Advanced Computer Networks

Assignment Two 2017

10/30/2017

1. Security and Applications

a) Discuss the problems caused for firewalls by the use of VPNs and IPSec.

A VPN connection is the extension of a private network that includes links across shared or public networks, such as the Internet.We can firewall with a VPN server.A firewall is a system or combination of systems that enforces a boundary between two or more networks.VPN Server can be placed behind the firewall,in front of the firewall and also use VPN server on the same box of the firewall.Putting a VPN Server inside the firewall leads more significant security problemsbecause it can be easily hacked by a hacker and creates severe damage.In some places, firewalls block ports which required toestablish a VPN connection.Another problem is the traffic between the VNS server and firewall is not encrypted. If VNS server is located in the same box of the firewall, management and troubleshooting problems occur.So [illegible] ll by the use of VPNs (Lewis, 2006).

IPSec (Internet Protocol security) is a framework of open standards for helping to ensure private, secure communications over Internet Protocol networks through the use of cryptographic security services. The Internet protocol Security Tunnel is in the VPN Router. From the VPN Router, the firewall central will NAT the IP-Adress. The Satellite Site firewall has only one IP-Adress. Therefore, we do PAT the VPN Router Satellite. The IPSec Tunnel is a magnetic tunnel, and we use NAT-T (UDP Port 500 and UDP Port 4500). The Tunnel is running well if nothing is changing. If someone configures on the firewalls, the IPSec Tunnel will sometimes never connect successfully. The firewall doesn't start till a network connection exists.IPSec can perform host-based packet filtering to provide limited firewall capabilities for end systems.These are the problems caused by firewall by the use of IPsec.

b) Security services may be placed within each of the layers ofthe OSI reference model. List, describe, and discuss the advantages and disadvantages of placement within each layer. Your answer should include examples of security services within at least three differing layers.

OSI Reference model helps to standardise the communication between the systems. OSI divide communications into seven layers in which each layer contain protocols, multiple hardware standards and so on.The security services included in the OSI security model are data integrity, data confidentiality authentication and access control services.The seven layers of the OSI reference model are

1. The Physical layer- It transmits bits over a transmission medium establishing mechanical and electrical specifications. The physical layer is concerned with physical characteristics of the optical signal and electrical signalling techniques such as a type of media shape of the connector,voltage levels and so on.

2. The Data Link layer-It is the second layer of OSI which provides error-free transfer of data frames from one node to another over the physical layer. It implements error control mechanism.
3. The Network layer-The third layer of OSI which include path determination and logical addressing.
4. The Transport layer-Itensures that to delivered error-free messages, in sequence, without any duplications or losses. Protocols that operate transport Layer are TCP (Transmission Control Protocol), and UDP (User Datagram Protocol) uses a mechanism known as "Port Number" to enable multiplexing and de-multiplexing.
5. The Session layer-It establishes, manages, and terminates communication sessions consisting of service requests and service responses that occur between applications located in different network devices.

For Example, A web servers may contain different users for communicating with the server at a specified time. So, keeping track of which user communicates on which path is important and session layer handle this responsibility accurately

6. The Presentation layer-This layer is usually part of an operating system and converts incoming and outgoing data from one presentation format to another. This segment includes compression, encryption, and ensuring that the character code set can be interpreted on other sides.
7. The Application layer-It is the top-most layer of the seven-layered Open Systems Interconnection (OSI) network model. It provides a platform to send and receive data over a network. Real traffic is generated from the Application Layer (Hura & Singhal, 2001). It may be a web request made from HTTP protocol, a command from telnet protocol, a file download request from FTP protocol.

For Example

Browsers like Google Chrome, Internet Explorer etc.

Some of the advantages of OSI reference model are

- OSI is a genuinely generic model and it has the flexibility to adapt to many protocols.
- Each Layer in OSI model is distinguished according to the protocols, servicesand interfaces.
- OSI offers connection-oriented and connectionless services. So it provides reliable and faster transmission of data.
- It implements divide and conquers method, so maintenance and administrations of OSI model architecture are effortless.
- OSI model is more secure and easily adaptable.
- Upper layers can share lower layers functionality.

Disadvantages of OSI reference model are listed below

- OSI does not explain any specific protocol.
- There is difficulty to fit a new protocol in this model.

- Some duplication is in services of various layers.That is both transport and data link have error control mechanism.
- Some interdependency problem among layers.

c) Both Alice and Bob have public-key capability. They wish to carry out mutual authentication. Let us assume that Alice and Bob already know each other's public keys. They want to establish a session, and then use symmetric session keys on that session, since it is typically 100 to 1000 times faster than public key cryptography. Write a protocol that enables Alice and Bob to mutually authenticate each other and agree on a shared secret key.

Alice and Bob are already having a public key capability through which they had accomplished a specific cryptography in which the system is having two keys. This key as in most cases is a private and public keys. The public key as usual will be known to all and the private key will be only accessible to the complete owner. This method is mainly employed in order to authenticate the owner of the two paired keys when the public key has sent over some message. It also has the characteristics that the particular owner of the paired key i.e. Alice and Bob [illegible]s send from those public keys that they have encrypted. In this scenario both Bob and Alice knows their public keys and is looking forward to for better keys which are way faster than the public keys like the symmetric session keys. They already know the main advantage of symmetric session keys that these keys are 100 to 1000 times faster than a public key sharing session cryptography. A special type of session keys which encrypts and decrypts same key to generate communication between two users. Another communication established is between a user and a computer and in other cases between two computers. If the total system is having only one key for both encryption and decryption are designed then the particular design is called a symmetric session key. They are enabling a special protocol through which both Alice and Bob are mutually authenticated and both have agreed to the common term that they will share a common secret key. Mutual authentication allows two users or parties which are trying to authenticate the same time. Basically a symmetric session will be between two machines and it has some of the common demerits also. The main two types of mutual authentication are certificate based and the one using the user name and password system. Bob and Alice will be employing the second type of symmetric session which is the protocol of engaging a username and password system which is applicable to both and is one among the speediest method which is existing nowadays in the technologically evolving world. A secret shared key will be introduced as it will have certain specific characteristics like it will be in specific format like a password with passphrase or may be a hexagonal string. The crypto systems usually depend only on one key for confidentiality purpose. There is always a chance of attack to Bobs and Alice's password also. Their protocol also includes the specification to pick up sufficiently long passwords and the key will be capable enough to resist against the odd force attacks. The secret key will be known to both Alice and Bob and it is also possible to compromise at one end without the knowledge of any others. The protocol also contains the necessary things to develop and keep the new encrypted passwords. The new protocol described is super efficient in time and will bring more safety to the total system.

2. TCP

Among the internet protocol suites the main and most established method of protocol is called the Transmission Control Protocol or TCP as short. It is usually originated at the initial implementation of the networks from the normal Internet protocol (IP). Since the TCP is often a initial product of internet protocol it is often termed as TCP/IP. A stream of octets between the hosts is delivered as a stream which usually provides a reliable as well as ordered. The stream of octets that they form is completely error checked. Almost all the internet applications of the works rely on TCP (Kozierok, 2015). That giant involved in the list of application that has employed the TCP includes email and World Wide Web. The other applications of TCP are in the fields of file transfer and remote administration all throughout the world. The other applications that don't tend to use this application will be using a user datagram protocol(UDP) which usually provides a non connecting datagram which is more focused on latency more than reliability. TCP defines the standard on how maintain and make up a network conservation using certain specific application programs which has the capability to exchange data. TCP usually works with the internet protocol which is the designer of how a computer receives and sends the datas which are send as packets between the computers. Basically the IP and TCP are the substances which defines the internet. TCP is given a definition by the Internet Engineering task Force(IETF) in the RFC format i.e. the standard document for request of command. TCP is the special type of protocol which is completely connection oriented which has the capabilities of mainly establishing and keeping up the connection since both the application programs at each end have completed the data transfer which usually includes messages from one system to another. The process of breaking up of data into packets that the network is capable of delivering and the sending and receiving of data packets from one network area to another and the total flow is controlled by the TCP. For making the system error free the TCP takes care of the handling of the garbled as well as the dropped packages and it also provides an acknowledgement of all the packets that are received. The different versions of TCP are mentioned and characterized below

TCP Tahoe

TCP Tahoe is considered as the base of TCP. The TCP Tahoe is the most initial algorithm that has all three transmission segment. Its transmission stages include slow start, congestion avoiding phase and the fast restraint phase.

TCP Reno

TCP Reno is the most broadly used internet protocol with specific four phases. The presence of thee four stages have added on to its merit and is more compatible. It one among the reasons for its wide use. The four stages ad they are the slow start phase, avoidance of congestion phase, fast restraint phase and the new version of fast recovery phase.

TCP New Reno

TCP New Reno is the modified version of TCP Reno. It is specially designed to initiate a phase which is capable of fast recovery of TCP Reno. It has the capability of detecting multiple losses in packets. The sole purpose of addition of the new phase is to reduce the leakage of packets by conducting congestion to the window over a multiple time.

3. IPv6

a) IPv6 has been standardized for almost 20 years, yet it has not seen widespread deployment. Describe the reasons for the slow adoption of IPv6.

The IPv6 is the latest version of the internet protocol. It is the commonly used communication system which is the source of identification and the main system for location on networks and has to control the specific routes across the internet. The Internet Engineering task Force was the designers of IPv6 and it was particularly developed by them in order to deal up with the issue of data address lose that was always a part of the IPv4. IPv6 was the answer for replacement of the IPv4 (radner & Mankin, 1998). But still now it is not that widespread. The internet is always expanding. The common problems faced in the internet now a days are the number of devices connected to the web. The increase in number of Smart phones and other gadgets and the connection to the internet and its vast possibilities has to be seen of. The transmission to IPv6 has become more and more inevitable but it [illegible] for the lack of spreading of IPv6 are

Expensive

Millions of routers, modems and switches are the components of the internet. They all were primarily designed for IPv4. Replacing all these components is surely a timely as well as highly expensive procedure. Its an edge network and time is the solution. The end user equipments are regularly replaced and it will lead to the condition were millions of devices have to be thrown away. The condition is so scary that their should be old age homes for those thrown away devices. In the core networking the replacement of some hardware like the router is not a everyday process. Hence the money as well as the time eating process is hard to achieve.

NAT the rescuer

The initial release of Pv6 was in 1998. It was planning an extension of the address to more than 7.9*1028 as of IPv4. The total exhaustion of IPv4 was the main reason for the development of IPv6. Unfortunately by the proper development of IPv6 NAT has started to rule the whole world.

NAT was the feature which had expanded the life cycle of the IPv4 protocol. NAT usually provide certain basic security and it is also available at the lowest cost.

Compatibility

The primary design target of IPv6 doesn't contain the reverse compatibility. The critical signature failure of the IPv6 was that its inability to get compact with IPv4. It was the main thing that they should have provided. The installation of IPv6 is so slow over the world because there is no available standardized tool by which the system of IPv4 can communicate with the system of IPv6.

Lack of competitors moving to IPv6

Due to the high maintenance charges and time eating procedures in installing the IPv6 many have opted to continue using IPv4. There is no benefits or credits for the early installer of IPv6 and no one will want to change the IPv4 unless it becomes idle or members including the competitor companies and other friend company have started to switch to IPv6.

Reachabilty issues

Most of the users are unaware of the IPv6 and the profit and the easiness that it can bring on. But increased knowledge now days the use of IPv6 has shown a little bit of improvement comparing the unawareness time.

b) What changes are required in regular routing protocols (that operate with IPv4) in order to prepare them for routing within IP v6 domain?

IPv4 is the fourth version of internet protocol which uses the identification techniques like addressing a system to identify the device. IPv4 is the most widely used internet protocol which connects the systems to the internet. The internet usage has increased rapidly in the last decades and this increase in the amount of smart phones and other gadgets will pull us to a situation where the internet will run out of Ip address (Smith, 2013). An Ip address is the main internet address for any device using the internet. Ipv6 is the new method developed to address the internet. Ipv6 is the direct successor of Ipv4 with unlimited addressing option. Ipv6 was developed in such a way that the data traffic and the number of hosts that are providing and using will only grow in a steady way creating a harmony. Ipv6 is often referred to us the next generation Internet standard.

Benefits of IPv6 over Ipv4

- NAT can be completely removed.
- Addition of auto configuration techniques.
- Private address collisions will be dealt with
- Improvement in multicasting routing
- More easier header formats
- More efficient and simplest routing.
- The genuine quality of service and labeling flow
- Support and other authentication are built in
- Options and extensions are made flexible.
- Administration made easy.

The various conversion techniques which are employed in the transition from IPv4 to Ipv6 are

Dual Stack Network

The transition technology employed in the transmission of IPv4 to IPv6 is termed as Dual stack. Dual stack has an operational way of operating in tandem or shared and dedicated links. In the dual stack mode both the iov4 and ipv6 [illegible] Even though the Dual stack sounds perfect it also has the demerits like the

- The current network which is working with the Ipv4 has to be capable of running IPv6 directly. In most cases the existing systems will not be capable for the same.
- Extreme business delay will be caused at the time of redesigning the current set up as it has to operate every IPv6 network attributes.

Tunneling

Overlaying networks which builds a tunneling option and enables the organizations to introduce the IPv6 over the IPv4. The main advantage that tunneling posses is that the new protocol can be installed without disturbing the older one. The main disadvantages or the effects in current network includes

- The users who had started the use of IPv6 wont be able to access the IPv4 which is completely underplayed in the infrastructure.
- Lack of new protocol to do the communication with the old customers without using dual slacks. This is one reason for the negativity in interoperability.

Translation

Translation or in other words family translation has the ability to get communication between the hosts of IPv4 and IPv6. It is done by performing ip header and other organised address translation between the families. It is just a medium term strategy which the company’s cant be that sure of applying

Translation present two main advantages,

- The gradual migration of the Ipv6 is provided by seamless internet existence that the Ip4 was accessing.
- Existing content holders will be able to provide the service to the newest incorporation which is highly helpful for the new IPv6 competitors.

The transition from IPv4 to IPv6 is a timely processes and the router as well as all the components of the older version has to undergo certain variations and has to suffer many disadvantages which are already mentioned above. The complete disappearance of the IPv4 is the newest target of the highest internet authority people and they won’t hesitate to do the need full changes in the current existing IPv4 systems even though many companies may suffer or get exterminated.