National Conference on Communication Technology & Network Security In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Communication Technology and Network Security

Prof. Ganapathi A
M.Tech(CNE), MSc(IT), B.Tech(CS), DCS &E, Triveni Institute of Commerce & Management, Bangalore, Karnataka, India

ABSTRACT

Security is a fundamental component in the Communication Technology and network Security. The first and foremost thing of every network planning, designing, building, and operating a network is the importance of a strong security policy. Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern. The internet structure itself allowed for many security threats to occur. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are different kinds of attack that can be when sent across the network. By knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide and all of these required different security mechanisms. In this paper, I am trying to discuss current communication technology different kinds of attacks along with various different kinds of security mechanism that can be applied according to the need and architecture of the network.

Keywords : Information and Communication Technology, Intrusion, Confidentiality, Firewall, Spoofing, Byzantine attack.

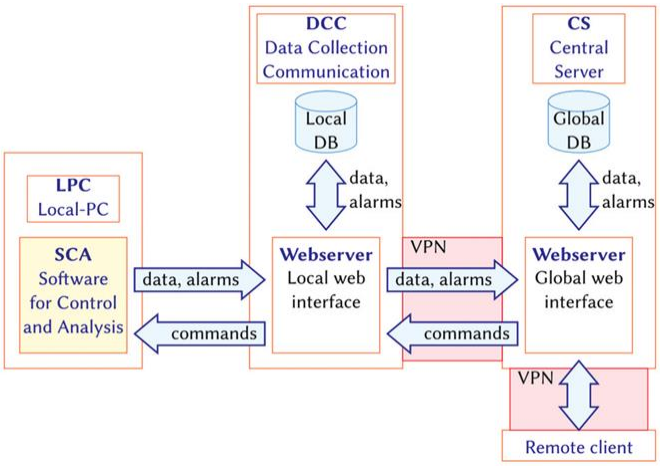
I. INTRODUCTION

Information and communications technology (ICT) is an extended term for information technology (IT) which stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary software, its storage and the audio-visual systems, which enable all users to access, store, transmit, and manipulate information. The term ICT is also used to refer to the combining of audio-visual and telephone networks with computer networks through a single cabling or link system. There are large economic incentives (huge cost savings due to elimination of the telephone network) to merge the telephone network with the computer network system using a single unified system of cabling, signal distribution and management. However, ICT has no universal definition, as "the concepts, methods and applications involved in ICT are constantly evolving on an almost daily basis. "The broadness of ICT covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form e.g. personal computers, digital television, email and even the modern day robots. The last few decades have witnessed a tremendous & phenomenal growth in the field of Information & Communication Technology (ICT) in education also which has influenced life of people especially students in some way or the other. ICT is arguably the technology area that has had the strongest impact on society during the past 60 years. The technology is visibly present in our use of computers, smart phones, information search, robotics and intelligent agents, but, has an even

greater impact as an enabling technology for a large number of application areas, such as medicine and healthcare, energy production and distribution, finance, public management and transport logistics to name a few. This progress has enabled to get prompt access to any required information. In these modern times of technological advancements, children are more interested in trying out; hence, a teacher should act as a facilitator and should encourage a child / student to advance technologically and in the right direction. In the field of education, ICT can be used to enhance quality and value of education especially through integration.

The massive global infrastructure has no fundamental security mechanisms built in to protect itself. It is thus set for unbelievable information sharing on both levels of unimportance and extreme necessity and so the need for network security is paramount to prevent against countless threats. Network Security is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. Security has become important issue for large computing organizations [1]. Computer network security is concerned with preventing the intrusion of an unauthorised person into a computer network. As computer connectivity increases, computer network security becomes more complex. Intrusion [2] is any set of actions that attempt to compromise the integrity, confidentiality or availability of a computer system resource (for example, unauthorised distribution of sensitive material over the Internet).

A Typical ICT Model



II. Types of Security Attacks

Here we are presenting some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc. Attacks to network from malicious nodes. Attacks can be categories in three: "Passive Attacks" when a network intruder intercepts data travelling through the network, and "Active Attacks" in which an intruder initiates commands to disrupt the network's normal operation. An advanced persistent threat (APT) is a prolonged and targeted cyberattack in

which an intruder gains access to a network and remains undetected for a period of time. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization.

2.1 Active attack

Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

a. Spoofing

When a malicious node miss- present his identity, so that the sender change the topology.

b. Modification

When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.

c. Wormhole

This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network [1].

d. Fabrication

A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices [2].

e. Denial of services

In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

f. Sinkhole

Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack [1].

g. Sybil

This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network [1, 2, and 3].

2.2 Passive attack

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring [1, 2, and 3].

a. Traffic analysis

In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

b. Eavesdropping

This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be private or public key of sender or receiver or any secrete data.

c. Monitoring

In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

2.3 Advance attacks

a. Black hole attack

Black hole attack is one of the advance attacking which attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An hacker use the flooding based protocol for listing the request for a route from the initiator, then hacker create a reply message he has the shortest path to the receiver . As this message from the hacker reached to the initiator before the reply from the actual node, then initiator will consider that, it is the shortest path to the receiver.

b. Rushing attack

In rushing attack, when sender send packet to the receiver, then attacker alter the packet and forward to receiver. Attacker performs duplicate sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so the receiver becomes busy continuously.

c. Replay attack

It this attack a malicious node may repeat the data or delayed the data. This can be done by originator who

intercept the data and retransmit it. At that time, an attacker can intercept the password.

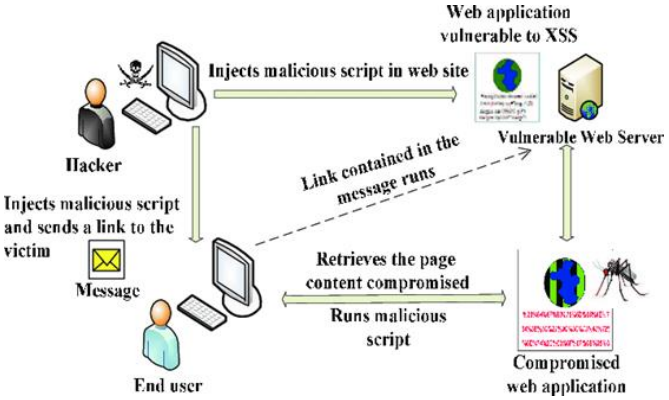
d. Byzantine attack

A set of intermediate node works between the sender and receiver and perform some changes such as creating routing loops, sending packet through non optimal path or selectively dropping packet, which result in disruption or degradation of routing services.

e. Location disclosure attack

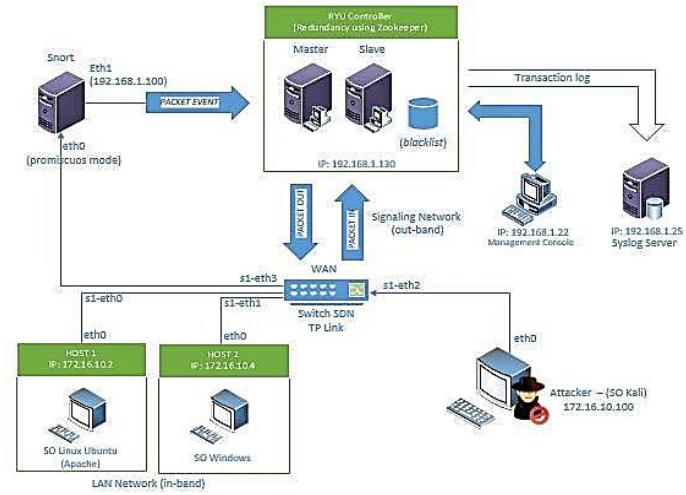
Malicious node collects the information about the node and about the route by computing and monitoring the traffic. So malicious node may perform more attack on the network.

Overview of Security Attacks



III. Internet Security Technology

Open Flow Network Security Architecture



With the rapid growth of interest in the Internet, network security has become a major concern to companies throughout the world. The fact that the information and tools needed to penetrate the security of corporate networks are widely available has increased that concern. Internet security tools typically provide authentication, encryption, identify attacks, and block and filter packets. There are two different access control approach used, the Discretionary Access Control (DAC) and the Mandatory Access Control (MAC). Commercial systems are based on DACs which indicates that the resources' owner specifies who may access and who may not access the resources. MAC on the other hand, works as a security officer that decides who is allowed and who is disallowed access to a particular resource.

3.1 Cryptographic systems

Cryptography originally denotes the art of keeping information secret by the use of codes and ciphers. It is a prevalent tool for security engineering today since one can notice that the computer industry has extensively utilized cryptography as a basic standard in secured software development. The main process of cryptography is to encrypt or scramble an input message called 'plain text' with cryptography algorithm, which results in an output message called 'cipher text or cryptogram'. At the receiver side, in order to change cipher text into a readable format, a cryptographic key must be used for decryption. A cryptographic key is created from a string of digits. If the same key is used for both encryption and decryption, it is called a symmetric key. Another kind of key is an asymmetric key, which simply means the encryption key differs from the decryption key. At the present time, a strong cryptography is considerably powerful security technology. The strong cryptography algorithm is based on reliability of mathematical calculation. The calculation of cryptographic key is so complicated that it could not be cracked within a short time. Anyone, who wants to crack it, is supposed to take several years to achieve his goal.

As long as people rely on mathematical complexity, the strong cryptography is still the most efficient tool to safeguard computer security. The immediate or significant arguments against this idea have not yet come forward.

3.2 Firewall

A firewall is a typical border control mechanism or perimeter defence. The purpose of a firewall is to the front line defence mechanism against intruders. It 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. There are basically two different types of firewalls packet filters and proxies. Packet filtering firewalls are those designed to filter IP addresses, MAC addresses, TCP or UDP ports, and subnets, among others. A packet filter is, in principle, a router with the ability to filter or block traffic to and from a network. Packets to a specific service can also be blocked. IP packets to a computer on an internal network with certain options turned on or off could also be screened. Information on the TCP/IP level is used to decide whether to allow or disallow a particular type of traffic. Packet filtering firewalls look at each packet header entering or leaving the network and accept or reject a particular packet based on specific rules defined by the user/network administrator. Packet filtering is fairly effective and transparent to users. They, however, are difficult to configure and are also susceptible to IP spoofing a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. Proxy servers, on the other hand, intercept all the messages entering and leaving the network but it differs in that the proxy hides IP addresses of the clients in the internal network.

3.3 Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure to firewalls, virus scanners, and encryption that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. Attacks can take many forms, as previously discussed. Attack can occur through applications such as Netscape, Internet Explorer, Eudora, or Microsoft Outlook and also via the operating system, regardless of whether it is UNIX, Windows or Mac-based. You also can be attacked via the network through Denial of Service (DoS) attacks or attacks against protocols. IDS products are used to monitor connection in determining whether attacks are been launched. Everything from a simple port scan to a full attack against your Web server can be detected by the IDS system. A flag is raised when an attack is suspected. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack. Software and hardware designed to detect attackers can pick up many levels of intrusions. IDSs will not be capable of detecting certain things, such as information about ISP and IP address range. Public information doesn't really affect the system until the attackers begin to ping the system to see if it is alive. These techniques are used for reconnaissance and mapping out potential targets.

3.4 Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so called anti- Malware tools are used to detect them and cure an infected system. This type of tool acts as an internal defence mechanism. The most common type of anti-Malware software is virus scanners. These tools often consist of two different but related parts: a scanner (or verifier) and a disinfector. Vulnerability scanners are special tools designed to automatically find vulnerabilities in systems.

3.5 Internet Protocol Security (IPSec)

The technology that brings secure communications to the Internet Protocol (IP) is called Internet Protocol Security (IPSec). IPSec as a framework that provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithms(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPSec is a point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPSec can be used in two modes, namely transport mode and tunnel modes. IPSec is a collection of open standards that work together to establish data confidentiality, data integrity and authentication between peer devices.

3.6 Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that actually uses many different standards of key exchange, authentication and encryption to get its job done. The server typically provides regular web service http on port 80, and SSL- encrypted web traffic https over port 443. SSL is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL is a good choice for adding end-to-end protection to applications, it protects against eavesdropping, session hijacking and Trojan servers. SSL can be applied to online security and privacy that provide authentication, integrity, confidentiality and Non-repudiation. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity

3.7 Data Encryption Technology

Data encryption technology categories can be divided in data storage, data transfer, data integrity, authentication and key management techniques. Data encryption is stored in the memory in order to prevent data loss and destruction. The transmission process in the information encrypted is commonly in the form of circuit encryption and port encryption. Data integrity identification technology is to protect information transfer, storage, access, identification and confidential treatment of people and data. In this process, the system is characterized by the parameter value judgment on whether the input is in line with the set value. Data are subject to validation, and encryption enhanced the protection. Key management is a common encryption in many cases. Key management techniques include key generation, distribution, storage, and destruction, etc.

3.8 Intrusion detection technology

Intrusion detection technology is to ensure the safety of the design and the rational allocation. Intrusion detection technology can quickly find anomalies in the system and the authorized condition in the report. It can address and resolve system vulnerabilities in a timely manner. Technologies that are not in line with security policies are frequently used.

IV. CONCLUSION

Security is a very difficult and vital important topic. Everyone has a different idea regarding security' policies, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your need of the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him but Users who find security policies and systems too restrictive will find ways around them. There are different kinds of attacks on the security policies and also growing with the advancement and the growing use of internet. In this

paper, I have mentioned different kinds of attacks that penetrates our system. As the threats are increasing, so for secure use of our systems and internet there are various different security policies are also developing. I have mentioned some of the security policies that can be used mostly by number of users and some new advance qualities that fits to the todays more penetrating environments like Trend micro security mechanism, use of big data qualities in providing security, etc. Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, it is achievable.

V. REFERENCES

[1]. Importance of Network Security, found at http://www.content4reprint.com/computers/security/importance-of-networksecurity-system.htm

[2]. R. Heady, G. Luger, A. Maccabe, and M. Servilla(1990). The Architecture of a Network Level Intrusion Detection System. Technical Report Dept. of Computer Science, University of New Mexico, New Mexico, August.

[3]. Neha Khandelwal, Prabhakar.M. Kuldeep Sharma, “An Overview Of security Problems in MANET”. [4]. Anupam Joshi and Wenjia Li. “Security Issues in Mobile Ad Hoc Networks- A Survey”.

[4]. Ali Ghaffari, “Vulnerability and Security of Mobile Ad hoc Networks”

[5]. Predictions and Trends for Information, Computer and Network Security [Online] available: http://www.sans.edu/research/security-laboratory/article/2140

[6]. A White Paper, —Securing the Intelligent Network‖, powered by Intel corporation.

[7]. Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.

[8]. Network Security: History, Importance, and Future‖, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.

[9]. Ateeq Ahmad, Type of Security Threats and its Prevention”, Ateeq Ahmad, Int.J.Computer Technology & Applications, Vol 3 (2), 750-752.

[10]. Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257

Cite this article as :

Prof. Ganapathi A, "Communication Technology and Network Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 43-49, September-October 2019.

Journal URL : http://ijsrcseit.com/CSEIT19478