International Journal of Trend in Research and Development, Volume 2(6), ISSN: 2394-9333
www.ijtrd.com

A Study on Communication Security in Networks

[1]B.Vinothini, [2]D.Shobana and [3]S.Ranjeesha,
[1,3]Scholar, [2]Assistant professor,
Department of Information and Technology,
Sri Krishna College of Arts and Science, kuniamuthur, Coimbatore, India

Abstract: This Paper shows that it is possible to select a key over open communications channels in such a fashion that communications security can be maintained. A Method is described which forces any enemy to expend an amount of work which increases as the square of the work required of the two communicants to select the key. The Method provides a logically new kind of protection against the passive eavesdropper. It suggests that further research on this topic will be highly rewarding, both in a theoretical and a practical sense. [7]

Keywords: *COMSEC, IP sec, Encryption, Cryptograph, Secure Shell, ACC, VPN.*

I. INTRODUCTION TO SECURITY IN NETWORKS

Computer Security is the protection of computing systems and the data that they store or access. Computer Security allows the University to carry out its mission by:

Enabling people to carry out their jobs, education, and research

- Supporting critical business process
- Protecting personal and sensitive information

A. Security Objectives

- Learn **"good computing security practices."**
- Incorporate these practices into your everyday routine. Encourage others to do so as well.
- Report anything unusual - Notify your supervisor and the ITS Support Centre if you become aware of a suspected security incident. [6]

II. COMMUNICATION SECURITY

Communications security (COMSEC) is the prevention of unauthorized access to telecommunications traffic, or to any written information that is transmitted or transferred. In the United States Department of Defence culture, it is often referred to by the abbreviation **COMSEC**. The field includes crypto security, transmission security, and physical security of COMSEC equipment. COMSEC is used to protect both classified and unclassified traffic on military communications networks, including voice, video, and data. It is used for both analog and digital applications, and both wired and wireless links. [1]

A. IP Security

Internet Protocol Security (**IPsec**) is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

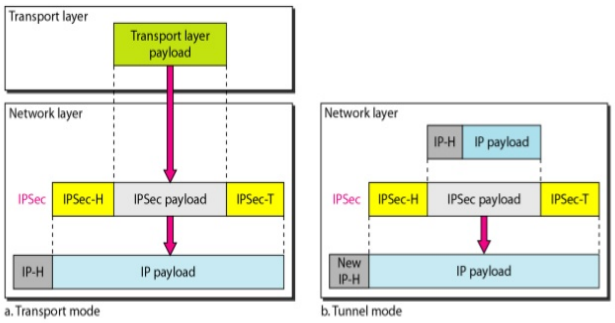

Figure 1: IP security

Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, and data confidentiality (encryption), and replay protection.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use,

such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in[2]

III. FIREWALLS

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

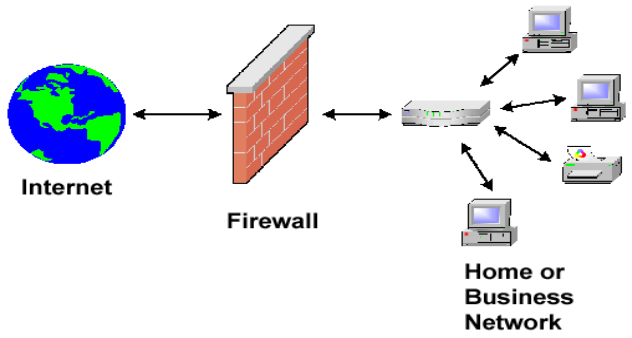

Fig 2: Firewalls

A. Common Firewall Techniques

Firewalls are used to protect both home and corporate networks. A typical firewall program or hardware device filters all information coming through the Internet to your network or computer system. There are several types of firewall techniques that will prevent potentially harmful information from getting through:

B. Packet Filter

Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

C. Application Gateway

Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.

D. Circuit Level Gateway

Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

PROXY intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defence in protecting private information. For greater security, data can be encrypted. [3].

Firewall with Identity-based policy creation. Access Control Criteria (ACC) – User-Identity, Source & Destination Zone, MAC and IP address, Service. Policy creation for multiple security features through single interface in firewalls. Firewalls well-integrated with VPN, IPS, Anti-Virus & Anti-Spyware, Anti-Spam, Web Filtering, Bandwidth Management, Multiple Link Management.

- Firewall with High Availability with stateful failover
- Available as Next-Generation Firewalls and UTMs
- Multiple Security Zones
- Firewall appliance offering Dynamic Routing
- VLAN support
- Virtual host capability [8]

IV. VIRTUAL PRIVATE NETWORK

A virtual private network (VPN) is a technology that creates an encrypted connection over a less secure network. The benefit of using a VPN is that it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it. The justification for using a VPN instead of a private network usually boils down to cost and feasibility: It is either not feasible to have a private network (e.g., for a traveling sales rep) or it is too costly to do so. The most common types of VPNs are remote-access VPNs and site-to-site VPNs.

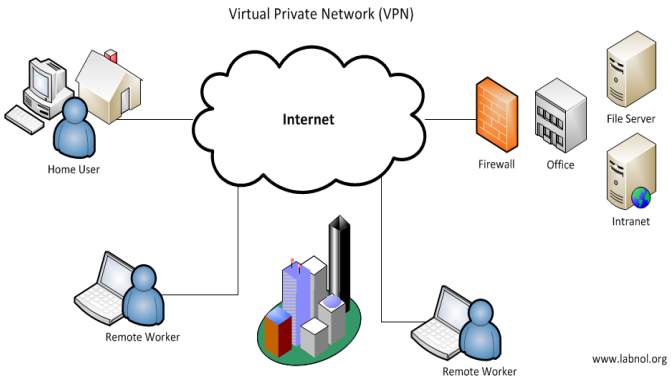

Figure 3: Virtual Private Networks

A remote-access VPN uses a public telecommunication infrastructure like the Internet to provide remote users secure access to their organization's network. A VPN client on the remote user's computer or mobile device connects to a VPN gateway on the organization's network, which typically requires the device to authenticate its identity, then creates a network link back to the device that allows it to reach internal network resources (e.g., file servers, printers, intranets) as though it was on that network locally. A remote-access VPN usually relies on either IPsec or SSL to secure the connection, although SSL VPNs are often focused on supplying secure access to a single application rather than to the whole internal network. Some VPNs provide Layer 2 access to the target network; these require a tunnellingprotocol like PPTP or L2TP running across the base IPsec connection.

A site-to-site VPN uses a gateway device to connect the entire network in one location to the network in another, usually a small branch connecting to a data centre. End-node devices in the remote location do not need VPN clients because the gateway handles the connection. Most site-to-site VPNs connecting over the Internet use IPsec. It is also common to use carrier MPLS clouds rather than the public Internet as the transport for site VPNs. Here, too, it is possible to have either Layer 3 connectivity (MPLS IP VPN) or Layer 2 (Virtual Private LAN Service, or VPLS) running across the base transport.

VPNs can also be defined between specific computers, typically servers in separate data centres, when security requirements for their exchanges exceed what the enterprise network can deliver. Increasingly, enterprises also use VPNs in either remote-access mode or site-to-site mode to connect (or connect to) resources in a public infrastructure as a service environment. Newer hybrid-access scenarios put the VPN gateway itself in the cloud, with a secure link from the cloud service provider into the internal network. [4]

V. WIRELESS SECURITY

Various wireless security protocols were developed to protect home wireless networks. These wireless security protocols include WEP, WPA, and WPA2, each with their own strengths — and weaknesses. In addition to preventing uninvited guests from connecting to your wireless network, wireless security protocols encrypt your private data as it is being transmitted over the airwaves.

Wireless networks are inherently insecure. In the early days of wireless networking, manufacturers tried to make it as easy as possible for end users. The out-of-the-box configuration for most wireless networking equipment provided easy (but insecure) access to a wireless network.

Although many of these issues have since been addressed, wireless networks are generally not as secure as wired networks. Wired networks, at their most basic level, send data between two points, A and B, which are connected by a network cable. Wireless networks, on the other hand, broadcast data in every direction to every device that happens to be listening, within a limited range.

A. Wired Equivalent Privacy (WEP)

The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well-known security flaws, is difficult to configure, and is easily broken.

B. Wifi Protected Access (WPA)

Introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a preshared key (PSK), commonly referred to as *WPA Personal*, and the Temporal Key Integrity Protocol (TKIP, pronounced *tee-kip*) for encryption. *WPA Enterprise* uses an authentication server to generate keys or certificates.

C. Wifi Protected Access Version 2 (WPA2)

Based on the 802.11i wireless security standard, this was finalized in 2004. The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is sufficient (and approved) for use by the U.S. government to encrypt information classified as top secret — it's probably good enough to protect your secrets as well. [5]

CONCLUSION

Hence with this we can able to know about the basic of communication security. Here we discussed about the internet protocol security, wireless security, VPN, and why the communication security is necessary. It is so important to transfer the data or to store the data with high security.

References

1. http://its.ucsc.edu/security/training/intro.html
2. https://en.wikipedia.org/wiki/IPsec
3. http://www.webopedia.com/TERM/F/firewall.html
4. http://searchenterprisewan.techtarget.com/definitio n/virtual-private-network
5. http://www.dummies.com/how-to/content/wireless-security-protocols-wep-wpa-and-wpa2.html
6. http://its.ucsc.edu/security/training/intro.html
7. http://www.merkle.com/1974/PuzzlesAsPublished. pdf
8. http://www.cyberoam.com/firewall.html