Research Focus
Volume 1, Issue 2, 2019, p. 27-40
ISSN: 2668-4675
www.researchfocus.org

Photo by Armando Castillejos on Unsplash

Providing Security for Client-Server Applications

Madalina-Eleonora GHEORGHE
Computer Science for Business, Romanian-American University, Romania

Abstract

In the context of digital evolution, the security of client-server applications is a matter of great importance in the Internet and intranet networks. Ensuring network security is done through a multitude of security services such as authentication, authorization, availability, confidentiality, integrity, and non-repudiation. Their implementation is accomplished through different security models, such as arborescent and stratified. Some of the security techniques are physical security, logic, public-key cryptography, private key cryptography, digital signature, digital certificate, hash technique, bookmarks, and security policies. Some of the aspects studied are vulnerabilities, types of attacks: local, remote, active, cryptographic and security protocols.

Keywords: security, client, server, network

Introduction

Security services are a category of network services offered as part of the operating system in multiple types of software. These are either part of certain programs or are offered independently. Also, some of these services can also be deployed directly into the hardware circuitry (Blockmon, 2018).

Applying security measures is justified for sensitive data, which must indeed be protected because their implementation is expensive in terms of prices and resources.

The choice of services is conditioned by the nature of the information and its costs. Choosing an effective security strategy involves preventing exposure risks and covering vulnerabilities in order to tailor the security solution to the needs of each network and reduce costs.

The paper contains a brief presentation of security models and their application at the network level. According to Reinhardt Bota, some of the security services are (Information Security in the Client/Server environment, 1997):

- Authentication - a mechanism for identifying a human user, equipment or software program
- Authorization - the framing, delimitation of a user's access to data or programs, after the authentication process ends successfully
- Availability - the service that manages users' access to other services through groups
- Privacy - the protection of private data
- Integrity - refers to keeping the data unchanged
- Irrelevance - the prevention of impersonating another account to perform fraudulent actions

Factors and delimiters

Some of the factors that affect the cost of Security services are physical transmission medium, the performance of network equipment, the performance of packages (applications / operating system) software used, and Data Security Encryption Level.

According to Scripcariu (Luminita Scripcariu, 2008) , it is important to prioritize and classify data stored or transferred to the network, i.e. the information, for proper security.

According to the ownership criterion, the information is divided into user information and network information. By the criterion of importance, the information can be public and private. By location, the information can be internal or external. According to the field of use, there are different types of data (information): advertising, commercial, educational, entertainment, with or without payment, government, military. Each of these types of data and information can have different security models that are applied to them.

I. Security Models

A computer network is a system of interconnected resources, used by a lot of users, with specific rights to use them, and network security should be provided modularly, on the three levels, i.e. information, logical, physical (Oracle, 2013).

In the security-centered security or information model, the layers represent security levels. They offer protection to the subject that will be secured. Each level gives another layer of isolation to the subject and makes it harder to access in unpredictable ways. This model is called "onion model" in the literature because each level offers added security:

- Level II - Integrity of information
- Level SI – Suppressing the information
- Level SLS - Logical Security of Services
- Level SLA - Logical Security of Access
- Level SF - Physical security

The layered security model described above is used with maximum network node efficiency. Communication processes involve at least two nodes, as well as transmission paths between them. As a result, security must be evaluated in each node as well as in each flow or flow path in the network.

Another type of model used for security services is the "tree type”. This model should be applied to networks where distributed resources are deployed on multiple servers in the network. Information is transmitted from the source node to the destination node using network nodes

and different physical communication paths, whether they are used or not. The “weakest” element on the transfer path (communication channel or node) determines the degree of security of the data transfer process in the network will be given by the "weakest" segment of the transfer path. As a result, all segments used in the transmission path need to be secured to increase network security.

In the arborescent security model, the client is considered the root in the diagram, the servers are terminal nodes, and communication equipment is intermediate nodes. At each node, the first security centered model of the subject can be applied. The links between the nodes are the physical communication paths that can be wired or radio. In the case of networks with redundant mesh topology[1], it is difficult to identify the "tree" of communication, but it can be imposed by strict routing decisions on a certain path in the network.

Defining a network security metric is recommended for routing a specific security packet. Unlike the usual metrics used by routing algorithms, the security metric must include the security level provided by the nodes delineating a graph arc. It is also useful to use oriented graphs and separate representation of up-link and downlink links between two network nodes in asymmetric communications with different transmission media and technologies. The security metric will be based on the security risk that a particular element of the network graph shows. The decision on the optimal transmission security route will aim to reduce the security risk to the level required by the maximum admissible costs. The security degree of a packet can be expressed by optional security bits included in the package header.

The utility of this model is enhanced in the analysis of distributed attacks, launched across multiple nodes, in which it is difficult to identify the attacker.

In the field of communications networks, various security models have been proposed by software companies and software vendors for different application areas that require the protection of privacy or confidential information (for example, the HIPAA “Health Insurance Portability and Accountability Act”, the GLBA “Gramm-Leach-Bliley Act”, as well as payments through PCI DSS - Payment Card Industry Data Security Standard).

[1] Type of networking where all nodes cooperate to distribute data amongst each other.

Physical security

Physical security is the external level of the security model and generally consists of the "under-key"[2] protection of computer equipment in an office or other premises, as well as the provision of security and access control.

Because a lot of attacks starts from within the network, communications networks have a high degree of difficulty in managing them effectively, being vulnerable to internal and external attacks. This degree of complexity is generated by multi-organization management for the same network, geographic spread, diversity of equipment types, operating systems, and a high number of entities in the same network.

Employees who administer the network must comply with and ensure the rules of good functioning and physical security delineated by the security policy. Thus, equipment and cables used in the network must be mounted on the wall to protect them, in places that are not used frequently, in order to avoid damage either intentionally or accidentally. Servers should be located in closed rooms with restricted access to protect them from unauthorized physical access and the equipment must be protected from electrical disturbances by the use of uninterruptible power supplies (UPS), which ensures the continuous operation of highly important equipment. Physical access must be secured through various equipment, such as key devices, cards and access codes, biometric and motion sensors (voice, fingerprints, retina/face, signature, hand, etc.).

Physical security can be ensured by proper network space provisioning, physical access control, restriction, and video monitoring, Intrusion Detection System (IDS) from unattended areas with Remote Alarm Indicator (RAI).

Physical security measures of the network are established on the basis of security vulnerability and security risk analysis of the network, based on the security policy adopted and implemented by the management group using different software and hardware.

[2] Locked away safely

Logical security

Logical security refers to the protection of logical access to network resources and services. This is achieved through software tools and facilities that ensure the control of access and use rights.

There are two great levels of logical security: (1) Access logic security (SLA) that refers to system/network access, user account, and documents (files) and (2) Service Logic Security (SLS) that includes access to system/network services based on waiting lists, disk entry/exit, control, and management. Service Control (CS) monitors and reports service status, activates or disables the services provided by the system and the network. Service Rights (DS) determine who and how to use a particular service.

Security of information

Cryptography is a branch of mathematics, which deals with the secrecy, authentication, and restriction of access to information in a computer system. Cryptography uses mathematical methods, based, for example, on generating large numbers (Andersson, 2009).

Encryption is the process of converting the original information (plain text - plain text - M) into a text that cannot be read by people (ciphertext - C) using an encryption key (KE) (SecureBlackbox, 2006).

Decryption is the inverse of the encryption, that is, the transition from the unintelligible ciphertext to the original text using a key (KD).

Security Policies

These are the principles underpinning the security of a communications network and are expressed as a set of rules and practices. Thus, the needs of each category of users with regard to network resources and access rights, whether inside or outside, using the wired structure or wireless access to the network, must be established. It also needs to be established which users really need access to the public Internet network. All these aspects are dealt with within the access policy.

A breach in the security of any network is the connection to the Internet and to the public network in general because it acts on attacks from outside the network. Clear principles are needed to secure the interfaces between the public and the private network. The principles according to which Internet access routes are secured and rights granted in this respect constitute the Internet-Acceptable Use Policy (I-AUP).

The user-name and password authentication method implies applying passwords for accepting, managing, and changing passwords within the password management policy.

Access rights to the network must be differentiated in terms of access to documents and their rights (reading, writing, modification or deletion).

Knowing in detail all the equipment that connects to the network and the guarantees offered by each user is the premise of right decisions on the privileges or restrictions that are imposed on each case (connection policy). The denial of network access for those entities for which the intention to attack is proven through traffic monitoring is a major force measure, which is necessary to keep the network operating safely.

Security vulnerabilities are caused by various factors, including not updating operating systems, antivirus programs, or other security programs or modules. Periodically it is necessary to install the latest versions of software, to update the databases with newly discovered viruses or other recently identified forms of attack. Also, periodically, staff involved in network security should be trained to know any new risks to which the network is exposed and the procedures to be followed to resolve problems. The different network equipment needs to be periodically reviewed to determine whether they meet network security needs at a particular time, including passwords, access control lists, MAC addresses, encryption keys.

Encryption of information is required as the last measure to ensure transmission secrecy when an intruder manages to download packets from the private network. Also, encryption is a measure of security with regard to the secrecy of special information that can be attacked by outside and within the network. The principles of information security are included in the information protection policy.

Virtual Private Networks (VPN) are a good security solution, adopted primarily by companies with multiple locations spread over a wide geographical area. Remote access often presents high-security risks caused by attack attempts by people outside the company, and security is

required based on clear principles of remote access rights and restrictions and security tactics which have to be adopted according to the remote access policy. Specific security policies can be set for each network service (e-mail, file transfer, network user information, etc.).

Security rules may be binding or optional, resulting in several categories of security provisions:

- Mandatory provisions resulting from agreements, regulations, and laws, expressed in detail, as many specific elements, depending on the field of use, are intended to provide reliable confidence in a communications network or a particular entity (server, service, program, etc.).
- The recommended though non-binding, provisions are motivated by the serious consequences of not applying them. For best network security, they must be considered as mandatory, although their deployment costs are generally high. For example, it is not required to run antivirus programs or install any security patches from operating systems. all this involves some additional costs (price, system memory, processing time), but in a network, each unsecured node can be a gateway for attackers.
- Informative provisions have the role of alerting users to the existence of vulnerabilities (for example, not updating virus lists for antivirus programs), the risks and consequences of security breaches of systems and networks.

II. Vulnerabilities and attacks

Because a communications network is a complex, heterogeneous system with many users, it is a convenient area for various attacks. Therefore, security is a vital operational objective of any communications network.

The computer networks of the various organizations are used both to communicate between employees and to external communications so that they can no longer be isolated and must be secured at the level of the public and private network access interfaces.

Vulnerability of networks

Depending on the vulnerabilities of the communications network they can exploit, attacks can be manifested in many ways, for example, unauthorized access to the network or its resources inside or outside the organization; attempts to disrupt or interrupt the physical functioning of the network; modifying or destroying information, that is, attacking the physical integrity of data Other examples of attacks are the attempts to interrupt or overload network traffic by transmitting a large number of packets to one or more flood nodes, soft attacks on network equipment that concentrate and direct flows into critical nodes (switch, router , access point etc.) by modifying configuration files and access rights set by authorized personnel. Take over and unauthorized use of information, that is, breach of confidentiality and copyright is also a form of attack.

Types of attacks

Taking into account where they run, attacks can be local (local), remote (remote). Another classification of attacks on communications networks, depending on how they act as a source and destination, attacks can be centered on a single entity (for example, a particular server is attacked on a single device), or can be distributed (launched from multiple locations or multiple cars simultaneously).

Distributed attacks make it difficult to identify and locate the authors, and their effects are maximized by attacking the network in multiple nodes simultaneously.

According to the attacker's interaction with information obtained from a successful attack, the attacks are active or passive and it is hard to say which one has a higher risk. At first glance, the most dangerous are the active attacks. However, in the passive attack encryption keys are taken without the key server to figure out which keys are compromised, thus all the information encrypted with those keys becomes completely unprotected.

Although there are no solutions that are able to protect the network from any kind of attack, there are some security systems that can greatly reduce the chances and effects of attacks. It is necessary to develop a security policy appropriate to each network, to apply it simultaneously with user education and to adopt security, software or hardware solutions that are suited to the vulnerabilities and attack risks specific to each network.

III. Protocols and security servers

TCP/IP Protocols

Internet services are based on the exchange of messages between a source and a recipient. The principle of communication is inspired by the postal system. The data unit thus obtained is called 'packet', by analogy with the regular postal system.

The Internet Protocol (IP) provides packet delivery only if there are no errors in network operation. If a message is too long, the IP requires its fragmentation into multiple packages. The transmission of IP packets is done between host computers and not directly between application programs. For these reasons, the IP protocol is complemented by another one, the TCP (Transmission Control Protocol), which makes fragmentation and ensure the correct transmission of messages between users. The packets of a message are numbered, making it possible to check their receipt in the form in which the long, multi-packet messages have been transmitted and reconstructed.

Protocols are grouped by levels, following the principle of stratification. The protocols are designed so that the N level of the destination receives (without modification) the object transmitted by the level N of the source. In order to comply with this principle, the definition of any protocol has to establish two aspects, the format of the data units being manipulated, and the possible actions of the protocol entities that compete to achieve the protocol-specific services.

IPv4 Protocols

Data is sent as a block of characters, called datagrams or packages. Each packet is composed of a small set of bytes, called ‘the header’ followed by the actual data that forms the contents of the package. Upon arrival at the destination, the data transmitted in the form of distinct packets are reassembled into logical units of file type, message, etc. The internet switches the packets on different routes from source to destination, so it is called a “packet switching network”.

There are three distinct ways to connect two gliders using the IP protocol. The two computers can be in the same local area network (Ethernet or Token Ring[3]). In this case, the packets are encapsulated in the packets used by the LAN protocols[4]; The two computers are directly linked by a serial line. IP packets are transmitted using one of the SLIP (Serial Line Internet Protocol) protocols, such as CSLIP (Compressed SLIP) or PPP (Point-to-Point Protocol). If the two computers are each connected to a local network, the telephone line links the two LANs via bridges; IP packages can be encapsulated within other packages used by other network protocols.

TCP/IP Security

Connecting a computer to the Internet generally involves using the UNIX[5] operating system and the TCP/IP protocols suite. These components have their own security issues highlighted in previous sections of the book. Internet access also involves the use of a set of dozens of services, programs, with many security issues, either due to software mistakes or due to the failure to incorporate the right security features. In general, for a user to be able to take the appropriate security measures when connecting to the network, he/she must understand how the UNIX operating system works with the Internet. That is the security issues associated with TCP and IP.

Firewall

For computer science, perhaps the easiest way is to first describe what a firewall is not: a firewall is not just a router or a host computer that provides network security (Loza, n.d.). Broadly speaking, a firewall (sometimes called a security bridge) is a system that requires a policy of access control between two networks. A firewall is the implementation of this policy in

[3] Local area network in which a node can only transmit when in possession of a sequence of bits (the token), which is passed to each node in turn.
[4] Standards that define how data is ultimately transferred from one system to another
[5] Proprietary operating system

terms of network configuration, one or more host and router systems with special functions, other security measures, such as cryptographic authentication of clients.

As Justin says (WIlingwood, 2015), because a firewall is disposed at the intersection between two networks, it can be used for purposes other than access control. For example, it can be used to monitor communications between an internal network and an external network. A firewall can monitor the services used and the amount of data transferred through TCP/IP connections between its own organization and the outside world in another example, a firewall can be used to intercept and record all communications between the internal and external networks. A leased line that allows speeds of up to 128 Kbps, assuming 100 percent of the time would transfer about 1.4GB per day, which would allow for a few days to run on a single digital magnetic tape 8mm

If an organization has several geographically separate networks, each with a firewall, it is possible to program these firewalls to automatically encrypt the contents of the packets transmitted between them. In this way, on the Internet, the organization can create its own private virtual network.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) are a complement to firewall activity in the security of a communications network and consist of passive solutions for analyzing, classifying, and reporting unwanted network events.

IDS systems detect network attacks, alert management staff and eventually trigger response actions, such as quarantining certain processes until the situation is clarified. There may also be false alarms, but the procedures applied in the first phase will only delay some transmissions (Rozenblum, 2001).

VPN - Private virtual networks

A VPN is a private communications network commonly used by one or more organizations to communicate in a confidential way through a public network (Mason, 2019). VPN traffic messages can be transmitted through the infrastructure of a public data network, such as the Internet, using standard protocols, or through a private network of the Internet service provider.

VPN is a cost-effective solution so that different organizations can provide access to the internal network for remote employees and collaborators. The term VPN describes two ways to address the problem of private networks that support a public network from the point of view of accessibility. VPNs built between several LANs (LAN-to-LAN VPNs, also known as Site-to-Site VPNs) that connect to a central node several different LANs at a distance some others but that are part of the same intranet, so as to ensure connectivity between them. Remote Access VPNs that provide remote access to a private network, for example, for mobile Internet users. At the transport level, several security protocols have been imposed, such as Secure Socket Layer (SSL), which ensures authentication and integrity of TCP-based applications but has a major drawback to lack of flexibility and application-level dependence; TLS (Transport Layer Security), that has developed as an alternative to SSL that solves most of its inconveniences.

Conclusions

There are many issues of access control and network security that need to be considered in implementing and maintaining a client-server system. Although there are a large number of tools for security features, they are significantly less for this type of system.

To avoid possible security breaches, the security of storage and data transfer channels, the security of data encryption and accessibility to the public should be analyzed.

References

Andersson, F. (2009, 9). *Designing a Secure Client-Server System.* Retrieved from Chalmers Publication Library: http://publications.lib.chalmers.se/records/fulltext/116816.pdf

SecureBlackbox. (2006). *Securing Your Client-Server or Multi-Tier Application* . Retrieved from https://www.secureblackbox.com/kb/articles/Securing-client-server-app.rst

Oracle. (2013). *Client-Server Security.* Retrieved from Oracle: https://docs.oracle.com/cd/E35310_01/E35309/html/Security.html

Information Security in the Client/Server environment. (1997, 5). Retrieved from Academia: https://www.academia.edu/850783/Information_security_in_a_client_server_environment

Blockmon, R. (2018). *What Is a Client-Server Network? - Definition, Advantages & Disadvantages.* Retrieved from Study: https://study.com/academy/lesson/what-is-a-client-server-network-definition-advantages-disadvantages.html

Luminita Scripcariu, I. B. (2008). *Securitatea retelelor de comunicatii.* Retrieved from Universitatea Tehnică "Gh. Asachi" din Iași: http://telecom.etc.tuiasi.ro/telecom/staff/lscripca/SECURITATEA%20RC%20LSCRIPCARIU.pdf?fbclid=IwAR2LCtFFLx9k-Vo4THgNb241nZrzRfeaMGCExOCTZ-z1bDih4RtqNVuL7DE

Wllingwood, J. (2015, 3 5). *DigitalOcean*. Retrieved from 7 Security Measures to Protect Your Servers: https://www.digitalocean.com/community/tutorials/7-security-measures-to-protect-your-servers

Loza, C. (n.d.). *Differences Between a Firewall and a Proxy Server*. Retrieved from azcentral.: https://yourbusiness.azcentral.com/difference-between-firewall-proxy-server-20024.html

Rozenblum, D. (2001, 8 9). *Understanting Intrusion Detection Systems.* Retrieved from Sans: https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337

Mason, J. (2019, 2 26). *thebestvpn*. Retrieved from VPN Beginner's Guide: https://thebestvpn.com/what-is-vpn-beginners-guide/

Please cite this article as:

Gheorghe., M. (2019). Providing Security for Client-Server Applications. Research Focus, 1(2), 27-40. DOI: https://doi.org/10.36068/1.12

Research Focus. International Open-Access Scientific Journal for Students and Graduates Research

ISSN: 2668-4675