longer history of security-related problems, a Java hacker can actively and successfully disable a user's system, so far only cases of sending confidential client information to a Web server are known about JavaScript . Java applets run on the client side, not on the server side, and therefore increase the risk of server-side attacks. Do I need to worry about this?

The Java embedded tools to limit access to the client machine. Applets are not allowed to execute system commands, load system libraries, or open system devices such as disks. Applets, depending on the WWW client, are prohibited from all disk operations (Netscape), or almost all (HotJava). Applets are allowed to establish a network connection only to the server from where the applet was loaded. But Drew Dean (ddean@cs.princenton.edu) found that you can write an applet that will establish a connection to any computer on the Internet, that is, an applet from the Internet downloaded by your client to your local WWW machine can connect via TCP / IP to any a machine on your local network, even if it is protected through a firewall . This issue is due to Java verifying for a connection through Domain .

Name System (DNS). An attacker using his own DNS server can create an incorrect DNS link to force the Java system to assume that the applet is allowed to connect to a computer to which it does not have the right to connect. The bug was fixed in Netscape Navigator 2.01 and JDK 1.0.1.

David Hopwood discovered that by downloading applets from 2 different WWW servers, a hacker could violate the Java Virtual Machine namespace . This allows you to convert variable types to each other, convert integers to links, etc. As a result, the applet can read and write local files, execute machine code. Without any problems, a file can be created on UNIX. rhosts . This error manifests itself, at least in HotJava , the code can be written entirely in Java and be platform independent .

In real versions of Java , tricks are possible with calling the constructor of the superclass, as a result of which this call may be skipped. This is due to the algorithm that the Java interpreter is currently using . Possible ways to do this:

-super inside try.

-super inside if.

- cathcer / thrower.

JavaScript - this is built into the Netscape navigator . From time to time, the Netscape navigator detected security issues with JavaScript , which Netscape periodically fixes in newer versions of the navigator. Andy Augustine in its JavaScript FAQ describes the following problems: 1) Read custom URL history - fixed in Netscape 2.0.

2) Read custom URL cache - fixed in Netscape 2.0.

3) Reading a user e- mail address and transmitting it over the Internet is fixed in Netscape 2.01.

4) Getting recursive file system table of contents - fixed in Netscape 2.01.

5) Opening a 1-pixel window, receiving the URL of open documents and transferring them to a remote server. This is a common network graphics system problem with a long history. Users of x- windows who run the ` xhost +` command without arguments may encounter someone else's invisible window that transmits user input over the Internet to the hacker.

In order to work with Java and JavaScript applications without security problems it is recommended:

-Do not use older versions of WWW clients that support Java and JavaScript . Web client manufacturers fix their programs if a new security bug is discovered.

-Follow the current state of affairs with Java and Javascript security . Javasoft has a Java and security page . In netscape has a similar page about JavaScript . Each manufacturer of the web client has a security page on its server.

In conclusion, a few general rules that will help you avoid many problems.

1.When creating a web server, use a reliable product. Use a web server that suits your needs, not necessarily the most comprehensive and fashionable.

2. Read the server documentation. Deficiencies in the configuration often create security problems than errors in the server itself.

3. Do not forget about the SSL protocol when it comes to commercial information.

4. Take care of the security of CGI applications, as these are parts of the server itself. Do not forget to check other people's CGI applications if you have a multi-user server.

5. Do not use older versions of Web clients that support Java and JavaScript . Keep for updates.

4. Conclusion

In this paper, I examined the problems of information security in the global Internet . This problem has been and remains relevant to this day, since no one can guarantee one hundred percent that your information will be protected or a virus will not get into your computer. The urgency of this problem is also confirmed by the fact that a huge number of pages on the Internet are devoted to it . However, most of the information is in English, which makes it difficult to work with it. Of course, in this paper, only part of the problem is considered (for example, information protection with the help of firewalls (firewalls) is not considered). Studies have shown that the developed many ways to protect information: access control, password protection, data encryption itp . However, despite all this, we still hear about hackers breaking into various servers and computer systems. This suggests that the problem of information security has not yet been resolved and a lot of time and effort will be spent on its solution.

5. List of special terms

ARP (Address Resolution Protocol) - protocol for determining the address, converts the address of a computer on the Internet into its physical address.

ARPA (Advanced Research Projects Agency) is the US Department of Defense's Advanced Research Projects Bureau.

Ethernet is a type of local area network. A good variety of wire types for connections that provide bandwidths from 2 to 10 million bps (2-10 Mbps). Quite often, computers using the TCP / IP protocols connect via Ethernet to the Internet .

FTP (File Transfer Protocol) - file transfer protocol, a protocol that defines the rules for transferring files from one computer to another.

FAQ (Frequently Asked Qustions) - Frequently Asked Questions. The section of public archives of the Internet in which information is stored for "novice" users of the network infrastructure.

Gopher is an interactive shell for finding, joining and using Internet resources and features . The user interface is implemented through the menu system.

HTML (Hypertext Markup Language) is a language for writing hypertext documents. The main feature is the presence of hypertext links between documents located in various archives of the network; thanks to these links, you can go directly to other documents while viewing one document.

Internet is a global computer network.

IP (Internet Protocol) - the protocol of interworking, the most important of the protocols of the Internet , provides routing of packets on the network.

IP address - a unique 32-bit address of each computer on the Internet .

Telnet - remote access. It enables the subscriber to work on any Internet computer as on his own.

TCP \ IP - TCP \ IP usually means all the many protocols supported on the Internet .

TCP (Transmission Control Protocol) - a protocol for controlling the transmission of information on a network. TCP is a transport layer protocol, one of the main Internet protocols . Responsible for establishing and maintaining a virtual channel (i.e. logical connection), as well as for error-free transmission of information on the channel.

UDP (User Datagram Protocol) is a transport layer protocol, unlike TCP, it does not provide error-free packet transmission.

Unix is a multi-tasking operating system, the main operating environment on the Internet . It has various implementations: Unix -BSD, Unix-Ware , Unix-Interactive .

UUCP is a protocol for copying information from one Unix host to another. UUCP - is not part of the TCP / IP protocols, but is nevertheless still widely used on the Internet . Based on the UUCP protocol, many mail exchange systems have been built that are still used on the network.

WWW (World Wide Web) - World Wide Web. A system of distributed databases with hypertext links between documents.

6. References

1.Http: //www.lanmag.ru/

2. Eager B. Work on the Internet / Ed. A. Tikhonova; Per. c English - M .: BINOM, 1998 .-- 313 p.

3.LAN / NetworkSolutionMagazine # 7-8 1998.

4. Levin in . To . Information protection in information and computing systems and networks // Programming. - 1994. - N5. - C. 5-16.