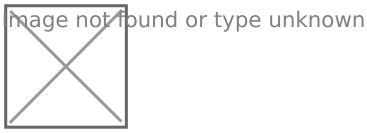
Содержание:



Internet - a global computer network that covers the entire world. Today, the Internet has about 15 million subscribers in more than 150 countries. The network size increases by 7-10% every month. The Internet forms a kind of core that connects various information networks belonging to various institutions around the world, one with another.

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, we created wrappers that support network search and access to distributed information resources and electronic archives.

The Internet, which once served exclusively for research and training groups whose interests extended all the way to access 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 database of the Internet. They view the global network as an extension of their own local area networks.

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

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

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

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

Currently, the Internet is experiencing a period of recovery, largely due to the active support from the governments of European countries and the United States. Every year, the US allocates about 1-2 million dollars to create a new network infrastructure. Research in the field of network communications is also funded by the governments of great Britain, Sweden, Finland, and Germany.

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

1.1 information security Issues

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

As you know, the easier access to the Network, the worse its information security, so we can say with good reason that the initial ease of access to the Internet is worse than theft, since the user may not even know that they have copied files and programs, not to mention the possibility of their damage and correction.

What determines the rapid growth of the Internet, characterized by an annual doubling of the number of users? The answer is simple - " freebies”, that is, the cheapness of 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 the world's information resources.

The cost of using the Internet is a General reduction in information security, so to prevent unauthorized access to their computers, all corporate and departmental networks, as well as enterprises using intranet technology, put filters (fire-wall) between the internal network and the Internet, which actually means leaving the single address space. Even more security will be provided by moving away from the TCP/IP Protocol and accessing the Internet through gateways.

This transition can be performed simultaneously with the process of building a worldwide public information network, based on the use of network computers that use a 10Base-T network card and a cable modem to provide high-speed access (10 Mbit/s) to a local Web server via a cable TV network.

To address these and other issues when transitioning to a new architecture

Internet you need to provide the following:

First, to eliminate the physical link between the future Internet (which will become a global public information network) and corporate and departmental networks, preserving only the information link between them through the World Wide Web system.

Second, replace routers with switches, eliminating processing in IP Protocol nodes and replacing it with Ethernet frame translation mode, in which the switching process is reduced to a simple MAC address comparison operation.

Third, move to a new unified address space based on physical media access addresses (MAC layer), linked to the geographical location of the network, and allowing 48-bit addresses to be created for more than 64 trillion independent nodes.

Data security is one of the main problems in the Internet. There are more and more horror stories about how computer hackers, using more and more sophisticated techniques, get into other people's databases. Of course, all this does not contribute to the popularity of the Internet in business circles. Just the thought that some hooligans or, even worse, competitors will be able to get access to the archives of commercial data, makes corporate management refuse to use open information systems. Experts say that such fears are groundless, since companies with access to both open and private networks have almost equal chances of becoming victims of computer terror.

Every organization that deals with any kind of values, sooner or later faces an attack on them. The prudent begin to plan protection in advance, the unintelligent-after the first major "puncture". Anyway, the question arises about what, how and from whom to protect.

Usually the first reaction to a threat is to hide valuables in an inaccessible place and put guards on them. This is relatively easy if we are talking about such values that you will not need for a long time: removed and forgotten. It is much more difficult if you need to constantly work with them. Each request to the store for your valuables will require a special procedure, take time, and create additional inconvenience. This is the security dilemma: you have to choose between the security of your property and its availability for you, and therefore the possibility of useful use.

This is also true of information. For example, a database containing confidential information is only fully protected when it is located on disks removed from the computer and stored in a secure location. As soon as you install these disks in your computer and start using them, several channels appear at once, through which an attacker, in principle, can get access to your secrets without your knowledge. In other words, your information is either inaccessible to everyone, including you, or it is not protected one hundred percent.

It may seem that there is no way out of this situation, but information security is akin to the safety of navigation: both are possible only with a certain acceptable 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.

In the banking sector, the problem of information security is complicated by two factors: first, almost all the values that a Bank deals with (except for cash and something else) exist only in the form of some information. Secondly, a Bank cannot exist without connections with the outside world: without clients, correspondents, etc. At the same time, the same information that expresses the values that the Bank works with (or information about these values and their movement, which sometimes cost more than the values themselves) is necessarily transmitted through external relations. Documents are sent from outside that the Bank uses to transfer money from one account to another. Externally, the Bank transmits orders on the movement of funds on correspondent accounts, so that the Bank's openness is set a priori.

It is worth noting that these considerations apply not only to automated systems, but also to systems that are built on traditional paper document management and do not use other links than courier mail. Automation has added to the security services ' headaches, and new trends in the development of banking services based entirely on information technology are exacerbating the problem.

1.1.1 Information security and information technology

At the early stage of automation, the introduction of banking systems (and in General, banking automation tools) did not increase the Bank's openness. Communication with the outside world, as before, went through operators and couriers, so the additional threat to the security of information arose only from possible abuse by the Bank's own information technology specialists.

This situation changed after the financial services market began to offer products that could not have been created without information technology. First of all, these are plastic cards. While card service was in voice authorization mode, the Bank's information system was slightly more open, but then ATMs, POS terminals, and other self-service devices appeared—that is, funds belonging to the Bank's information system, but located outside it and accessible to persons outside the Bank.

The increased openness of the system required special measures to control and regulate information exchange: additional means of identification and authentication of persons who request access to the system (PIN code, customer information on the magnetic stripe or in the memory of the card chip, data encryption, control numbers and other means of card protection), means of cryptographic protection of information in communication channels, etc.

An even greater shift in the security-openness balance towards the latter is related to telecommunications. It is relatively easy to protect electronic payment systems between banks, since banks themselves are the subjects of electronic information exchange. However, where protection was not given the necessary attention, the results were quite predictable. Unfortunately, our country is the most glaring example. The use of extremely primitive telecommunications security tools in 1992 resulted in huge losses on fake vouchers.

The General trend in the development of telecommunications and the mass distribution of computer technology eventually led to the fact that new, purely telecommunications products appeared on the banking market all over the world, and first of all, Home Banking systems (the domestic equivalent is“client—Bank”). This required providing customers with round-the-clock access to an automated banking system for conducting transactions, and the customer was authorized to perform Bank transactions directly. The degree of openness of the Bank's information system has increased almost to the limit. Accordingly, special measures are required to ensure that its security does not fall as significantly. Finally, the era of the “information superhighway " has come: the explosive development of the Internet and its associated services. Along with new opportunities, this network has brought new dangers. It would seem that what difference does it make if the client contacts the Bank via a dial-up line that comes to the modem pool of the Bank's communication node, or via the Internet over IP Protocol? However, in the first case, the maximum possible number of connections is limited by the technical characteristics of the modem pool, while in the second case, the Internet capabilities can be significantly higher. In addition, the Bank's network address is generally public, while the modem pool's phone numbers can only be shared with interested parties. Accordingly, the openness of a Bank whose information system is connected to the Internet is significantly higher than in the first case. So in just five months of 1995, the Citicorp computer network was hacked 40 times! (This indicates, however, not so much about some “danger” of the Internet in General, as about the insufficiently qualified work of Citicorp security administrators.)

All this makes it necessary to review approaches to ensuring the Bank's information security. When connecting to the Internet, you should re-conduct a risk analysis and draw up a plan to protect the information system, as well as a specific plan to eliminate the consequences that arise in the event of certain violations of confidentiality, security and availability of information.

At first glance, for our country, the problem of Bank information security is not so acute: whether we care about the Internet, if most banks have second-generation systems running in the "file server" technology. Unfortunately, we have already registered “computer theft". The situation is complicated by two problems. First of all, as experience with representatives of banking security services shows, both in the management and among the staff of these services, former operational employees of the internal Affairs or state security agencies predominate. They are highly qualified in their field, but most of them are not familiar with information technology. There are very few specialists in information security in our country, because this profession is becoming popular only now.

The second problem is related to the fact that in many banks, the security of the automated banking system is not analyzed and is not seriously provided. Very few places have the necessary set of organizational documents (risk analysis, protection plan, and response plan) described above. Moreover, the security of information often simply cannot be ensured within the framework of the Bank's automated system and the accepted rules for working with it.

Not so long ago, I had a chance to give a lecture on the basics of information security at one of the seminars for heads of automation departments of commercial banks. To the question “ " do you Know how many people have the right to enter the premises where Your Bank's database server is located?", no more than 40% of those present answered in the affirmative. Only 20% were able to name those who have this right by name. In other banks, access to this room is not restricted and is not controlled in any way. What to say about access to workstations!

As for automated banking systems, the most common second-and third-generation systems consist of a set of standalone software modules that are run from the DOS command line on workstations. The operator can log out to DOS from such a software module at any time. It is assumed that this is necessary to switch to another software module, but in fact, in such a system, there are no ways not only to prevent the operator from running any other programs (from a harmless game to a program that modifies Bank account data), but also to control the operator's actions. It is worth noting that in a number of systems of these generations, including those developed by highly respected domestic firms and sold by the hundreds, account files are not encrypted, i.e. the data in them can be viewed by the simplest public means. Many developers restrict security administration tools to the regular network operating system tools: log in to the network -- do what you want.

The situation is changing, but too slowly. Even in many new developments, security issues are clearly not given enough attention. At the Bank and Office—95 exhibition, an automated banking system with a client-server architecture was presented, with workstations running under Windows. In this system, the operator's login to the program is very peculiar: a password is requested in the dialog box, and then a list of surnames of all operators who have the right to work with this module is presented for selection! There are many more such examples.

Nevertheless, our banks pay a lot of attention to information technologies, and they quickly learn new things. The Internet and financial products associated with it will enter the life of Russian banks faster than sceptics expect, so now it is necessary to take care of information security issues at a different, more professional level than it has been done so far.

1.3 Information security in Intranet

The Intranet architecture involves connecting to external open networks, using external services, and providing your own services externally, which imposes increased requirements for data protection.

Intranet systems use a client-server approach, and the main role is currently assigned to the Web service. Web servers must support traditional security measures, such as authentication and access control, and new features must be provided, especially the security of the software environment on both the server and client sides.

These are, to put it very briefly, the challenges in the field of information security that arise in connection with the transition to Intranet technology. Next, we will look at possible approaches to solving them.

The formation of an information security regime is a complex problem.

Measures to address this problem can be divided into four levels:

* legislative (laws, regulations, standards, etc.);

* administrative (General actions taken by the organization's management);

* procedural (specific security measures dealing with people);

* software and technical (specific technical measures).

In this order, the following statement will be constructed.

SECURITY OF THE SOFTWARE ENVIRONMENT

The idea of networks with so-called active agents, when not only passive but also active executable data (i.e. programs) are transmitted between computers, is certainly not new. The original goal was to reduce network traffic by performing most of the processing where the data is located (bringing programs closer to the data). In practice, this meant moving programs to servers. A classic example of implementing this approach is stored procedures in relational databases.

For Web servers, stored procedures are analogous to programs that serve the Common Gateway Interface (CGI).

CGI procedures are located on servers and are usually used for dynamic generation of HTML documents. The organization's security policy and procedural measures should determine who has the right to place CGI procedures on the server. Strict control is necessary here, since the server executing an incorrect program can lead to any severe consequences. A reasonable technical measure is to minimize the privileges of the user on whose behalf the Web server is running.

In Intranet technology, if you care about the quality and expressive power of the user interface, you need to move programs from Web servers

PROTECTING WEB SERVERS

Along with ensuring the security of the software environment (see the previous section), the most important issue will be the issue of delimiting access to Web service objects. To resolve this issue, you need to understand what the object is, how the subjects are identified, and whether the access control model is enforced or arbitrary.

In Web servers, access objects are universal resource locators (URL - Uniform (Universal) Resource Locator). These locators can be used by various entities - HTML files, CGI procedures, and so on.

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

In most Web servers, permissions are delimited up to directories using arbitrary access control. You can grant rights to read HTML files, perform CGI procedures, and so on.

Regular analysis of registration information is important for early detection of attempts to illegally enter the Web server.

Of course, the protection of the system on which the Web server operates must follow universal recommendations, the main of which is the maximum simp

AUTHENTICATION IN OPEN NETWORKS

Methods used in open networks to confirm and verify the authenticity of subjects must be resistant to passive and active listening to the network. Their essence boils down to the following.

* The subject demonstrates knowledge of the secret key, and the key is either not transmitted over the network at all, or it is transmitted in encrypted form.

* The subject demonstrates possession of a software or hardware tool for generating one-time passwords or a tool that operates in the “request-response " mode. It is easy to see

that intercepting and then replaying a one-time password or response to a request does not give the attacker anything.

* The subject demonstrates the authenticity of its location using a navigation satellite system.

VPNs

One of the most important tasks is to protect corporate data flows transmitted over open networks. Open channels can only be securely secured by one method - cryptographic.

Note that the so-called dedicated lines do not have special advantages over public lines in terms of information security. Dedicated lines will be located at least partially in an uncontrolled zone, where they can be damaged or unauthorized connection to them. The only rea