International Journal of Computer Sciences and Engineering Systems
Vol. 10 No. 1 (June, 2016)

Overview of Secure Network System

Karan SINGH[1] and Rama Shankar YADAV[2]

[1]Computer Science and Engineering, Motilal National Institute of Technology Allahabad, UP 211004, India
E-mail:karancs12@yahoo.com

[2]G Computer Science and Engineering, Motilal National Institute of Technology Allahabad, UP 211004, India
E-mail:rsy@mnnit.ac.in

Abstract: *After some Days when we will complete all task from ours home or office called information age. This information flow from ours home to others place through the computer network via various communication devices. These computer network device may be wired or wireless in LAN or WAN so we need to protect computer network. We are providing a secure computer network. In this paper we are providing the issues related to computer network security follows by attack, attackers, security goal which in needed for secure computer network system.*

Keywords: *Attacks, Security Standards, Security Elements, Firewall*

1. INTRODUCTION

A coming world is an information world in which every thing as form of information and information walking through a computer network.

A network is set of devices connected by links where devices may be computer, printer or any other devices used for sending and receiving data [3]. That is a computer network means an interconnected collection of autonomous computers which are connected via fiber, optics microwave and communication satellites etc. [2]. The different computers used in computer network are shown by Figure 1 whereas OSI and TCP/IP model is used. Topology defines the architecture of network which is depends upon application environment and access technology. The different types of topology are mesh, tree, ring, star and bus. Also, Computer network can be classified on the basis of domain network such as local area network, campus area network etc. which depend to geographical distance of network. The media use for transmit to information via wired (coaxial cable, fiber) and wireless (microwave, radio frequency) whereas information flow by media via unicast, broadcast, anycast and multicast [9]. The topology is fixed for wired network whereas varying topology is applicable to wireless one. The opponents can be injecting malicious information to the network misuse the information flowing through network. Thus, information required to be security while moving from one network to another network and it's more critical for heterogeneous network. Thus, an efficient, adoptive (able to adjust from attacker to attacker), security mechanism is that provides to the information while adding least overhead. In this paper we summarize the different security mechanism available. Rest of paper is organized as below.

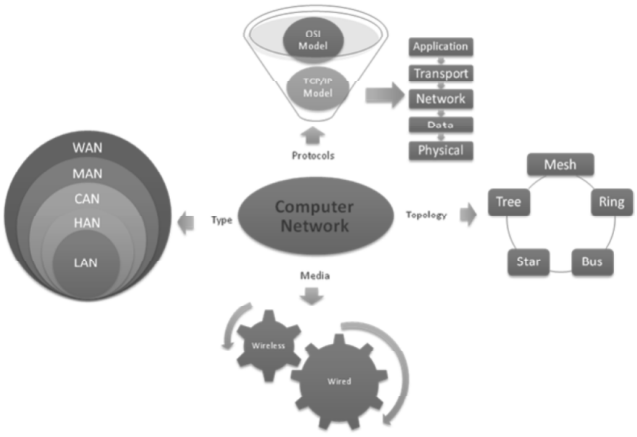

Figure 1: Computer Network System.

Section II deal with security model where as computer security system is given section III. Section IV is providing the secure network system while security analysis tools have been discuss in section V. Finally section VI concludes the paper.

2. SECURITY MODEL

In general protection of assets is called security while protection to information and information device for example, books, faxes, computer data voice communication is the information security. The computer network security protects the network and their services from unauthorized modification, disclosure, access control etc. There are lots

of applications such as banking system, web services, emails etc. where information security is very critical. The network security model is shown by Figure 2.

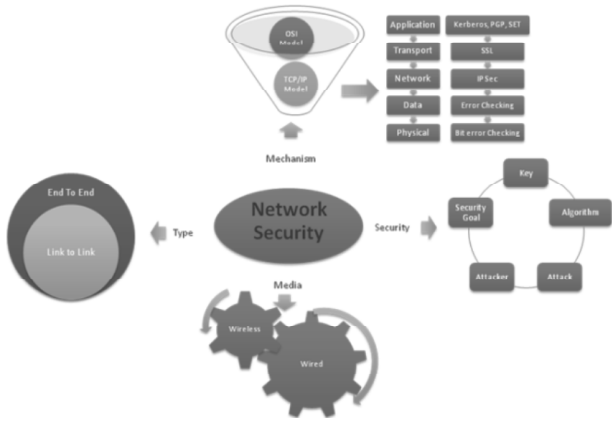

Figure 2: Computer Network Security.

The information security can be achieved system as logical level for example user password, antivirus, firewall etc. These physical and logical in different environment [18] like global, local and electronics. In the age of information threat, vulnerability and attack depends in the next sub section.

2.1 Threat

The Disturb of operation, function, integrity, availability of network system is called threat also known as warning. The natural threats, occurrences such as floods, earthquakes, and storms are threat for damage of environment. There are also unintentional threats that are the result of accidents and stupidity whereas unintentional types of threats [16] are replaced as results of decedent or stupid information security faces all these kind of malfunction, water damage virus worm spoofing, tunneling, equipment software, civil damage etc.

2.2 Vulnerability

The weakness [12] of system which may be occurs as results of poor design, implement, management of computer system such as protocols, drivers, media etc. For example, boot sector, application software, manufacture equipment others inefficient antivirus or absence of antivirus.

2.3 Attacks

Attacks are technique that breaks the security mechanism employed to the system for example: denial of service, password cracking, SPAM, forgery and replay are the basic attacks. The efficiency of attacking technique is based on the following

1. How does look?
2. Where does store?
3. How does this work?
4. Where does implemented?
5. How does implemented?
6. What does the size of attack?

Table 1
Example for Attack

Attack	*Description*
Email-Worm. Win32.Mydoom.l	This worm spreads via the Internet as an attachment to infected messages, via file sharing networks and open network resources. The worm sends itself to email addresses harvested from infected machines. The worm also contains a backdoor function. The worm itself is a Windows PE EXE file approximately 21 KB in size.
Trojan.Win32. Krotten.cl	This Trojan has a malicious payload. It is a Windows PE EXE file. It is 137728 bytes in size. It is written in C++.
DoS.Win32.VB.z	This malicious program is designed to conduct Denial of Service attacks on a remote server. It is a Windows PE EXE file. It is 40960 bytes in size. It is written in Visual Basic.

The above feeling of attacks (Worm.Win32.Mydoom, TorzanWin32 and Denial of Service) [2] whose brief description is given in Table 1. Further details about attacks are given in Table 4 in section III.

3. COMPUTER NETWORK SECURITY

Computer network securities have the many component such as mechanism, security package (security goal, key, algorithm, attack, attackers), media, type etc. Computer network use the TCP/IP suite divided in various five layers. Computer network use the TCP/IP suite divided in various layers.

We have surveyed some standards [10] to provide the security according to these layered. Basic concept of computer network security is cryptography where information is changed to another pattern at services while reverse of it is being done at receivers to achieve exact information. The cryptography system required encryption/ decryption schemes which are furthers enhances take more advanced threats and attacks. Security standards [10, 15] for each layer along with its provider are given Table 2. For example: IPSec, XML, signature security standards are provided by International Engineering Task Force (IETF). The complete lists for standard along with application domain are given in Table 3. For example: Kerberos, IPSec, S/MIME, PGP are used to provide network security while X 5.09, RSA, BSAFE, DSA, and XML are used is used in digital signature.

Furthers network security can be divided in two category first is link to link (L2L) second is end to end (E2E). Link to link security deals with protection of nodes shared by link whereas source to destination type of protection is received for cause of end to end security. For example : L2L deals between node A to N1 whereas Node A to Node B security is provided through end to end concept details security is given in Figure 3.

Table 2
Organization and Standards

Organization	*Standards*
IETF	IPSec, XML Signature XPath Filter 2,X,509, Kerberos, S /MIME,
ISO	ISO 7498-2 :1989 Information Proccssing Systems –Open Systems Interconnection,ISO /IEC979 11xx, ISO/IEC DTR 13xxx,13xxx,ISO/IECDTR14xxx
ITU	X,2xx,X.5xx,X.7xx,X.80
ECBS	TR-40x
ECMA	ECMA-13x,ECMA-20x
NIST	X3 Information Procession, X9.xx Financial, X12,xx Electronic Data Exchange
IEEE	P1363 Standard Specification, FOR Public-Key Cryptography, IEEE 802.xx IEEEP802, 11g, wireless LAN Medium Access Control(Mac) and Physical Layer(PHY) Specifications,
RSA	PKCS#x –Public key cryptographic Standard
W3C	XML Encryptions, XML, Signature ex Xensible Key Management Spécification (XKMS)

Table 3
Standards and Services

Security Standard	*Services*	*Area Application*
Kerberos	Network authentication	Internet Security
IPSec	Secure TCP/IP communication over the Internet	
S/MIME,PGP	Privacy-enhanced electronic mail	
3-DES, DSA, RSA, MD-5, SHA-1, PKCS	Public key cryptography standard	
S-HTTP	SECURE Hypertext Transfer Protocol	
X.509/ISO/IEC/ 9594-8: 2000:	Authentiquassions of directory user	
SSL,TLS,SET	Security protocol for privacy on Internet/ transport security	
X509,RSA,BS AFE Secure XMLC,DES, AES,DSS/DSA, EESSI,ISO, SHA/SHS, XMLDigital Signature (XMLDSIG), XML Key Management Specification (XKMS)	Advanced encryption standard/PKI/digital certificates, XML digital signature	Digital signature and encryption
SAML, FIPS 112	Authentication of user's right to use system or network resources	Login and authentication

Play on important role to provide connectivity. Wired media faces both physical as well logical [7] types of threats whereas logical type problem in received most of time in the case of wireless [8]. In the case of wired physical threat is theft, physical access of network system and they(major problem in wired) can be take through providing security in person, locks. However, the chance of logical threating is vary less for wired network as compared to that received for the case of wireless, thus major concern over information security is on logical that can be take through security software.

The region for facing more threat in wireless network [8, 17] is given below:

A. Vulnerability of Nodes

Since the network nodes usually do not reside in physically protected places, such as locked rooms, they can more easily be captured and fall under the control of an attacker.

B. Vulnerability of Channels

As in any wireless network, messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to network components.

C. Absence of Infrastructure

Wireless networks are supposed to operate independently of any fixed infrastructure. This makes the classical security solutions based on certification authorities and on-line servers inapplicable.

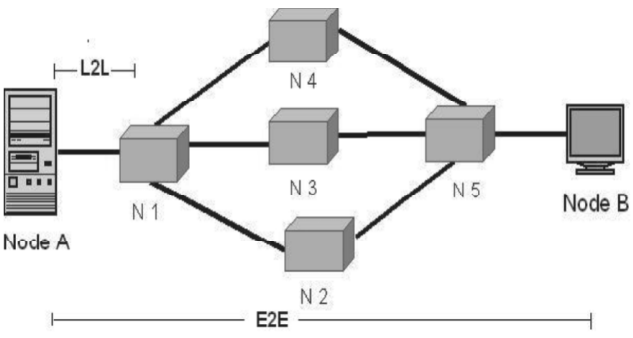

Figure 2: E2E and L2L Security

Table 4
Attacks

Attack	*Description*
Virus	A program that can't function independently to disturbs security
Worm	A program self contain and independent to disturbs security
Torzon Horse	A program or code fragment that inside a program
Trap Doors	Undocumented way of gaining access to system that built into the system by its designer
Logic Bomb	Program or subsection of program, it work when logic occurs
Port Scanning	Program that listen to well known port no. to detect services running on a system
Spoofing	Identity or masquerading as some other individual entity gain access to a system or network
Password Cracking	A program that decrypt the encrypt program
Social Engineering	Collect all social information related to person to crack computer network system
Sniffing	A process to monitoring a network in an attempt to gather information that may be useful in an attack
Ping of Death	Identity as some other individual entity gain access to a system or network
Denial of Service	Not to gain access or information but to make a network or system unavailable for use by other users
SPAM	We got unwanted emails in our message inbox such as rediffmail.com provides the spam mail index.
Forgery	A technique to make Froude
Replay	An attacker that performs a replay attack injects into the network routing traffic

D. Dynamically Changing Topology

Wireless networks, the permanent changes of topology require sophisticated routing protocols, the security of which is an additional challenge.

E. Non Repudiation

Its provide proof of origin and delivery of service and/or information. Source or receiver can't deny of message for sending or receiving due to non repudiation.

We are providing the table which illustrates the development of our CAMAN from basic to complex architecture level [6]. The architecture of secure network system is given in next section.

4. SECURE NETWORK SYSTEM

A secure network provide the security goal which implemented by two way one is firewall, it may be hardware and software at various layers others is security standards which provides security at each layers and created by standards organization such as IPSec, SSL, transport layer security (TLS) etc. Here we are providing an example for secure network system in Figure 4.

Table 5
CAMAN Implement

	Authentication	*Authorization*	*Confidentiality*	*Message Integrity*	*Non-Repudiation*
Architecture			RAS PKI FPKI SET WLAN/802.11		
Inte-grated	Firewalls: Packet filter, Circuit-level gateway, ALG Higher-layer VPN's: IPSec, SSL, TLS, TTLS, PEAP, SSOs: OGSF SSO, SSG, GSS-API				
Enhanced	UserID and Password: CHAP, Kerberos EAP Digital certificate	UserID and Password: CHAP, Kerberos Token card	Encrypted VPN: MPPE Key management: ISAKMP, OAKLEY, IKE, SKIP, STS Wi-Fi WEP, 802.11i	Digital Signature: RSA, DSA, ECDSA MAC	Digital signature: RSA, DSA, ECDSA MAC
Basic	Authentication headers: AH, ESP Packet filtering : Static, dynamic UserID and Password	Physical access control UserID and Password: PAP, SPAP ACLs DMZ	Hashing algorithm: MD5, SHA(SHA-1, SHA-256, SHA-384, and SHA-512) Secret-key Cryptography: RSA, DSA, ECDSA, key exchange: Diffie-Hellman	L2 VPNs: FR, ATM, MPLS, Ethernet VLAN Tunneling protocols: PPP, PPPoE, PPP over SONET/SDH, GRE, PPTP, L2TP Authentication headers: AH, ESP	Digital Signature MAC NAT and PAT

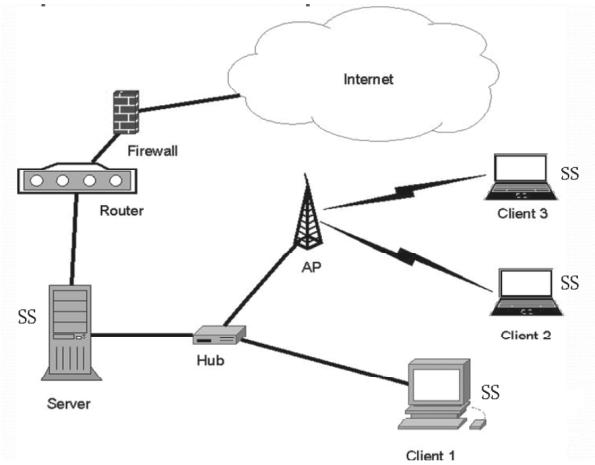

Figure 4: Secure Network System

A particular difficulty is that incorrect routing information can be generated by compromised nodes or as a result of some topology changes and it is hard to distinguish between the two cases.

The main part of network security is a security package such as key, algorithm, attacker and goals. An attacker such as hacker or cracker disturbs the network security via attacks [5, 13] summarizes in Table 4. An attack may be passive means no change in data or information only monitoring but in case of active change also possible.

We make cryptographically algorithm to provide the security goal [7, 14] in network system using keys. There are lot of keys available to achieve the security goal public, private, master, session and shared. The security goals are a CAMAN (confidentiality, authentication, message integrity, authorization, non-repudiation) is described as below:

A. Confidentiality

We maintained the secrecy using the Confidentiality. Confidentiality protects system data and information from

B. Authentication

With help of authentication we identify the user identity. It is used to identify a user such as source or receiver or receiver is right to access or use the network system services.

C. Massage Integrity

Our data is original or not means there is no modification, deletion, insertion. We help of message integrity; we check the message originality at destination side

D. Authorization

Our system is used by an authentic user. We prevent of unauthorized use of resource with help of authorization.

E. Non Repudiation

Its provide proof of origin and delivery of service and/or information. Source or receiver can't deny of message for sending or receiving due to non repudiation.

We are providing the table which illustrates the development of our CAMAN from basic to complex architecture level [6]. The architecture of secure network system is given in next section.

4. SECURE NETWORK SYSTEM

A secure network provide the security goal which implemented by two way one is firewall, it may be hardware and software at various layers others is security standards which provides security at each layers and created by standards organization such as IPSec, SSL, transport layer security (TLS) etc. Here we are providing an example for secure network system in Figure 4.

This system has the various parts which are following.

4.1 Client

A client is a personal computer which has the operating system and internet connection. Internet is used by internet browsers which have the facility to provide the security from opponent via SSL, TLS etc. standards and security, privacy option.

4.2 Hub or Access Point

A hub or switch connects the more than two computers for infrastructure networking. Access point connect the various computer without wire which have the range and own ID to connect the clients.

4.3 Server

A server receives the client requests and responses the client to providing the request response (services) form internet or local area. The proxy server is used to reduce the load of server. Also server has the security standards such as client to providing the protection of LAN.

4.4 Router

A router connects our home network to internet (global network). A router maintains the statics or dynamic routing table for local network and decides the path for client or server request packet. Lot attack may be occurs on routing table such as routing poisoning, routing overflow due to denial of service etc. so we need the firewall inside (LAN) and outside (Global).

4.5 Firewall

A firewall is usually placed between two networks to act as a gateway. The principal requirements of an effective firewall are described as follows

(A) It must act as a door through which all traffic must pass (incoming and outgoing).
(B) It must allow only authorized traffic to pass.
(C) It must be hide the inside network architecture characteristics from outside network (internet).

A firewall may be hardware and software for example Norton firewall, Window firewall, MacAfee firewall work as software and Router, Broadband, ISA 2004, PICK etc.

firewall works as hardware. We are providing a firewall category [15] according to TCP/IP layers in Table 6.

Table 6
Firewall and TCP/IP layers

Layer	*Firewall Services*
Application	Application-level gateways, encryption Socks, Proxy Server
Transport	Packet Filtering (TCP, UDP, ICMP)
Network	NAT, IP-Filtering
Data Link	MAC Address Filtering
Physical	May not be available

4.6 Internet

Internet is outside network which connect ours clients to others end. Through internet hackers/crackers break ours network the security using various analyses.

The purpose of secure network system is to provide the secure communication between clients at both ends. For example if clients is situated in a India city and others client in USA city. If they want to chat or mail to each others, they need the security at different-different level. According to Figure 3, we need the security at client, server using security standards and firewall at both side in LAN or WAN. The next section is dealing with security analysis tools.

5. SECURITY ANALYSIS TOOLS

Security can provide using the cryptography system and computer forensic.

In this paper we have discuss the cryptosystem but we can also provide a security via forensic tools [11, 12] which are given in Table 7. With help of these tools, we can analysis of our network to provide security from attacks. There are a lot of tools available for monitoring network but few are listed in Table 7.

Table 7
Security Analysis Tools

Tools	*Description*
Web packet sniffer	These are a pair of Perl scripts that together will listen to all TCP/IP traffic on a subnet, intercept all outgoing requests for Web documents and display them, intercept all incoming requests for Web
Cerberus Internet Scanner (CIS)	CIS is a free security scanner written and maintained by Cerberus Information Security, Ltd and is designed to help administrators locate and fix security holes in their computer systems. Runs on Windows NT or 2000.
Fremont	Fremont is a research prototype for discovering key network characteristics, such as hosts, gateways, and topology
HPing	hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols,
Netcat	Netcat is a program to create network connections, TCP or UDP, to or from any port number. It is most commonly used with other commands as part of a script
Internet Security Scanner (ISS)	This is a program by Christopher Klaus. A multi-level security scanner that checks a UNIX system for a number of known security holes such as problems with send mail, improperly configured NFS file sharing, etc
Nessus	Nesses is a free, open sourced and easy-to-use security auditing tool for Linux, BSD and some other system
nmap	nmap is a utility for port scanning large networks using various scanning techniques. nmap also supports a number of performance and reliability features such as dynamic delay time calculations
SAINT	SAINT is the Security Administrator's Integrated Network Tool. In its simplest mode, it gathers as much information about remote hosts and networks as possible by examining such network services as finger, NFS, NIS, ftp and tftp, rexd, statd, and other services
SARA	"Security Auditor's Research Assistant"-security audit tool, GPL license.It remotely probes systems via the network and stores its findings in a database.
SATAN	SATAN, the System Administrator Tool for Analyzing Networks, is a network security analyzer designed by Dan Farmer and Wietse Venema
YAPS	YAPS stands for Yet Another Port Scanner
John the Ripper	Another version of UNIX password cracker.
passwd+	Passwd+ is a proactive password checker which replaces the system passwd command
Xavior(BETA)	A remote password auditing and recovery tool that allows dictionary or complex brute-force scans. Scripting support allows you to define any plaintext login procedure
Tripwire	The Tripwire package from Purdue University. Scans file systems and computes digital signatures for the files therein, then can be used later to check those files for any changes.
VIPERDB	ViperDB was created as a smaller and faster option to Tripwire
AppScan	AppScan is the most comprehensive web application security testing and vulnerability assessment tool. It explores applications,automatically creates and customizes tests and provides comprehensive actionable results in the form of detailed and custom reports
Achilles	Achilles is a tool designed for testing the security of web applications
Nessus:	The premier Open Source vulnerability assessment tool Nessus is a remote security scanner for Windows, Linux, BSD, Solaris

6. CONCLUSION

In this paper we have discuss a secure network system which is needed for today's information age. We have summarized the various security standards and firewall. The paper is a basic Skelton for the researchers working in area of secure information system and tries to aware the security system for researching environment.

REFERENCES

[1] S. Tanenbaum, *Computer Network*, 4rd Edition, PHI publication.

[2] Attacks: *http://www.viruslist.com*

[3] Forouzan, *Data Communications and Networking*, 4th Edition, TMH Publication.

[4] Christopher Leidigh, *Fundamental Principal of Network Security*, white paper #101 American Power Conversion 2005.

[5] John E. Canavan, *Fundamentals of Network Security*, ISBN 1-58053-176-8, 2005.

[6] K. T. Fung, *Network Security Technology*, 2nd edition, Auerbach Publication.

[7] Karan Singh, R. S. Yadav, Ranvijay, "A Review Paper on Ad-Hoc Network Security", in *International Journal of Computer Science and Security*, Volume (1): Issue (1) pg. 52-69 Malaysia–2007.

[8] R. Shiva Kumaran, Rama Shankar Yadav, Karan Singh "Multihop Wireless LAN" *HIT haldia* March 2007.

[9] Karan Singh, Rama Shankar Yadav, Raghav Yadav, R. Shiva Kumaran, "Adaptive Multicast Congestion Control", *HIT haldia* March 2007.

[10] Sagi Bar, *Enforcing Network Security on Connection*, White Paper Intel Information Technology Feb. 2007.

[11] Security tools from: *http://www. cert- in.org*

[12] *NSIT ITL Security Bulletins*, The Common Vulnerability Scoring System (CVSS), October 2007.

[13] R. Stewart, M. Tuexen, G.C. Ericsson, *Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures*, RFC-5062 September 2007.

[14] William Stalling s, *Cryptography and Network Security*, 4th Edition, Person Publication.

[15] Joseph M. Kizza, *Computer Network Security*, ISBN 13: 978-0387204734 edition 1st Springer; 2005.

[16] Threats: *http://www.caci.com/business/ia/threats.html.*

[17] Shin, Justin, A. Mishra, A. William, "Wireless Network Security and Interworking", *Proceedings of the IEEE*, Vol. 94, No. 2, February 2006.

[18] Y. Hung , "Network Attack and Countermeasure", *IEEE Proceeding* 2007.