© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

PREVENTION OF SECURITY THREATS IN NETWORKS AND ELIMINATION PERFORMANCE ISSUE OF TRADITION SECURITY SYSTEM

,Mohd Iqbal Mir [1], Sohrab Ansari[2] ,Bandhanjot Singh [3]
AL-FALAH UNIVERSITY
Al-Falah School of Engineering & Technology
Iqbalmir06@gmail.com [1], Sohrab.ansari90@gmail.com[2], bandhan13@gmail.com[3]

Abstract: Networking is a process of information & ideas among individuals or groups that share common interests. Networking has been two categories: social or business. In this paper we have discussed the threats to the security of network and different security mechanisms. The research is that if there is secure transmission then the speed of data transfer gets degraded. But if packet size is reduced then the speed of data transmission could be improved in contrast of secure traditional work. Here we have discussed how to improve the security of networks

[1] NETWORK SECURITY

Networking is a process that fosters exchange of information & ideas among individuals or groups that share common interests. Networking may fall into one of two categories: social or business. Less commonly in finance, term "networking" may also refer to setting up & operation of a physical computer network. One line may intersect with another, & then second line goes in a different direction to connect to more lines, & soon & so forth to form a netlike structure. Metaphorically, someone's network remains connected through a series of symbolic ties. Business connections may form due to someone's education, employer, industry or common colleagues.

[2] LITERATURE REWIEW

In this section we have discussed existing work related to wired & wireless network. Satish Ms. Sonal Rane

Performance Evaluation of Wired & Wireless Local Area Networks Very large scale integration of complex circuits on to a smaller chip demands for evolution of high speed computer networks. Traditional wired network constraints like mobility & expensive cabling.

In 2006 Wormhole Attacks within Wireless Networks Yih-Chun Hu, [4]

As mobile ad hoc network applications are deployed requirement. We introduce wormhole attack, a severe attack within ad hoc networks that is particularly challenging to defend against. Wormhole attack is feasible even if attacker have been not compromised numerous hosts & although all communication provides dependability and confidentiality.

Wireless Local area network Security Overview was introduced by Ahmed M. Al Naamany, Ali Al Shidhani, Hadj Bourdoucen

Wireless Local Area Networks are cost effective & popular gateways to mobile computing. They allocate computers to be mobile, wireless & communicate with speeds close to speeds of wired LANs. These

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

features came with expensive price to pay within areas of security of network.

In 2010 security & privacy in emerging wireless networks article was written by di ma university of michigan-dearborn [2]

Wireless communication is continuing to make inroads into many facets of society & is gradually becoming more & more ubiquitous. Whereas within past wireless communication was for the mainly part of limited to first & last transmission hops, today's wireless networks are starting to offer purely wireless, often mobile, & even opportunistically connected operation. Purpose of this article was to examine security & privacy issues within some new & emerging types of wireless networks, & attempt to identify directions for future research.

[3] TYPES OF ATTACK

Five types of attacks are as follow:

- **Passive Attack**

A **passive attack normally** monitors unencrypted traffic & looks for clear-text passwords & insightful information which could be used in different types of attacks. **Passive attacks** consists of traffic analysis, decrypting weakly encrypted traffic, monitoring of unprotected communications & capturing authentication information like passwords. This interception of network operations by and large enables adversaries to view approaching procedures. Passive attacks usually result in information disclosure or data files to an attacker. It is done without knowledge of user.

- **Active Attack**

In an **active attack** attacker generally tries to bypass/break into secured systems. It could be performed through stealth/viruses/worms/Trojan horses. Active attacks consist of attempts to circumvent to introduce malicious code,& to steal information. Such attacks are mounted against a network backbone, electronically penetrate an enclave, exploit information in transit or attack an authorized remote user when an attempt to connect to an enclave. Active attacks would result in disclosure/dissemination of data files and modification of data.

- **Distributed Attack**

A **distributed attack** requires that adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies & users circulation attacks targeting on malicious modification of hardware & software at factory or at some point in distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

- **Insider Attack**

An **insider attack** involves someone from inside, for example a discontented employee, attacking network Insider attacks can be malicious or not malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks obviously results from lack of care, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

- **Close-in Attack**

A **close-in attack** involves someone attempting to get physically close to network components, data, & systems in order to learn more about a network

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

Close-in attacks consist of regular individuals attains close physical closeness of networks, systems, or services for function of modifying, congregation, or denying access to information. Close physical proximity is achieved through surreptitious entry in to net work, open access, or both.

One popular form of close in attack is **social engineering** in a social engineering attack, attacker compromises network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by individual to revealing information about security of company. Information which victim reveals to hacker would be used in a subsequent attack in order to gain unauthorized access to network.

- **Phishing Attack**

In phishing attack hacker develops a fake web site that looks exactly like a popular site such as SBI bank or pay pal. Phishing part of attack is that hacker then sends an e-mail message trying to trick user into clicking a link that leads to fake site. When user attempts to log on with their account information, hacker records username & password & then tries that information on real site.

- **Hijack attack**

Hijack attack in a hijack attack, a hacker takes over a session between you & another individual & disconnect so there individual from communication. You still believe that you are talking to original party& can send private information to hacker by accident.

- **Spoof attack**

Spoof attack In a spoof attack, hacker modifies source address of packets he or she is sending so that they appear to be coming from someone else. This can be an attempt to bypass your firewall rules.

- **Buffer overflow**

Buffer overflow a buffer overflow attack is when attacker sends more data to an application than is expected. A buffer overflow attack usually results in attacker gaining administrative access to system in a command prompt or shell.

- **Exploit attack**

Exploit attack are those type of attack in which attacker knows a security problem by having knowledge of exploiting vulnerability.

- **Password attack**

Password attack: - In this type of attack an attacker tries to crack passwords which is stored in a network account database with a password-protected file. Major types of attacks are password attacks: a dictionary attack, a brute-force attack, & a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. In brute-force attack attacker tries every possible combination of characters.

[3] **CRYPTOGRAPHY**

It had been discipline of information security had been called Cryptography. Meaning of Cryptography had been “hidden” imitative from Greek crypto’s. Cryptography means hide information within storage or transfer including methods such as microdots, integration of words with image.

Cryptography had been process of altering plaintext (ordinary text, just as letter) using process encryption into cipher text using procedure decryption. This procedure had been used to secure communication between two parties within occurrence of third party. There are four goals for Modern cryptography:

Confidentiality

It identifies that only participants (Sender & Receiver) should be able to access message.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

Integrity

Content of message should not be changed. If it had been altered, then it had been called type of modification attack.

Non-repudiation

There had been situation where sender converts content of message & after that he refuses that he had not sent message.

Authentication

Both sender & receiver had to prove credentials to each other.

In current times, cryptography had been basic requirement of computer experts for security purposes so that two parties could send data to each other without any modification & confidently. So both sender & receiver could validate to each other for secure communication so that material could be safely send to each other.

[4] RESEARCH METHOLOGY

Client Server Model

It is possible for two network applications to begin simultaneously, but it is impractical to require it. Therefore, it makes sense to design communicating network applications to perform complementary network operations in sequence, rather than simultaneously. The server executes first & waits to receive; client executes second & sends first network packet to server. After initial contact, either client or server is capable of sending & receiving data.

Symmetric Key Cryptography

Server authenticate user & user authenticate server generating a very strong session key using their shared password over an insecure channel by using symmetric cipher.

A special function issued by having distortion & picture subroutines used as password in order to save password from offline dictionary attack.

Work is implemented in one of major used language named java.

This model would create a separate layer for data transmission & hacker would not be capable to access data on wireless network without application layer required on client.

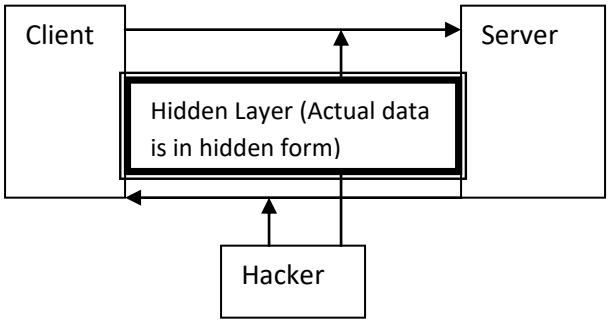

Fig 1 Proposed Model

Port based security

In this implementation data would be transferred to and from particular port. 0 to 1023 port are reserved for existing services. Here we are using port above 1024 in order to implement secure port transmission. So hacker would not be able to access data from that particular port as that port is open to authentic client. More over data is in non understandable from during transmission. Data is encrypted while sending and decrypted at recipient end.

Encryption Steps

Step 1 Encryption[11] of plaintext that is to be send by sender using encryption from secret Key which is actually sender's private key & thus generating cipher text using DES[12,13].

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

Step 2 Further, it will carry out procession secret Key which is receiver's public key & thus encrypting algorithm.

Step 3 A digital envelop is sent to receiver having cipher text & Key so encrypted.

1. TOOLS AND TECHNOLOGY

- HARDWARE
- CPU (1GB)
- Harddisk (10 gb free space)
- RAM (2 GB)
- High resolution monitor

SOFTWARE

- WINDOW 7
- JAVA
- NET BEANS
- MS ACCESS

[5] SCOPE OF RESEARCH

In this implementation packet transmits environmental data to destination. The content of packets have been replaced by corresponding small string in order to reduce the size of packet to be transmitted on network. The research is that if there is secure transmission then the speed of data transfer gets degraded. But if packet size is reduced then the speed of data transmission could be improved in contrast of secure traditional work.

As security mechanism is user defines so further security layer could be added within future. Such security mechanism may be applicable of o ther server like FTP Server, telnet, SMTP Server. Our security mechanism will first prevent hacker to access data within unauthenticated way & restrict them to understand data. Hacking has both its benefits & risks. Hackers are very diverse. They might bankrupt company or might protect data, increasing revenues for company. Battle btw ethical or white hat hackers & a malicious or black hat hacker has been long war that has no end. While ethical hacker help to understand companies' their security needs, malicious hackers intrudes illegally & harm network for their personal benefits.

REFERENCE

1. Artemios G. Voyiatzis, "A survey of delay – disruption tolerant networking applications", Journal of Internet engineering, Vol 5 no 1, pp: 331-343, June 2012.
2. K.Fall, "A Delay Tolerant Network Architecture for Challenged Internets", in Proceedings of ACM SIGCOMM, pp: 27-34, August 2003.
3. Evan P.C. Jones, Paul A.S. Ward, "Routing Strategies for Delay – Tolerant Networks", University of Waterloo, Canada.
4. RFC 4838, V. Cerf, S. Burleigh, A. Hooke, L.Torgerson, NASA Jet Propulsion Laboratory (NASA/JPL), R. Durst, K. Scott, MITRE Corporation, K. Fall, Intel Corporation. , H. Weiss, SPARTA, Inc. "Delay – Tolerant Networking Architecture", April 2007
5. Lloyd Wood, et. al, "Use of Delay Tolerant Networking Bundle Protocol from Space", IAC – 08 B2.3.10, Global Government Solutions Group, Cisco Systems, UK.

6. **S.** Heatly & D. Stokesberry, 'Analysis of Transport Measurements Over a Local Area Network,' I€€€ **Commun. Mag.,** June **1989.**
7. H. Kanakia & D. R. Cheriton, "The VMP Network Adapter Board (NAB): High-Performance Network Communication for Multiprocessors,' **Proc. SIGCOMM** '88, Stanford, CA, Aug. **16-19,**
8. K. Sabnani, M. H. Nguyen, & C. D. Tsao, 'High-speed Network Protocols," **6th** /€€€ **lnt% Workshop on Microelectronics & Photonics in Commun.,** New Seabury, MA June **6-9, 1989.**
9. Tantawy, H. Meleis, M. El Zarki, & G. Rajendran, "Towards a High-speed MAN Architecture," **ICC,** Boston, MA, June **11-14, 1989.**
10. V. Jacobson, "Congestion Avoidance & Control," **Proc. SIGCOMM** '88, Stanford, CA, Aug. **16-19, 1988.**
11. D. D. Clark, J. Romkey, & H. Salwen, -An Analysis of TCP Processing Overhead," **Proc. 13th Conf. on Local Comp. Networks,** Minneapolis, MN, Oct. **10-12, 1988.**
12. D. R. Cheriton & C. L. Williamson, 'VMTP as Transport Layer for High-Performance Distributed Systems,' **IEEE Commun. Mag.,** vol. **27,** no. **6,** June **1989.**
13. D. D. Clark, M. L. Lambert, & L. Zhang, "NETBLT: A High Throughput Transport Protocol," **Proc. SIGCOMM** '87and **Commun. Rev.,** vol. **17,** no. **5,' 1987.**
14. G. Chesson, 'XTP/PE Overview," **Proc. of 13th Conf on Local Comp. Networks,** Minneapolis, MN, Oct. **1988.**