International Journal of General Engineering and Technology (IJGET)
ISSN (P): 2278-9928; ISSN (E): 2278-9936
Vol. 6, Issue 5, Aug – Sep 2017; 37-42
© IASET

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations
IASET

CONCEPTUAL STUDY ON NETWORK SECURITY AND ITS TYPES

YUVRAJ SINGH

Student, Department of Electronics & Communication Engineering,
Guru Nanak Dev University, Amritsar, Punjab, India

ABSTRACT

With the invention of the internet and new networking technologies, the world has become more interconnected. The concept of network securities is becoming more eminent due to easily acquirable intellectual properties. Network security covers an assortment of computer networks, both public and private, that are utilized as a part of ordinary activity directing exchanges and interchanges among organizations, government offices and people. In this research, discussion paper on the concept of network security as well as various types of network securities is done.

KEYWORDS: Network Security, Wireless Network Security, IP Security, Electronic Mail Security, Transport-Level Security, Firewalls

INTRODUCTION

In this era of growing internet and information technology, every individual, groups, and organizations, public or private are connected to the internet, which has emerged as the boom in the economy. However, on the other hand, various unethical users are doing attack and trying to destroy the network by using fake websites, emails, various Trojan, and virus. The target of intrusion on the network is to attack computers and paralyze them to steal information related to users and seek benefits out of that. Some invaders look upon military and government departments as targets which are a cause of threat for society and national security [1] [2].

CONCEPT OF NETWORK SECURITY

Network Security is a concept to protect network, over a wireless network. A network security system typically relies on layers of protection and consists of multiple components, including network monitoring and security software, in addition to hardware and appliances. Security of data can be done by a technique called cryptography. So one can say that, cryptography is an emerging technology, which is important for network security. The concept of network security revolves all around protecting networks of wireless networks. The network security system depends on protection layers. It consists of several components like networking, monitoring, security software, hardware, and various other appliances. In addition to network security, data can also be secured and the technique used to secure data is called cryptography. This emerging technology is extremely important for network security. Network security includes the approval of access to data in a network, which is controlled by the network administrator. Users are chosen or are allocated an ID and secret key, or other verifying data that permits them access to data and projects within their authority. Network security [3] comprises of the arrangements and strategies, embraced by a network administrator to anticipate and screen unapproved access, misuse, alteration, or dissent of a computer network and network-accessible resources. The network can be private, for example, inside an organization, and others, which may be open for public access. Network security is included in associations, undertakings, and different sorts of organizations. It does as its title clarifies: It secures the network, and additionally ensuring and managing operations being done. The most well-known and straightforward method for protecting a network is by giving it a password and username name.

Network security controls cannot eliminate the risk. The goal is to minimize risk as much as possible and to avoid unnecessary or excessive risk [4]. There are two different networks, i.e. data network and synchronous network. The former network consists of computer based routers, in which information can be obtained by special programs like Trojan horses planted in routers. Because of this reason, security is important in data networks. The latter type of networks consists of switches that do not buffer data and are not threatened by attackers. Intrusion Detection Systems (IDS) are based on two concepts. The former is misuse detection, which detects matching the previously seen patterns from an internal database of signatures, and the latter is anomaly detected, which works by detecting deviations from expected behavior. Misuse detection is having high accuracy, but fails in the case of previously unseen attack, whereas anomaly detection may detect new unseen attacks, but it has a low detection accuracy [5], [6], [7]. It is recommended to use both the IDS to bridge the gap between detection capabilities of each of them. [8]. Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Antivirus software or an intrusion prevention system (IPS) [9] help detect and inhibit, the action of such malware. An anomaly-based intrusion detection system may also monitor the network like Wireshark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account. [10]

TYPES OF NETWORK SECURITY

Wireless Network Security

Wireless security is the counteractive action of unapproved access or damage to computers using wireless networks. The most widely recognized sorts of wireless security are Wired Equivalent Privacy (***WEP***) and Wi-Fi Protected Access (***WPA***). WEP is infamously frail security standard. The password it uses can be hacked in no time with a laptop, computer system using various software tools. WAP security is given by the Remote Transport Layer Security (WTLS), which gives security benefits between the mobile devices (customer) and the WAP gateway to the Web. There are a few ways to deal with WAP end - to-end security. One striking methodology expects that the mobile device implements TLS over TCP/IP and the wireless network supports exchange of IP packets. The WAP is intended to adapt to the two vital restrictions of wireless web access, i.e. mobile node (little screen size, constrained information ability) and the low data rates of wireless computerized systems. Two vital WTLS ideas are the secure session and the secure connection, which are as follows:

Secure Connection

This type of connection acts as a measure to provide a suitable type of service. This association is temporary and it related to one session, but between any match of gathering there might be different secure associations.

Secure Session

An SSL session is an affiliation between a client and a server. Sessions are made by the Handshake Convention. Sessions characterize an arrangement of cryptographic security parameters, which can be shared among various connections. Sessions are utilized to stay away from the costly transaction of new security parameters for every connection. There are various stages related to every session. Once a session is set up, there is a working state for both read and compose (i.e., get and send). Furthermore, amid the Handshake protocol, pending read and compose states are made. Upon finishing of the Handshake protocol, the pending states become the current states.

IP Security

Internet Protocol Security (IPsec) is a convention suite for securing Internet Protocol (IP) interchanges by validating and encoding every IP bundle of a corresponding session. IPsec incorporates conventions for building up common validation between specialists toward the start of the session and arrangement of cryptographic keys to be utilized amid the session. IPsec can be utilized as a part of ensuring information streams between a couple of hosts (have to-have), between a couple of security doors (arrange to-organize), or between a security passage and a host (organize to-have). IPsec is said to be particularly helpful for actualizing virtual private systems and for remote client access through dial-up association with private systems. A major preferred standpoint of IPsec is that security plans can be dealt with without expecting changes to singular client PCs.

IPsec gives two choices of security benefit: Authentication Header (AH), which permits verification of the sender of information, and Encapsulating Security Payload (ESP), which underpins both confirmation of the sender and encryption of data too. The particular data related to each of these administrations are embedded into the parcel in a header that takes after the IP bundle header. Isolate key conventions can be chosen, for example, the ISAKMP/Oakley convention. IPsec utilizes cryptographic security administrations, to ensure correspondences over Internet Protocol (IP) systems. IPsec underpins organize level associate verification, information root confirmation, information, trustworthiness, information secrecy (encryption), and replay security. IPsec ensures any application movement, over an IP arrange. Applications can be consequently secured by IPsec, at the IP layer.

Electronic Mail Security

Email is exposed to both latency and dynamic assaults. The defense of email from unapproved admittance and check is known as electronic protection. In nations with a constitutional guarantee of the secrecy, email is compared with letters and is officially protected from all forms of spy. With the dangerously developing dependence on email, there grows an interest for verification and privacy. Two plans emerge as methodologies that appreciate the far-reaching use: Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension S/MIME. PGP is an open-source, openly accessible programming bundle for email security. It gives authentication using digital signature, confidentiality using symmetric block encryption, compression utilizing the ZIP algorithm, and e - mail compatibility utilizing the radix-64 encoding scheme. PGP fuses instruments for building up a public key trust model and public key certificate management. S/MIME is an Internet standard way to deal with email security that joins an indistinguishable usefulness from PGP. It is a security upgrade to the MIME Internet email organize standard in light of innovation from RSA Data Security.

Transport-Level Security

Transport-Level Security (TLS) is an IETF institutionalization activity whose objective is to deliver an Internet standard adaptation of SSL. Secure Socket Layer (SSL) gives security benefits amongst TCP and applications that utilization TCP. The Internet standard rendition is called Transport Layer Service (TLS). The TLS Record Format is the same as that of the SSL Record Format. SSL/TLS gives classification utilizing symmetric encryption and message honesty utilizing a message verification code. SSL/TLS incorporates conventional instruments to empower two TCP clients to decide the security systems and administrations they will utilize. HTTPS (HTTP over SSL) alludes to the mix of HTTP and SSL to execute secure correspondence between a Web program and a Web server. Secure Shell (SSH) gives secure remote logon and other secure customer/server offices. The SSH Connection Protocol keeps running over the SSH Transport Layer Protocol and expect that a safe confirmation association is being used. A wide range of correspondence utilizing SSH, for example, a terminal session, are bolstered utilizing separate channels.

Firewalls

A firewall frames a boundary through which the activity going toward every path must pass. A firewall security approach manages which movement is approved to go toward every path. Firewalls force confinements on approaching and Active Network parcels to and from private systems. Approaching or active movement must go through the firewall; just approved activity is permitted to go through it. Firewalls make checkpoints between an inside private system and the general Internet population, otherwise called stifle points (borrowed from the indistinguishable military term of a battle constraining land highlight). Firewalls can make gag focuses in view of IP source and TCP port number. They can likewise fill in as the stage for IPsec. Utilizing the burrow mode capacity, firewalls can be utilized to actualize VPNs. Firewalls can likewise restrain arrange a presentation by concealing the inner system framework and data from the general society Internet. A firewall might be intended to work as a channel at the level of IP bundles, or may work at a higher convention layer.

CONCLUSIONS

The concept of network security has become foremost in almost every field and even in our day to day life. By having knowledge of this concept, one can defend themselves from attackers. Many companies defend themselves by modifying network architecture, using firewalls, and applying diversifying policies to defend their networks. However, the fact is, current networks are more prone to attacks. These attacks are rarely seen and difficult to detect easily before damage is done [11]. Therefore, the primary concern is to secure the network from unwanted malicious traffic.

REFERENCES

1. Wang, Z., Liu, Z., & Xie, X. (2009, August). The research on network security technologies. In Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on (pp. 585-587). IEEE.
2. Yue, X., Chen, W., & Wang, Y. (2009, November). The research of firewall technology in computer network security. In Computational Intelligence and Industrial Applications, 2009. PACIIA 2009. Asia-Pacific Conference on (Vol. 2, pp. 421-424). IEEE.

3. Simmonds, A., Sandilands, P., & Van Ekert, L. (2004, October). An ontology for network security attacks. In Asian Applied Computing Conference (pp. 317-323). Springer, Berlin, Heidelberg.

4. Yue, X., Chen, W., & Wang, Y. (2009, November). The research of firewall technology in computer network security. In Computational Intelligence and Industrial Applications, 2009. PACIIA 2009. Asia-Pacific Conference on (Vol. 2, pp. 421-424). IEEE.

5. Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on software engineering, (2), 222-232.

6. Kumar, S., & Spafford, E. H. (1994). An application of pattern matching in intrusion detection.

7. Ghosh, A. K., Schwartzbard, A., & Schatz, M. (1999, April). Learning Program Behavior Profiles for Intrusion Detection. In Workshop on Intrusion Detection and Network Monitoring (Vol. 51462, pp. 1-13).

8. Nath, K. K. G. B., & Ramamohanarao, K. (2006). Network security framework. IJCSNS, 6 (7B), 151.

9. Networking and Network Security — Dave Dittrich's home page [v2. 2.291]. (n.d.). Retrieved July 18, 2017, fromhttps://staff.washington.edu/dittrich/home/network.html#network-monitoring-intrusion-detection-systems-ids

10. Automating Breach Detection For The Way Security... (n.d.). Retrieved July 18, 2017, from http://www.darkreading.com/operations/automating-breach-detection-for-the-way-security-professionals-think/a/d-id/1322443

11. Gupta, K. K., Nath, B., Ramamohanarao, K., & Kazi, A. U. (2006, May). Attacking confidentiality: An agent based approach. In International Conference on Intelligence and Security Informatics (pp. 285-296). Springer, Berlin, Heidelberg.