International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 2

Popularly Used Security Protocols on All Layers of Network Communication

Arpana Chaturvedi
Assistant Professor, JIMS, Delhi

Poonam Verma
Assistant Professor, JIMS, Delhi

ABSTRACT

TCP/IP is used to provide network communication throughout the world. Now-a-days all organization are dependent on Internet and perform all sort of communication. Security controls exists for network communication at each layer of the TCP/IP Model. Even as this communication contains a lot of secret information which has to travel securely, more protection is required. Having developed and identified various security mechanisms for achieving network security, it is essential to decide where to apply them; both physically (at what location) and logically (at what layer of an architecture such as TCP/IP). Security professionals must understand the issues and risks associated with these transactions if they want to provide viable and scalable security solutions for Internet commerce. In this paper, we have discussed various security protocols existing in all layers and what are the best protocols which have to be implemented to perform any communication on the network.

Keywords: *Security, TCP/IP, HDFS, Hadoop, OSI Model*

1. Introduction:

TCP/IP communication consists of four layers. When a user wants to transfer data across the networks, the data is passed from the highest layers through intermediate layers to the lowest layer. During communication each layer adds information. At each layer logical unit composed of header and payload. The payload consists of the information passed down from the previous layer. The header contains layer specific information like addresses. The data produced by a layer is encapsulated in a larger container by the layer below it. From Highest to Lowest, these layers are:

1. Application Layer
2. Transport Layer
3. Network Layer
4. Data Link Layer

1. **Application Layer:** This layer is responsible to send and receive data for applications like Domain Name System, Hypertext Transfer Protocol, and Simple Mail Transfer Protocol etc.

2. **Transport Layer:** This layer is responsible to provide connection-oriented or connectionless services for transporting application layer services between networks. Transmission Control Protocol and User Datagram Protocol are commonly used transport layer protocols.

3. **Network Layer:** This layer is responsible to route packets across networks. Internet Protocol, Internet Control Messaging Protocol and Internet Group management Protocols are commonly used Network layer protocols.

4. **Data Link Layer:** This layer is responsible for communications on the physical network components. Ethernet protocol is the best Data Link Layer protocol.

2. Network Security:

2.1 Necessity for Network Security

The threats on wired or wireless networks have significantly increased due to advancement in modern technology with growing capacity of computer networks. The overwhelming use of Internet in today’s world for various business transactions has posed challenges of information theft and other attacks on business intellectual assets.

In the present era, most of the businesses are conducted via network application, and hence, all networks are at a risk of being attacked. Most common security threats to business network are data interception and theft, and identity theft.

Network security is a specialized field that deals with thwarting such threats and providing the protection of the usability, reliability, integrity, and safety of computer networking infrastructure of a business.

3. Objective of Network Security:

The proper network implementation of protocols and services as a tool is required to protect and mitigate threats against any network infrastructure based on organizational needs. The primary goal of network security are Confidentiality, Integrity, and Availability. These three pillars of Network Security are often represented as CIA triangle.

- **Confidentiality** − The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons.

- **Integrity** − This goal is maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.

- **Availability** − The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the legitimate users, whenever they require it.

4. Achieving Network Security

International Telecommunication Union (ITU), in its recommendation on security architecture X.800, has defined certain mechanisms to bring the standardization in methods to achieve network security. Some of these mechanisms are −

- **En-cipherment** − This mechanism provides data confidentiality services by transforming data into not-readable forms for the unauthorized persons. This mechanism uses encryption-decryption algorithm with secret keys.

- **Digital signatures** − This mechanism is the electronic equivalent of ordinary signatures in electronic data. It provides authenticity of the data.

- **Access Control** − This mechanism is used to provide access control services. These mechanisms may use the identification and authentication of an entity to determine and enforce the access rights of the entity

5. A LAYER-BY-LAYER LOOK AT SECURITY MEASURES

Before going into the particulars of application-based security, it may be helpful to look at how security is implemented at the different ISO layers. The ISO model divided into upper-layer protocols (those associated with the application of data) and lower-layer protocols (those associated with the transmission of data). Examples of some of the security protocols used at each layer are listed on the right. Begin with layer 1, the physical layer. Common methods for providing security at the physical layer include:

- securing the cabling conduits: encase them in concrete
- shielding against spurious emissions: TEMPEST
- using media that are difficult to tap: fiber optics

S.No	Layers	Protocols
1	Application Layer	○ PGP(Pretty Good Privacy) ○ S/MIME(Secure/Multipurpose Internet Mail Extension) ○ S-HTTP(Secure-Hyper Text Transfer Protocol) ○ HTTPS(Hyper Text Transfer Protocol-Secure Socket Layer) ○ SET(Secure Electronic transaction) ○ KERBEROS
2	Transport Layer:	○ SSL(Secure Socket layer) ○ TLS(Transport layer Security)
3	Network Layer	○ IPSec (Internet protocol Security) ○ VPN(Virtual Private Network)
4	Data Link Layer:	○ PPP(Point-to-Point Protocol) ○ RADIUS (Remote Authentication Dial-In User Service) ○ TACACS+ (Terminal Access Controller Access Control System)

While effective, these methods are limited to things within one's physical control. Common layer 2 measures include physical address filtering and tunneling (e.g., L2F, L2TP). These measures can be used to control access and provide confidentiality across certain types of connections, but are limited to segments where the endpoints are well-known to the security implementer. Layer 3 measures provide for more sophisticated filtering and tunneling (e.g., PPTP) techniques. Standardized implementations such as IPsec can provide a high degree of security across multiple platforms. However, layer 3 protocols are ill-suited for multiple-site implementations because they are limited to a single network. Layer 4 transport-based protocols overcome the single network limitation but still lack the sophistication required for multiple party transactions. Like all lower-layer protocols, transport-based protocols do not interact with the data contained in the payload, so they are unable to protect against payload corruption or content-based attacks.

5.1 Available Security Control Protocols at each layer

As we know that in TCP/IP model, the data is passed from the highest to the lowest layer, with each layer adding more information, a security control at a higher layer cannot provide protection for lower layers. This is because the lower layers perform functions of which the higher layers are not aware. The various Security controls that are available at each layer are:

5.2 Application Layer: Each application need separate controls as per the protection required by it. If an application need to protect sensitive data sent across networks, the application may need to be modified to provide this protection. Designing and implementing a cryptographically sound application protocol is challenging and difficult as requires a large resource investment, proper configuration of controls .Creating new application layer security controls is likely to create vulnerabilities. Software's at application layer can protect application data but cannot protect TCP/IP information such as IP addresses as exists at a lower layer. Sometimes Standard based solutions at Application layer controls for protecting network communications like Secure Multipurpose Internet Mail Extensions (S/MIME) is commonly used to encrypt email messages. DNSSEC is another protocol at this layer used for secure exchange of DNS query messages.

DNS Protocol: Domain Name System (DNS) is used to resolve host domain names to IP addresses.

Network users depend on DNS functionality mainly during browsing the Internet by typing a URL in the web browser.

In an attack on DNS, an attacker's aim is to modify a legitimate DNS record so that it gets resolved to an incorrect IP address. It can direct all traffic for that IP to the wrong computer. An attacker can either exploit DNS protocol vulnerability or compromise the DNS server for materializing an attack.

DNS cache poisoning is an attack exploiting a vulnerability found in the DNS protocol. An attacker may poison the cache by forging a response to a recursive DNS query sent by a resolver to an authoritative server. Once, the cache of DNS resolver is poisoned, the host will get directed to a malicious website and may compromise credential information by communication to this site.

5.3 Transport Layer: To protect the data in a single communication session between two hosts, controls of Transport layer is used. Transport layer controls cannot protect IP information added at the network layer. The most common use for transport layer security protocols is protecting the HTTP and FTP session traffic. The Transport Layer Security (TLS) and Secure Socket Layer (SSL) are the most common protocols used for this purpose. The Transport Layer Protocols i.e. Transport Layer Security (TLS) protocol is used to secure HTTP Traffic. TLS has been used to protect HTTP-based communications and can be used with SSL portal VPNs.TLS is the standards based version of SSL version 3.TLS is a well-tested protocol that has several implementations that have been added to many applications. It is a low risk option compared to adding protection at the application layer.

SSL, the most commonly used protocol can provide any combination of the following types of protection:
Confidentiality: SSL can ensure that data cannot be read by unauthorized parties. It is accomplished by encrypting data using a cryptographic algorithm and a secret key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.

Integrity: SSL can determine if data has been changed intentionally or unintentionally during the transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a keyed cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

Peer Authentication: Each SSL end point can confirm the identity of the other SSL endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from expected host. SSL authentication is typically performed one-way, authenticating the server to the client, but it can be performed mutually.

Replay Protection: The same data is not delivered multiple times and data is not delivered grossly out of order.

5.4 Network Layer: Network layer controls provide a way for network administrators to enforce security policies. Security measures at this layer can be applied to all applications; thus, they are not application-specific. IP Information i.e. IP Addresses is added at the network layer, hence the controls at this layer protect both the data within the packets and the IP information for each packet. Controls at this layer are not application- specific and protects all network communications between two hosts or networks. Internet Protocol Security (IPsec), a network layer control provides a better solution than transport or application layer controls because of the difficulties in adding controls to individual applications. SSL tunnel VPNs act as network layer VPNs and provide the ability to secure both TCP and UDP communications including client/server and other network traffic. However, security protocols at this layer provide less communication flexibility that may be required by some applications.

Network layer security controls are frequently used for securing communications as they can provide protection for many applications without modifying them and particularly over shared network such as the Internet. Network Layer Security controls provide a single solution for protecting data from all applications, as well as protecting IP information. Sometimes controls at another layer are better than providing protection through network layer. In case one or two applications only need protection, then network layer control may be excessive. In such situation Transport Layer protocols such as SSL are used to provide security for communication with individual HTTP-based applications. It also provides security for communication sessions of applications like SMTP, Point of Presence (POP), Internet

Message Access Protocol (IMAP) and File Transfer Protocol.

The Internet Protocol Security (IPsec) authentication and encapsulation standard is widely used to establish secure VPN communications. The use of IPsec can secure transmissions between critical servers and clients. This helps prevent attacks from taking place. Unlike most security systems that function within the application layer of the Open Systems Interconnection (OSI) model, IPsec functions within the network layer.

Internet Control Message Protocol (ICMP) is a protocol meant to be used as an aid for other protocols and system administrators to test for connectivity and search for configuration errors in a network. Ping uses the ICMP echo function and is the lowest-level test of whether a remote host is alive. A small packet containing an ICMP echo message is sent through the network to a particular IP address. The computer that sent the packet then waits for a return packet. If the connections are good and the target computer is up, the echo message return packet will be received. ICMP has its own vulnerabilities and can be abused to launch an attack on a network.

The common attacks that can occur on a network due to ICMP vulnerabilities are −

- ICMP allows an attacker to carry out network reconnaissance to determine network topology and paths into the network. ICMP sweep involves discovering all host IP addresses which are alive in the entire target's network.
- Trace route is a popular ICMP utility that is used to map target networking by describing the path in real-time from the client to the remote host.
- An attacker can launch a denial of service attack using the ICMP vulnerability. This attack involves sending IPMP ping packets that exceeds 65,535 bytes to the target device. The target computer fails to handle this packet properly and can cause the operating system to crush.

Other protocols such as ARP, DHCP, SMTP, etc. also have their vulnerabilities that can be exploited by the attacker to compromise the network security.

5.5 Data Link Layer: Data link Layer controls for dedicated circuits applied to all communications on a specific physical link between two buildings or a connection to an Internet service provider. Data Link Layer controls are provided by specialized hardware devices known as data link encryptors. It is below the network layer, controls at this layer can protect both data and IP information. Data Link layer protocols are simple and are specific to a particular physical link, they cannot protect connections with multiple links such as establishing a VPN over the Internet.

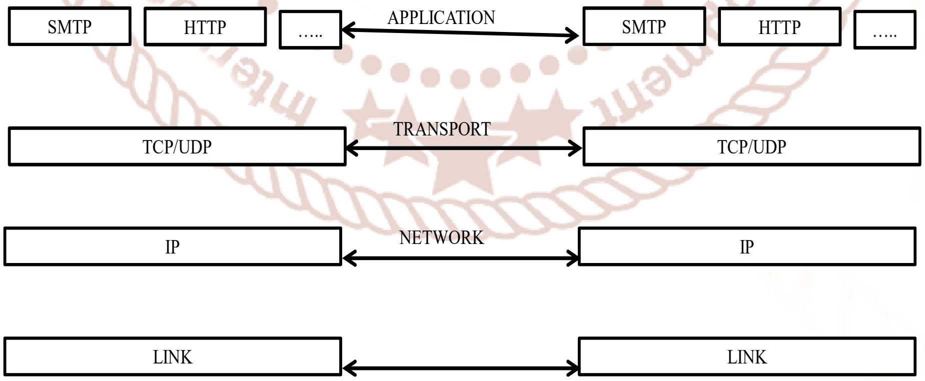

Fig: Internet Protocol

5.6 Security Vulnerabilities of TCP/IP protocol suite: Some of the common security vulnerabilities of TCP/IP protocol suits are −

- HTTP is an application layer protocol in TCP/IP suite used for transfer files that make up the web pages from the web servers. These transfers are done in plain text and an intruder can easily read the data packets exchanged between the server and a client.
- Another HTTP vulnerability is a weak authentication between the client and the web server during the initializing of the session. This vulnerability can lead to a session hijacking attack

where the attacker steals an HTTP session of the legitimate user.

- TCP protocol vulnerability is three-way handshake for connection establishment. An attacker can launch a denial of service attack "SYN-flooding" to exploit this vulnerability. He establishes lot of half-opened sessions by not completing handshake. This leads to server overloading and eventually a crash.
- IP layer is susceptible to much vulnerability. Through an IP protocol header modification, an attacker can launch an IP spoofing attack.

5.7 Application Layer Security: Application security is security provided by the application program itself Application based security has the capability of interpreting and interacting with the information contained in the payload portion of a datagram. Lower-layer security protocols like IPsec do not have this capability. They can encrypt the commands for confidentiality and authentication, but they cannot restrict their use. For example, a data warehouse using internally maintained access control lists to limit user access to files, records, or fields is implementing application-based security. Applying security at the application level makes it possible to deal with any number of sophisticated security requirements and accommodate additional requirements as they come along. This scenario works particularly well when all applications are contained on a single host or secure intranet, but it becomes problematic when one attempts to extend its functionality across the Internet to thousands of different systems and applications. The distributed nature of applications on the Internet has given rise to several standardized solutions designed to replace these ad hoc, vendor-specific security mechanisms.

6. HDFS on TCP/IP Suite:

In the recent times, there has been urgent requirement to have a special Distributed File System capable of processing large datasets. The Hadoop Distributed File System (HDFS) is a distributed file system designed to process the data on the low- cost hardware. HDFS is considered to be highly fault-tolerant and provides high throughput access to application data and is suitable for applications that have large data sets. All HDFS communication protocols are layered on top of the TCP/IP protocol. HDFS helps in security management of large data. The primary objective of HDFS is to store data reliably even in the presence of failures.

The basic procedure for establishing a connection is performed in the following steps:
A client establishes a connection to a configurable TCP port on the NameNode machine. A Client utilizes the ClientProtocol with the NameNode. The DataNodes talk to the NameNode using the DataNode Protocol. A Remote Procedure Call (RPC) abstraction includes both the Client Protocol and the DataNode Protocol. By design, the NameNode never initiates any RPCs. Instead, it only responds to RPC requests issued by DataNodes or clients.

Data Organization of HDFS Architecture is organized into Data Blocks:
HDFS is a distributed file system that supports very large scale dataset. Such data files generally write one or few times but are engaged in number of times of reading the content from the file system. A typical block size used by HDFS is 64 MB. Thus, an HDFS file is chopped up into 64 MB chunks, and if possible, each chunk will reside on a different DataNode.

There exists three types of failures which occur more commonly and they are: NameNode failures, DataNode failures and network partitions. Some of the other important tasks performed by the HDFS Architecture can be listed as below:

- **Data Disk Failure**

Each DataNode consisting of data periodically sends a message to the NameNode. If there is any absence of such periodic message, then it is assumed by the NameNode that the connection is lost with the DataNode and no further communication can be continued.

- **Data rebalancing in clusters**

If data in one DataNode surpasses the given threshold of the data capacity then the data is automatically shifted from one DataNode to another DataNode. This accounts for the rebalancing schemes in HDFS architecture.

- **HDFS also supports Data Integrity**

It is highly possible that a block of data fetched from a DataNode is corrupt and this can occur due to faults in a network, program handling it or a disrupted storage device. When a client retrieves file contents it verifies that the data it received from each DataNode matches the checksum stored in the associated checksum file. If not, then the client can opt to retrieve that block from another DataNode that has a replica of that block.

The NameNode machine is a single point of failure for an HDFS cluster. If the NameNode machine fails, manual intervention is necessary. Automatic restart and failover of the NameNode software to another machine is not supported.

Conclusion:

In this paper, we have discussed the security protocols on the different layers of the network communication. We have also provided an overview of the HDFS layer, which is popularly used in the present day scenario. Also other tasks are supported by the HDFS which are discussed here. In future, we would like to describe the application of upcoming security standards of network communication.

References:

1. D. G. Maryna Krotofil, Industrial Control Systems Security: What is happening?
2. Homeland Security U.S., Improving Industrial Control with Defense in Depth Strategies, 2009.
3. IEEE, IEEE Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3), 2010.
4. PJM, Jetstream Guide DNP SCADA over Internet with TLS Security, 2013.
5. P. -. Profinet, Profinet Security Guidelines. Guidelines for PROFINET, 2013.
6. DNP3 Quick Reference Guide, 2002.
7. http://ittoday.info/AIMS/DSM/87-30-04.pdf
8. https://en.wikipedia.org/wiki/Network_interface_layer_security
9. https://cse.sc.edu/~farkas/csce813-2014/lectures/csce813-lect8.3.ppt
10. http://www.ittoday.info/AIMS/DSM/87-30-02.pdf
11. ijcset.net/docs/Volumes/volume2issue6/ijcset2012020605.pdf
12. http://www.ittoday.info/AIMS/DSM/87-30-01.pdf
13. www.cse.yorku.ca/SecRAY/AppLayerSecurity_Andrade.pdf
14. https://securityintelligence.com › Topics › Application Security
15. http://www.ittoday.info/AIMS/DSM/87-30-03.pdf
16. https://www.veracode.com/solutions/security-professionals
17. https://www.checkmarx.com/2016/02/04/application-layer-security-within-osi-model/
18. https://lms.ksu.edu.sa/bbcswebdav/users/mdahshan/Courses/CEN585/Course-Notes/08-Network-Layer-Security.pdf
19. https://handouts.secappdev.org/handouts/2011/Bart%20Preneel/preneel_network_protocols_2010v1.pdf
20. https://www.w3.org/Security/
21. https://en.wikipedia.org/wiki/Application_layer