DOI https://doi.org/10.36059/978-966-397-104-9/96-117

CYBER SECURITY AND COMPUTER ATTACKS

Domnich V. I.

1. Virtual private networks and public information networks

The aspects of security of modern information networks and the specifics of the use of virtual private network technology are considered, considered on the example of the Internet sharing network, the information security features of which largely determine the modern directions of building information networks of large companies and organizations[1].

It is interesting to note that 95% of US Department of Defense traffic is transmitted through public networks (including the Internet) in peacetime. In wartime this proportion should be "only" 70%.

We can assume that the Pentagon is not the poorest organization. The US military relies on public service networks because it develops its infrastructure in the face of rapid technological change – a very expensive and futile exercise, justified even in critical national organizations only in exceptional cases.

There are a number of common attacks based on protocol features and network structure, describing the reasons why they are possible, and how to resolve vulnerabilities. Recommendations are given to increase the degree of protection of modern information networks.

Typical attacks are discussed, but some general definitions must be made first and security classification should be considered. In addition, it should be noted that, according to statistics, data destruction in computer systems is most often caused not by hackers, program errors or virus actions (17%) or technical failures (16%), but by errors and unauthorized user actions (67%).

2. Basic concepts of computer security

A computer system security threat is a potentially possible event that may adversely affect the system itself, as well as the information stored therein[2].

[1] Крол Эд. Все об Internet: Руководство и каталог. Пер. с англ. С.М. Тимачева. Киев: BNV, 1995. 591 с.

[2] Вертузаев М. С., Юрченко О.М. Защита информации в компьютерных системах от несанкционированного доступа. Київ: Европ. ун-т, 2001. 320 с.

The vulnerability of a computer system is some of its unsuccessful characteristics that make it possible to create a threat.

Finally, an attack on a computer system is an action taken by an attacker to identify and exploit a particular vulnerability.

Researchers typically identify three major types of security threats:

- disclosure,
- integrity,
- denial of service.

The threat of disclosure is that the information becomes known to those who should not know it. Sometimes, the term "disclosure" uses the terms "theft" or "leakage."

The threat of integrity involves any deliberate alteration of data stored in a computer system or transmitted from one system to another. Disclosure threats are generally considered to be predominantly exposed by government agencies, and threats to integrity are business or commercial.

The threat of denial of service occurs every time that some actions block access to some computing system resource.

In fact, the blocking can be permanent, so that the requested resource is never received, or it can only cause a delay of the requested resource, long enough for it to become unnecessary. In such cases, the resource is said to be exhausted.

In local area network (LAN), the most common threats are disclosure and integrity, and in the global are the threat of denial of service.

3. Computer network security features

The main feature of any network system is that its components are distributed in space and the connection between them is physically carried out through network connections (coaxial cable, twisted pair, optical fiber, etc.). п.) And programmatically through a message mechanism. In this case, all control messages and data transmitted between the objects of the distributed computing system are transmitted over the network connections in the form of packets[3].

Network systems are characterized by the fact that, in addition to the usual (local) attacks carried out within the same computer system, they are

[3] Ярочкин В.И. Основы защиты информации. Москва: Летописец, 2000. 150 с.

subject to a specific type of attacks, due to the distribution of resources and information in space.

These are so-called remote or network attacks. They are characterized, first, by the fact that the attacker can be located thousands of kilometers from the attacked object, and, second, by the fact that the information transmitted over network connections may not be attacked by a specific computer[4].

With the development of local and global networks, it is remote attacks that are leading in both the number of attempts and the success of their application and, accordingly, ensuring the security of the OS in terms of counteracting remote attacks is of paramount importance.

4. Classification of computer attacks

The forms of organization of attacks are very diverse, but in general they all fall into one of the following categories[5]:

- Remote Computer Intrusion: Applications that gain unauthorized access to another computer over the Internet (or local area network).
- Local Computer Intrusion: Applications that gain unauthorized access to the computer they are running.
- Remote computer lock: Programs that block the entire remote computer or an individual program on it through the Internet (or network).
- Local computer lock: Programs that block the computer on which they work.
- Network Scanners: Applications that collect network information to determine which computers and applications running on them are potentially vulnerable to attack.
- Vulnerability Scanners: Applications that scan large groups of computers on the Internet in search of computers vulnerable to one or * other specific type of attack.
- Password crackers: applications that detect easily guessed passwords in encrypted password files.
- Network Analyzers (sniffers): Applications that listen to network traffic. Often, they have the ability to automatically isolate usernames, passwords, and credit card numbers from traffic.

[4] Зепкды П.Д. Теория и практика обеспечения информационной безопасности. Под ред. Москва: Яхтсмен, 1996. 302 с.

[5] HackZone- территория взлома (httn://www.hackzone.ru).

- Modification of transmitted data or substitution of information. Replacing a trusted distributed CS object (working on its behalf) or a faulty distributed system object (DCS).
- Social engineering is unauthorized access to information, other than hacking software. The goal is to trick people into getting passwords to the system or other information that will help break the security of the system.

5. Statistics of the most common attacks

In 1999, NIST (National Institute of Standards and Technology) analyzed 237 computer attacks, the information of which was published on the Internet. This analysis provided the following statistics:

29% of the attacks were from Windows.

Conclusion: It is not necessary to consider only the Unix system dangerous. The availability of hacking applications on the network allows them to be used not only by specialists.

In the future, this percentage is likely to grow.

In 20% of attacks, attackers were able to remotely infiltrate network elements (routers, switches, hosts, printers, and firewalls).

Conclusion: Attacks in which an attacker gains unauthorized access to remote hosts are not that rare.

In 3% of attacks, websites attacked their visitors.

Conclusion: Finding information on the WWW (World Wide Web) is no longer a completely safe activity.

In 4% of attacks, the Internet was scanned for vulnerable hosts.

Conclusion: There are many auto-scanning tools that can compromise hosts. System administrators must scan their systems regularly (otherwise someone else will do it).

5% of attacks were successful attacks against routers and firewalls.

The components of the Internet infrastructure themselves are vulnerable to attack (though, most of these attacks were remote computer-locked and scanned attacks, and only a small fraction were remote-penetration).

According to a 1999 survey by the Computer Security Institute and the FBI on computer crimes, 57% of organizations surveyed said they consider the connection point from local network to the Internet as point from where attacks are often organized. 30% of those surveyed reported

that they had penetrated their network, and 26% said that the information had been stolen in the course of the attacks. The Federal Center for Computer Crime in the US – FedCIRC reported that in 1999, about 130,000 state networks with 1,100,000 computers were attacked.

6. Network Traffic Analysis of the Internet

One way to obtain passwords and user IDs on the Internet is to analyze network traffic. Network analysis is carried out by means of a special program-package analyzer (sniffer), intercepts all packets transmitted by a segment of the network, and distinguishes among them those in which the user ID and his password are transmitted.

In many protocols, data is transmitted in an open, unencrypted form. Network traffic analysis allows to intercept data transmitted via FTP and TELNET protocols (passwords and user IDs), HTTP (transfer of hypertext between web-server and browser, including user-entered forms on web-pages), SMTP, POP3, IMAP, NNTP (email and conferences) and IRC (online chat). Thus, passwords can be intercepted to access mail systems with a web interface, credit card numbers when working with e-commerce systems and various personal information, the disclosure of which is undesirable.

Currently, various exchange protocols have been developed to protect the network connection and encrypt the traffic (for example, SSL and TLS, SKIP, S-HTTP, etc.). Unfortunately, they have not yet changed the old protocols and have not become the standard for every user.

To some extent, restrictions on the export of strong cryptography tools have prevented their proliferation. Because of this, the implementation of these protocols either did not build into the software, or significantly weakened (limited the maximum key length), which led to the practical futility of them, as the ciphers could be opened within an acceptable time.

7. Fake ARP-server on the Internet

To address IP packets on the Internet, in addition to the host IP address, you need either the Ethemet address of its network adapter (in the case of addressing within one subnet), or the Ethemet address of the router (in the case of inter-network addressing). Initially, the host may not have information about the Ethemet addresses of other hosts that reside with it in the same segment, including the router's Ethernet address.

Therefore, a standard problem solved with the remote search algorithm is facing the host.

The Internet uses the Address Resolution Protocol (ARP) to solve this problem. The ARP protocol allows one-to-one correspondence of IP and Ethemet addresses for hosts within one segment. This protocol works as follows: the first time you access a network resource, the host sends a ARP broadcast request, which specifies the IP address of the desired resource (router or host) and asks for its Ethemet address.

This request is received by all stations in this segment of the network, including the station being searched for. Upon receiving this request, the host enters the station request record into its ADR table and then sends an ADR response to the host with its Ethemet address.

Received in the ARP response The Ethemet address is stored in the ARP table stored in the operating system memory on the host.

Because of the use of remote search algorithms, it is possible to execute a typical remote attack in such a network.

The general scheme of this attack:

- waiting for an ARP request;
- upon receipt of an APR request, a network transmission to the host of an erroneous ARP response that specifies the address of the network adapter of the attack station (erroneous ARP server) or the Ethernet address at which the ARP server will receive packets;
- receiving, analyzing, influencing and transmitting packets of exchange between interacting hosts (affecting the intercepted information);
- The simplest solution to eliminating this attack is to create a static ARP table as a file containing address information and install this file on each host within the segment.

8. Fake DNS-server on the Internet

As you know, 32-bit IP addresses are used to access hosts on the Internet, uniquely identifying each network computer. But for users, the use of IP addresses when accessing hosts is not very convenient and not the most obvious. Therefore, for their convenience, it was decided to assign all computers on the Network names, which in turn required the transformation of these names into IP addresses, since at the network level packet addressing goes not by names, but by IP addresses.

Initially, when there were few computers on the Internet, there was a special file (the so-called hosts file) to solve the problem of converting names into addresses, in which the names were assigned IP addresses. The file was regularly updated and sent to the Web.

As the Internet evolved, the number of networked hosts increased, and such a scheme became less efficient. Therefore, she was replaced by a new name conversion system that allows the user to obtain an IP address corresponding to a specific name from the nearest DNS server. This workaround is named Domain Name System, (DNS). A DNS protocol was developed to implement this system.

The algorithm for DNS service:

The host sends the IP address of the nearest DNS server to the DNS request, which specifies the name of the server whose IP address you want to find.

When receiving such a request, the DNS server looks for the specified name in its name database. If it and the corresponding IP address are found, the DNS server sends a DNS response to the host, which specifies that address.

If the name is not found in its name database, the DNS server sends a DNS request to one of the top-level DNS servers responsible for the domains. This procedure is repeated until the name is found or found.

As you can see from the above algorithm, in the network using the DNS protocol, it is possible to introduce an erroneous object – a false DNS server.

Because by default, the DNS service is UDP-based, which does not provide messaging tools, unlike TCP, which makes it less secure.

The following scheme of operation of the erroneous DNS server is possible:

- Waiting for a DNS request.
- Extracting from the received message the necessary information and sending to the host a false DNS response on behalf (from IP address) of the real DNS server and indicating the IP address of the false DNS server in that response.
- When a packet is received from a host, the IP header of the packet of its IP address is changed to the IP address of the fake DNS server and the packet is transmitted to the server. An fake DNS server is running the server on its own behalf.

➢ When a packet is received from a server, it changes the IP header of the packet to its IP address to the fake DNS server address and transmits the packet to the host.

The false DNS server for the host is the real server.

There are two possible options for implementing this attack.

In the first case, a prerequisite is the interception of a DNS request, which requires finding the attacker either in the path of the main traffic, or in the same segment with the DNS server.

In the second case, a directional storm of false prepared DNS responses to the attacked host is created.

On the Internet, when using an existing version of DNS, there is no acceptable solution to protect against a fake DNS server. You can drop the remote search engine and go back to the method with the hosts file, as it was before the DNS service appeared, but so far, this file can only include information about the most frequently visited addresses.

You can also use TCP instead of UDP to make this attack more difficult, although documentation does not always tell you how to do this, and TCP still does not provide complete security.

9. Connecting a False Route Host Using ICMP to Create an Fake Internet Router

Consider another attack related to the introduction of a false object in the DCS. Routing on the Internet is performed on a network layer (IP layer). To provide it in the memory of the network operating system of each host there are routing tables containing information about possible routes.

Each segment of the network is connected to the Internet at least through one router.

All messages addressed to other segments of the network are forwarded to the router, which, in turn, forwards them further to the IP address specified in the packet, while choosing the optimal route.

As mentioned earlier, there is an ICMP management protocol on the Internet, one of the purposes of which is to dynamically modify the routing table of end network systems. Remote routing management is implemented as a transmission to the host of the Redirect ICMP Message.

To perform this attack, you must prepare an fake ICMP Redirect Datagrams for the Host, where you specify the host address to which the route will be changed, and the IP address of the fake router. This message is then transmitted to the attacked host on behalf of the router.

This attack allows you to gain control over the traffic between that host and the server of interest to the attacker if the host and the attacker are in the same segment, or disrupt the host if they are located in different segments.

It is possible to protect against this influence by filtering passing ICMP-messages by the Firewall systems. Another way is to change the network kernel of the OS to prevent the response to the Redirect ICMP message.

10. Changing one of the subjects of a TCP connection on the Internet (hijacking)

TCP (Transmission Control Protocol) is one of the basic protocols of the transport layer of the Internet. It allows you to correct errors that may occur during packet transmission by establishing a logical connection – a virtual channel. This channel is transmitted and received packets with the registration of their sequence, is managed information flow, organized retransmission of distorted packets, and at the end of the session the channel is disconnected. The TCP protocol is the only basic protocol of the TCP/IP family, which has an additional message and connection identification system.

To identify a TCP packet, there are two 32-bit identifiers in the TCP header that also play the role of a packet counter.

Their names are Sequence Number and Acknowledgment Number.

To generate an fake TCP packet, the attacker needs to know the current identifiers for the connection. This means that it is sufficient for it, having selected the corresponding current values of the TCP packet identifiers for the given TCP connection, to send the packet from any host on the Network on behalf of one of the participants of the given connection, and this packet will be perceived as correct.

When finding a cracker and an attack object in the same segment, the task of obtaining the ID values is solved by network traffic analysis. If they are in different segments, you have to use mathematical prediction of the initial value of the identifier by extrapolating its previous values.

To protect against such attacks, it is necessary to use OS, in which the initial value of the identifier is really randomly generated. You must also use secure protocols such as SSL, S-HTTP, Kerberos, etc.

11. Flood of false TCP connection requests

For each TCP connection request received, the operating system must generate the initial value of the ISN and send it in response to the host. Since the Internet (IPv4 standard) does not provide control over the IP address of the sender of the message, it is impossible to track the true route traveled by the IP packet, and therefore, the end subscribers of the network can not limit the number of possible requests received per unit of time from one host. Therefore, a typical Denial of Service attack is possible, which will involve sending as many false TCP requests to the attacked host to create a connection on behalf of any host on the network. At the same time attack the network OS, depending on the computing power of the computer or – in the worst case – almost freezes, or – in the best case – ceases to respond to legal requests for connection (denial of service).

This is because, for the whole mass of fake requests received, the system must, first, store the information received in each request and, second, produce and send a response to each request

Thus, all system resources are "eaten up" by fake queries: the query queue overflows, and the system deals only with their processing.

A new type of attack has recently been reported on the Web. Instead of typical Denial of Service attacks, hackers overflow their corporate router packet buffer, not from single machines, but from as many as thousands of zombie computers.

Such attacks are capable of blocking channels up to and including T3 (44.736 Mbps) and several such cases have already been noted. The risk of attack becomes more important as more businesses use private VPN networks and other Internet technologies. After all, the failure of the channel with a public service provider will not just lead to the shutdown of individual users, but to the halt of huge corporations.

In this case, there are difficulties in determining the source of the attack – erroneous packets come from different unique IPs. "Zombie attack" is called the most difficult of the known. The lone victim is attacked by an entire army, and each zombie hits only once.

There are no acceptable methods of protection against such attacks in the IPv4 network, since it is impossible to control the message route.

To increase the reliability of the system, you can use as powerful as possible computers capable of withstanding the directional storm of erroneous connection requests.

12. Attacks that use network service implementation errors

In addition to these attacks, there are various attacks against specific platforms. example:

Land Attack – An IP packet is formed in which the sender's address matches the recipient's address. All Windows versions of Windows NT 4.0 Service Pack 4, are vulnerable to this vulnerability. When such requests are received, access to the system becomes impossible.

Teardrop and bonk attacks are based on bugs of OS developers in the module responsible for compiling fragmented IP packages. In this case, a block of negative length is copied or "holes" remain in the package after the fragments are assembled – empty, not filled with space data, which can also cause the OS kernel to crash. Both of these vulnerabilities are present in Windows95 / NT before Service Pack 4, including early versions of Linux (2.0.0).

WinNuke – Windows systems attack by sending TCP/IP packets with Out Of Band (OOB) flag to an open (usually 139th) TCP port. Today, this attack is outdated. Early versions of Windows95 / NT were freezing.

There are various other attacks specific to certain operating systems only.

13. WWW Attack

In the last few years, with the rapid development of WorldWideWeb, the number of attacks through the Web has increased significantly. In general, all types of attacks through the Web can be divided into two large groups:

- Attack on the client;
- Attack on the server.

In their development, browsers went very far from the original versions intended only for viewing hypertext. Browser functionality is constantly increasing, now it is already a complete component of the OS. In parallel, there are numerous security issues with the technologies used,

such as plug-ins, ActiveX elements, Java applications, JavaScript scripting tools, VBScript, PerlScript, Dynamic HTML.

Thanks to the support of these technologies, not only browsers but also mail clients and the presence of bugs in them, in the last year or two a large number of email viruses as well as viruses that infect html files (implemented on VBScript using ActiveX). Trojans are very common.

The event of the year was the release of the BackOrifice 2000 Cult of the Dead Cow hacker group, which, unlike the previous version, runs on WindowsNT and is also distributed in source texts, enabling anyone to create a clone of this program for their specific needs, probably cannot be detected by antivirus programs.

Server software security is mainly determined by the absence of the following types of errors:

- server errors:

errors that lead to a loss of privacy; errors that lead to denial-of-service attacks and errors that cause unauthorized code to execute on the server;

- errors in utilities;
- administration errors.

14. Reasons for the success of remote attacks

"What is invented by one person
can be understood by another," – Holmes.
A. Conan Doyle The Adventure of the Dancing Men

Use of unstable identification algorithms. Unfortunately, the interaction of objects on a virtual channel in a distributed CS is not a panacea for all problems associated with the identification of objects of the DCS. VC is a necessary but not sufficient condition for safe interaction. It is extremely important in this case to choose the identification algorithm when creating a virtual channel.

The basic requirement for these algorithms is the following: the interception of key information exchanged by DCS objects when creating VCs should not allow the attacker to obtain summary channel and object IDs.

However, in the basic identification algorithms used in the creation of VC in most existing network OS, this requirement is virtually ignored.

Lack of control over virtual communication channels. Distributed CS objects that interact across virtual channels may be subject to a typical denial of service attack. The peculiarity of this influence is that, acting by absolutely legal means of the system, one can remotely achieve a violation of its performance.

What is the reason for the success of this attack? In the absence of the necessary control over the connection.

The task of control is divided into two sub-tasks:

- control over connection creation;
- control over connection usage.

If the ways to solve the second problem are clear – usually the connection is broken by a timeout defined by the system – so done in all known network OS (but there is a serious problem of choosing a specific timeout value), then control over the creation of VC is quite difficult: In a system where static key information about all its objects is missing, it is impossible to separate false connection requests from real ones.

It is also clear that if one network interaction entity is able to anonymously occupy an unlimited number of channels due to a remote object, then such a system may be completely paralyzed by that entity.

Thus, if any object in a distributed system is able to anonymously send messages on behalf of another object (for example, routers do not check the IP address of the sender), it is virtually impossible to control virtual creation of connections.

Therefore, the main reason for the typical threat of "denial of service" is the lack of an acceptable solution to the task of controlling the message route.

Inability to control the message route. If the DCS does not provide control over the route of the message, then the address of the sender of the message is not confirmed.

Thus, the system will be able to work on behalf of any object by specifying a message in the header of another sender's address (IP Spoofing).

In such a DCS it is difficult to determine where the message actually came from, and therefore to calculate the coordinates of the attacker (the initiator of a unidirectional remote attack cannot be found on the Internet).

Lack of complete information about network objects. In a distributed system with a branched structure consisting of a large number of objects, there may be a situation where the necessary information, that is, the address of the given object, will not be available for access to a particular host.

Obviously, in a system of this type, there is a potential danger of entering an fake object and issuing one object at a time by transmitting an incorrect response to a search query.

No dedicated channel of communication between Internet objects. A global network cannot be built on the principle of direct communication between objects, because for each object it is impossible to provide a dedicated communication channel with any other object. Therefore, the Internet connects through a chain of routers, and therefore, messages passing through a large number of intermediate subnets can be intercepted.

Also, a large number of local Ethernet networks that use the "common bus" topology are connected to the Internet; In networks with this topology, it is easy to programmatically intercept messages.

Insufficient identification and authentication. In the basic protocols of exchange, identification and authentication of objects are virtually absent.

For example, in application protocols – FTP, TELNET, POP3, the user names and passwords are transmitted over the network as unencrypted open messages.

Use of unstable object identification algorithms when creating a virtual TCP connection. As already emphasized, TCP is the only basic transport layer protocol that has connection protection.

However, using the simplest object identification algorithm when creating a virtual TCP channel, especially when the simplest time-dependent TCP generation laws apply to network OSs, nullifies all attempts to provide channel and object identification when interacting with TCP.

No cryptographic protection of messages. The existing TCP / IP core protocols that provide network and transport interactions do not provide the ability to encrypt messages, although it is obvious that adding them to TCP did not pose any problems. The developers have decided to shift cryptographic protection tasks to higher-level

protocols, such as the application layer. The basic application protocols (FTP, TELNET, HTTP, etc.)

They also did not provide any encryption of messages. Just recently, a publicly available SSL application built into browsers has emerged, allowing both secure encryption and authentication of messages.

In conclusion, I would like to point out that all of the reasons described above, for which a successful implementation of the security threats to the DCS is possible, make the Internet unsafe. Therefore, all network users can be attacked at any time.

15. Virtual Private Networks

One of the most important tasks is protecting the flow of corporate data transmitted over open networks. Open channels can be securely protected by only one method – cryptographic.

The so-called dedicated lines do not have special advantages over the public security lines in terms of information security. The selected ones will be located at least in part in an uncontrolled area where they may be damaged or unauthorized.

The only real dignity is the guaranteed bandwidth of the dedicated lines, and not increased security. However, modern fiber-optic channels are able to meet the needs of many subscribers, and therefore the dignity is not always dressed up in a real form.

Of course it is natural to put on the firewall the task of encrypting and decrypting corporate traffic on the way to and from the external network. In order for such encryption/decryption to be possible, an initial allocation of keys must take place.

Modern cryptographic technologies offer a number of methods for this purpose.

After the firewalls have encrypted the closure of corporate data streams, the territorial location of the network segments is detected only at different rates of exchange with different segments. The rest of the network looks like a whole, and subscribers do not need to bring any additional security.

Probably, nowhere the word "virtual" has become as widespread as in the field of information technology: virtual memory, virtual machine, virtual reality, virtual channel, virtual office. This is due to the ability to

simulate the logic of the operation of the object so that for the user its (logical) behavior and properties will not differ from the real prototype.

Escape to the "virtual world" can be caused by, say, a fundamental inability to operate with a real object, economic considerations, or a temporary factor.

Virtual Private Networks (VPNs) are not only a hot topic for industry analysts, but are also receiving close attention from both Network Service Provider (NSP) and Intemet (ISP) providers and corporate users.

Infonetics Research expects the VPN market to grow more than 100% annually by 2002, reaching 12 billion. $ She also reports that 92% of major ISPs and 60% of total ISPs planned to provide VPN services by the end of 1999.

Before proceeding to the analysis of the causes that have caused such a rapid increase in the popularity of VPNs, it should be reminded that simple (corporate) data networks are built, as a rule, using leased (dedicated) public switched telephone networks (Public Switched Telephone Network – PSTN).

Over the years, such private networks have been designed to meet specific corporate requirements, resulting in branded protocols that support proprietary applications (though Frame Relay and ATM have recently become popular).

Dedicated channels allow for reliable protection of sensitive information, but the downside of the coin is the high cost of operation and difficulty in expanding the network, not to mention the possibility of connecting to it by a mobile user at an unpredictable point.

At the same time, modern business is characterized by considerable dispersion and labor mobility.

More and more users need access to corporate information through dial-up channels, and the number of employees working at home is also increasing. Western analysts predict that by the end of 1999, 80% of corporate users will have at least one laptop computer (of course, the projection of this prediction on Ukraine can only cause a smile, but sooner or later the Ukrainian economy, raped by progress, will have to adopt game rules dictated by industrialized countries).

Further, private networks are unable to provide the same business opportunities offered by the Internet and IP-based applications, such as product promotion, customer support or ongoing contact with suppliers.

Such online interaction requires the integration of private networks, which typically use different protocols and applications, different network management systems, and different communications providers.

Thus, the high cost, static and difficulties that arise when necessary to unite private networks based on different technologies, contradict with the dynamically developing business, its desire for decentralization and is a recent tendency to merge companies.

At the same time, there are, at the same time, devoid of these shortcomings of the public data network and the Internet, literally enveloping its "web" with the whole globe. However, they are also deprived of the most important dignity of private networks – reliable protection of corporate information.

Virtual Private Networking technology combines the flexibility, scalability, low cost and availability of virtually anytime anywhere Internet and public-facing networks with the security of private networks. VPNs are essentially private networks that use global public networks (Internet, Frame Relay, ATM) to transmit traffic. The virtuality, however, is that for corporate users, they appear to be dedicated private networks.

Let's look at the basic requirements for virtual private networks.

15.1 Compatibility

Compatibility issues do not arise when Frame Relay and ATM services are directly used by VPNs, as they are well suited for multi-protocol environments and are suitable for both IP and full IP applications.

All that is required in this case is the availability of an appropriate network infrastructure covering the required geographical area. Frame Relay Access Device (FRAD) or routers with Frame Relay and ATM interfaces are most commonly used as access devices. Numerous permanent or switched virtual channels can work (virtually) with any mix of protocols and topologies. It's complicated if a VPN is based on the Internet. In this case, the programs need to be IP-compatible. If this requirement is fulfilled, you can use the Internet as it is to build a VPN, providing the necessary level of security beforehand.

But since most private networks are multi-protocol or use unofficial, internal IPs, they cannot connect directly to the Internet without proper adaptation. There are many compatibility solutions available.

The most popular are:

- converting existing protocols (IPX, NetBEUI, AppleTalk, or others) into an IP protocol with an official address;
- converting internal IPs to official IPs;
- installation of special IP-gateways on servers;
- use of virtual IP routing;
- use of universal tunneling technique.

The first way, at least conceptually, is clear, so let's briefly look at others.

Converting internal IPs to official IPs is required if the private network is IP-based. Class B addresses that are in the range 192.168.0.0 – 192.168.255.255 are typically used for internal addressing, which allows 65536 nodes to be identified.

Address transformation for the entire corporate network is unnecessary, as official IP addresses can coexist with the internal switches and routers of the enterprise network. In other words, the server with the official IP address is still accessible to the private network client through the local infrastructure.

Most often use the technique of sharing a small block of official addresses by many users. It is similar to sharing a modem pool because it also relies on the assumption that not all users need Internet access at the same time.

There are two industry standards: Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT), which differ slightly. DHCP "leases" the node address for the time specified by the set administrator, while NAT translates the internal IP address to the official dynamically, during a session with the Internet.

Another way to make a private network compatible with the Internet is to install an IP gateway. The gateway does not transmit IP protocols to IP protocols and vice versa. Most network operating systems that use native protocols have IP gateway software.

The essence of virtual IP routing lies in the extension of private routing tables and address space to the infrastructure (routers and switches) of the ISP.

A virtual IP router is a logical part of a physical IP owned and operated by service provider. Each virtual router serves a specific group of users.

However, perhaps the best way to ensure compatibility is through tunneling methods. These methods, along with various encapsulation techniques, have long been used to transmit multiprotocol packet flow over a common line.

Currently, this proven technology is optimized for Internet-based VPNs.

The main components of the tunnel are:

- the initiator of the tunnel;
- routed network;
- tunnel switch (optional);
- one or more tunnel terminators.

Tunneling must be performed at both ends of the through channel. The tunnel should begin with a tunnel initiator and end with a tunnel terminator. The initialization and completion of tunnel operations can be performed by various network devices and software. For example, a tunnel can be initiated by a remote computer that has a modem and VPN software needed, a corporate branch front-end router, or a service provider's network access hub.

To transmit packets other than IP network protocols over the Internet, they are encapsulated into IP packets by the source.

The most commonly used method of creating VPN tunnels is to encapsulate the NOT IP packet into the PPP (Point-to-Point Protocol) package, followed by encapsulation into the IP packet. Recall that the PPP protocol is used to connect point-to-point, for example, to communicate with the client server.

The process of IP encapsulation involves adding a standard IP header to the original packet, which is then considered as useful information. The corresponding process at the other end of the tunnel removes the IP header, leaving the original package unchanged.

The PPP protocol provides service at level 2 of the OSI reference model, so this approach is called level 2 tunneling (L2 Tunneling Protocol – L2TP).

Today, the Point-to-Point Tunneling Protocol, developed by 3Com and Microsoft, which comes with Windows 95 and Windows NT operating systems, has become quite widespread.

Because tunneling technology is quite simple, it is also the most cost-effective.

15.2 Security

Providing the right level of security is often a key consideration when considering a corporation's ability to use a Intemet-based VPN. Many IT managers have become accustomed to the inherent privacy of private information security networks and consider the Internet as too "public" to use as a private network.

However, if the necessary steps are taken, Intemet-based virtual private networks can become more secure than PSTN-based VPNs.

If you use English terminology, there are three "P", the implementation of which together provides complete protection of information:

- Protection – protection of resources by means of firewalls;
- Proof – authentication (integrity) of the package and authentication of the sender (confirmation of the right of access);
- Privacy – protect sensitive information through encryption.

All three P's are equally relevant to any corporate network, including VPN. In purely private networks, it is enough to use simple passwords to protect the resources and confidentiality of information.

Once a private network connects to a public network, none of the three P's can provide the necessary protection. Therefore, for any VPN, firewalls must be installed at all points of its interaction with the public network, and packets must be encrypted and authenticated.

Firewalls are an essential component in any VPN. They skip only authorized traffic for trusted users and block all other traffic. In other words, all attempts to reach unknown or untrusted users intersect.

This form of protection should be provided for each site and user, since the lack of it anywhere means the absence of everywhere.

Special protocols are used to ensure the security of VPNs. These protocols allow hosts to "agree" on the encryption and digital signature technique used, which preserves the confidentiality and integrity of the data and performs user authentication.

Microsoft Point-to-Point Encryption (MPRE) encrypts PPP packets on a client machine before sending them to a tunnel. The 40-bit key version comes with Windows 95 and Windows NT (there is also a 128-bit key version). The encryption session is initialized during communication with the PPP tunnel terminator.

Secure IP (IPSec) protocols are a series of previous standards developed by the Internet Engineering Task Force (IETF). The group

offered two protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP).

The AH protocol adds a digital signature to the header that authenticates the user and ensures the integrity of the data by tracking any changes in the transmission process. This protocol only protects data, leaving the IP address packet unchanged.

ESP, on the other hand, can either encrypt the entire packet (Tunnel Mode) or only the data (Transport Mode). These protocols are used both individually and in combination.

Security management uses the industry standard RADIUS (Remote Authentication Dial-In User Service), which is a database of user profiles containing passwords (authentication) and permissions (authorization).

Security measures are not limited to the following examples. Many router and firewall vendors offer their solutions. These include 3COM, Checkpoint and Cisco.

15.3 Availability

Availability includes three equally important components: service time, bandwidth, and delay time. Service time is the subject of a contract with a service provider, and the other two components are related to the elements of Quality Of Service.

Modern transportation technologies allow you to build VPNs that meet the requirements of virtually all existing applications.

15.4 Controllability

Network administrators always want to be able to manage end-to-end, corporate networking, including the part that relates to a telecommunications company, and it turns out that VPNs provide more power than conventional private networks.

Typical private networks are administered from border to border, that is, the service provider manages the network to the front routers of the corporate network, while the subscriber manages the corporate network to the WAN access devices.

VPN technology avoids this peculiar separation of "spheres of influence" by providing both the provider and the subscriber with a unified system for managing the network as a whole, both its corporate part and the network infrastructure of the public network.

The enterprise network administrator has the ability to monitor and reconfigure the network, manage front-end access devices, and determine the network status in real time.

REFERENCES

1. Крол Эд. Все об Internet: Руководство и каталог. Пер. с англ. С.М. Тимачева. Киев: BNV, 1995. 591 с.

2. Вертузаев М.С., Юрченко О.М. Защита информации в компьютерных системах от несанкционированного доступа. Київ: Европ. ун-т, 2001. 320 с.

3. Ярочкин В.И. Основы защиты информации. Москва: Летописец, 2000. 150 с.

4. Зепкды П.Д. Теория и практика обеспечения информационной безопасности. Под ред. Москва: Яхтсмен, 1996. 302 с.

5. HackZone- территория взлома (httn://www.hackzone.ru).

Information about the author:
Domnich V. I.
Candidate of Technical Sciences, Professor,
Head at the Department of Automated Process Control
of the V. I. Vernadsky Taurida National University