Network Security Issues in Regard to OSI Reference Model Layers

Marko Martinović
College of Slavonski Brod

NETWORK SECURITY ISSUES IN REGARD TO OSI REFERENCE MODEL LAYERS

Marko Martinović*, Dino Lovaković and Tomislav Ćosić

College of Slavonski Brod, Dr. Mile Budaka 1, 35000 Slavonski Brod, Croatia

** Corresponding author e-mail: marko.martinovic@vusb.hr*

Abstract

Today, almost all aspects of what we regard as data-in-storage and data-on-move is connected. Entire organizational infrastructure is networked and capable of inter-communication. Such capabilities offer easy reach and focus on data, which is considered a primary value to any organization or institution that possesses it.

However, with the need for high data and communications availability also comes a potential risk. Various threats can compromise and breach data integrity and confidentiality by finding a way into or "taping" regular network channels.

Computer networks based on TCP/IP stack use various layers of communication and underlying protocols respectively.

Such design can provide independent fault tolerance and ensures compatibility of equipment made from different vendors as they all adhere to open standards.

Here, we will address the issues of most common security threats on Layers 2, 3 and 4 of the OSI model, and their DoD model counterparts, as they are, by far, the most targeted by todays potential threats.

Mitigation techniques and security policies will also be mentioned as they are vital part of both data confidentiality and integrity.

Keywords:
Network, security, OSI Model, IP protocol, security issues

1. Introduction

Any network today relies on networking devices such as routers and switches. These devices form a network itself and enable creation of communication channels between devices and end users.

In their process of inter-communication, these devices use protocols which have the role of language necessary for understanding. Most of the common protocols used are developed in an open manner and adhere to certain standards, which, in return, enable devices to communicate regardless of vendor or country of origin.

Through the development of layered model, with each layer being interdependent of adherent layers, standards establishing the communication framework emerged. Example is ISO's theoretical OSI layered model, while in practice, we encounter US DoD's IP practical model.

OSI communications model consists of seven layers which are Application, Presentation, Session, Transport, Network, Data link and Physical. Each layer houses its own protocols which cooperate in sending and receiving user and application data and passing it up and down the stack.

Their equivalents in IP model are Application layer, Transport Layer, Internet Layer and Network Interface layer, respectively.

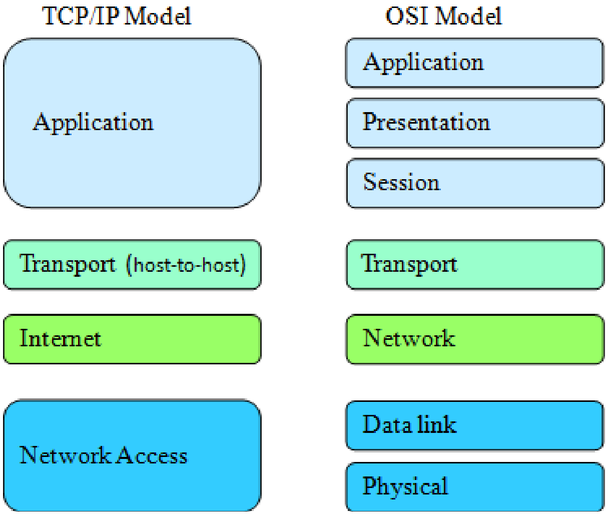


Figure 1. OSI and IP models[1]

In data protection and security, steps have to be taken to ensure secure means of data transportation between two or more endpoints.

2. Methods of protection

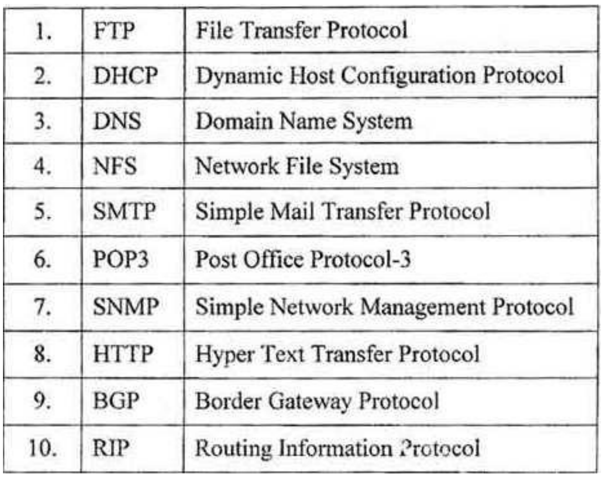
IP model's Application layer incorporates functions of Application, Presentation and Session layers in OSI model. Therefore, its purpose is to handle users input and application raw data values, which is the first step of communication.

Protocols domesticated on this layer are HTTP and HTTPS, POP, SMTP and IMAP, IRC, FTP and SFTP. Of course, number is quite large and, therefore, not all are listed [2].

Data protection of Application layer relies primarily on inspection of data in transit using Application layer firewalls. Such devices filter traffic primarily by application data type and those types of devices are considered application-aware.

Ability of determining source and destination of data, application that uses it and preprogramed rules of communications, such types of devices can quickly disseminate arbitrary traffic and the potential malicious payload that lies underneath such as viruses, worms or simply a non-compliance to defined criteria.

The ability to consider and inspect traffic as a whole, throughout separate communications channels, is what gives Application layer firewalls an edge over devices that filter traffic on underlying layers of the OSI model, but also carries a need for greater quantity of computational resources.



1.	FTP	File Transfer Protocol
2.	DHCP	Dynamic Host Configuration Protocol
3.	DNS	Domain Name System
4.	NFS	Network File System
5.	SMTP	Simple Mail Transfer Protocol
6.	POP3	Post Office Protocol-3
7.	SNMP	Simple Network Management Protocol
8.	HTTP	Hyper Text Transfer Protocol
9.	BGP	Border Gateway Protocol
10.	RIP	Routing Information Protocol

Figure 2. Application layer protocols [3]

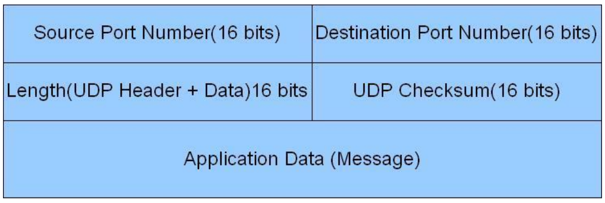
On the Transport layer of the IP and OSI models, most common protocols are TCP and UDP. These protocols are in charge of separation of data depending of the source and destination ports and application using it.

On this layer, initial segmentation of data is done and each segment or datagram, whether TCP or UDP, has an Transport layer header attached to it before its passed down the stack to a layer beneath.

Regardless of differences between TCP and UDP, and underlying mechanics, Transport layer header always contains source and destination port number.

Devices that filter traffic on Transport layer depend mostly on this given data to successfully deny, reject or allow traffic flow to a certain application or service port number.

All popular services have well known or introduced port numbers and by inspecting and matching the packet construction and payload, Transport layer firewalls can quickly differentiate between legitimate or allowed and illegitimate or arbitrary traffic and make a decision based on those criteria[4].



Source Port Number(16 bits)	Destination Port Number(16 bits)
Length(UDP Header + Data)16 bits	UDP Checksum(16 bits)
Application Data (Message)	

Figure 3. Transport layer header of the UDP datagram along with data[5]

Network layer of the OSI model, also known as IP models Internet layer is the layer where Internet traffic routing takes place. On this layer, TCP and UDP segments that are passed down get IP header attached and thus become referred to as packets. On the Internet layer, IP addresses play a major role in packet routing and relay.

Filtering packets is primarily done in that regard as well, by usage of source and destination IP addresses in each packets header (such as packet-per-packet filtering).

Network layer filtering gives the ability of allowing, dropping or denying traffic originating from one or more addresses and termed for single or multiple destinations.

Since the Network layer handles packet delivery across Internet and other IPv4 based networks, such mechanism allows the discardment of packets before sending them to higher layer (e. Transport) and thereby reducing the overhead of upper layer process and filtering.

IPs Network access layer incorporates first two layers of the OSI model; Physical and Data link, respectively. Main characteristic of this layer is that it is comprised of both physical and logical aspects of networking. Such setup allows for unified standards, and indirectly, better protection of local networking space.

Just like IP addresses are used in determining source and destination on Internet layer of IP model, in Network access layer, a concept of MAC addresses is used.

As packets are passed down to this layer, a header and a trailer are attached and thus a packet becomes referred to as frame.

Most often, communication is done via frame switching as each client's network interface card has a unique MAC (Media Access Control) address which represents them in a network.

Physical control of the network is accomplished through challenge and filtering of allowed devices upon connection initiation.

A type of firewall control can also be included in communication process which enables the setting of allow or deny decisions based on source and destination MAC addresses.

Pseudo-physical separation can also be implemented via the usage of VLAN technology, which allows grouping and isolation of chosen hosts on the network, based on various criteria such as location or purpose[3].

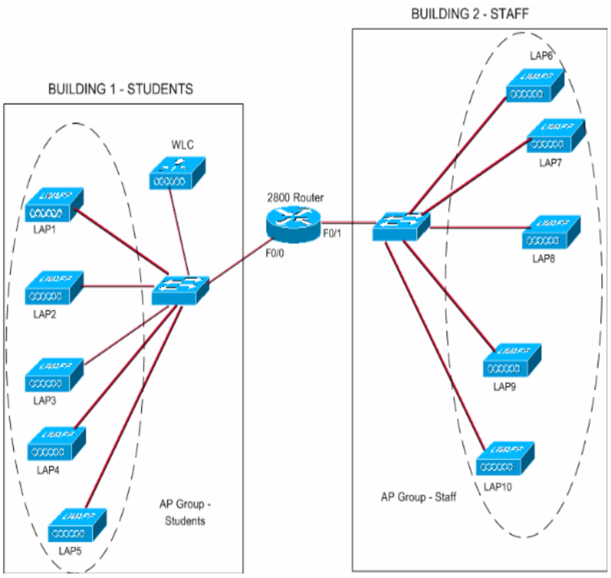


Figure 4. Topology of VLAN technologies [7]

3. Viewing the results

By using suggested methods of protection on various layers of the OSI or IP models, a certain level of granularity is achieved in network security matter that goes from more general security measures to more specific ones.

All this is achieved for the purpose of enhancing the security through combination of multiple layers of security, usually known as “Defense-in-Depth” which states that: “even if one measure fails, another one will take its place”.

Along with security benefits, this type of administration allows the avoidance of congestion by permitting only traffic that passed the entire security infrastructure and also cuts down on resource overhead by stopping various threats as low as possible, without sending it up the stack.

4. Conclusion

While security issues represent a significant threat to today’s enterprise environments, both from internal and external subjects, well placed preemptive security measures can minimize or almost completely mitigate large portions of risk involved with the ability to keep data access allowed purposely for legitimate use.

References

[1] networklessons.com (retrieved 21.07.2014)

[2] Cole E., Krutz R and Conley J, “Network security bible”, Wiley publishing, ISBN 0-7645-7397-7

[3] highteck.net (Retrieved 26.07.2014)

[4] Gibson D, “Security+ Guide”, Gibson, ISBN 1-4637-6236-4

[5] tcp-udp.de (Retrieved 28.07.2014)

[6] Barker K., Morris S., “CCNA Security Guide”, Ciscopress, ISBN 1-5872-0446-0

[7] cisco.com (Retrieved 09.08.2014)