International Journal of Research in Science advanced Technology and management studies (IJRSTMS)

ISSN: 2459-425X • Website: www.ijrstms.com

A Preliminary Study on Network Security Attacks & Preventive Measures

Prof.V. Vinay Krishna
Assistant professor, Dept. of CSE
Christhu Jyoti Institute of Technology &Science
Jangaon, India

Dr Julie
Assistant professor, Dept. of CSE
Christhu Jyoti Institute of Technology &Science
Jangaon, India

ABSTRACT

Nowadays, computers are available everywhere ranging from small shops to large organizations. Computer security is one of the most expected factors in the current & future industry. Systems connected to networks suffer a lot from attacks. Networks are necessary, but still they are not considered much safer to provide security to the users because of the many flaws in a conventional system. Network attacks had become a curse to technology, where the attacker destroys or gain illegal access to system recourses and restrict the legitimate users from accessing the information.In this paper, we are going to existent various attacks the operation that were used for data security.

Keywords: Algorithms, protocols, Security Attacks, Networks, Hackers.

I. INTRODUCTION

There are many kinds of attacks in networking. We can classify into wired and wireless attacks. The network is a basic components involved in connecting computers across small and large distances around the world [1]. Networks are used to access the information from various places around the world. Types of networks can be classified as *Personal area network (PAN):* This type of network Connects the devices of a system internally and external devices like printer, modem, telephone, etc..

Local area network (LAN): This network connects and able to transfer data between systems within Some range of systems likes within offices and campus.

Wide area network (WAN): *A wide area network (WAN) is a geographically distributed private telecommunications network that interconnects multiple local area networks (LANs). In an enterprise, a WAN may consist of connections to a company's headquarters, branch offices, collocation facilities, cloud services and other facilities. This network is expanding in a fashion which connects the whole world.*

Metropolitan area network (MAN): *A MAN is ideal for many kinds of network users because it is a medium-sized network. MANs are used to build networks with high data connection speeds for cities and towns.The working mechanism of a MAN is similar to an Internet Service Provider (ISP), but a MAN is not owned by a single organization. Like a WAN, a MAN provides shared network connections to its users. A MAN mostly works on the data link layer, which is Layer 2 of the Open Systems Interconnection (OSI) model.*

Global area network (GAN): *A global area network (GAN) refers to a network composed of different interconnected networks that cover an unlimited geographical area. This connects systems worldwide like WAN but the connections are wireless where mobile communications are implemented.*

Virtual private network (VPN): A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. This network is useful for companies in which two companies want to communicate privately in public networks and expects safe communications.

Hackers: Hacking generally refers to the unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.Hacking can also refer to non-malicious activities, usually involving unusual or improvised alterations to equipment or processes.

Cracker: Detects vulnerability and take advantage over it.

- The following Hacker types are considered to develop the secure system.
- Black Hat Hackers: criminals and wrongdoers
- White Hat Hackers: ethical hackers who work to protect systems and people
- Gray Hat Hackers: dabble in both black hat and white hat tinkering
- Blue Hat Hackers If a Script Kiddie took revenge, he/she might become a Blue Hat.
- Vulnerability–Weak point used as an entry point Threat –Attacks Control 4 types of attacks
- Interception: Watches packets
- Interruption: Steals or disturbs the data.
- Modification: changes the data
- Fabrication: sends message apart from the original, but having the same sender name.

Attacks on Password:

To understand how to protect yourself from a password attack, you should become familiar with the most commonly used types of attacks. Loose Lipped Systems: When System asks for password and username to type in the system accepts username before the password is typed in where unrevealing the user name. Exhaustive Attack: Tries all types of passwords Probable likely for the user: Thinks of user familiarities and guesses what the password the user could might have chosen. Plain text system password list: Accesses the password database directly.

Defending mechanisms:

Password selection criteria: Carefully selecting password where one cannot guess so. One time

Passwords: On every access change password by giving a function and the user solves. Encrypted Password File: Even when the database is accessed the passwords cannot be accessed when it is stored in an encrypted form.

Attacks Phishing and Pharming:

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate site Unsuspecting user submits sensitive information in to a fraud system believing it is a trustworthy one.

Pharming

Domain Name Server (DNS) spoofing is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

Packet sniffing

Packet sniffing, a network attack strategy, captures network traffic at the Ethernet frame level. After capture, this data can be analyzed and sensitive information can be retrieved. A network attack starts with a tool such as Wireshark. Wireshark allows you to capture and examine data that is flowing across your network. Any data that is not encrypted is readable, and unfortunately, many types of traffic on your network are passed as unencrypted data,even passwords and other sensitive data.Obviously, this situation represents a danger to your corporate data. Many applications that house corporate data still use Telnet as the data transfer mechanism. Telnet is a clear text, unencrypted data transfer mechanism. A person with a packet sniffer can view this data as it crosses your network.

Attacks Phishing: The unsuspecting user submits sensitive information into a fraud system, believing it is a trustworthy one.

Pharming: Also called as DNS Spoofing. It changes the DNS address of the original website. Redirects to fake Website.

Packet sniffing: Hackers observers conversation between two conversations.

II. PREVENTIVE MEASURES Data Encryption Standard (DES:)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm Since DES is based on the Feistel Cipher, all that is required to specify DES is

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

AES (Advanced Encryption Standard)

AES is also known by its original name Rijndael is a specification for the encryption of electronic data For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES encrypts 128 bit data block for a minimum of 10 to a maximum of 14 rounds according to the key size. AES can be implemented on small device platforms such as smart cards. AES is fast and flexible. AES has been tested for many security applications. In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered.

Blowfish

With the rapid growing of internet and network applications, data security becomes more Important than ever before. Encryption algorithms play a crucial role in information security systems. Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Block Cipher Speed Comparison. 18 clock cycles per byte of encryption on a Pentium. 8.3 Megabytes per second on a Pentium 150.It can be used in compact devices with memory less than 5 kb.No attack is successful againt Blowfish,although it suffers from weak key problem.

IDEA (International Data Encryption Algorithm)

IDEA (International Data Encryption Algorithm) is one of the strongest secret-key block ciphers. The mentioned algorithm works on 64-bit plain text and cipher text block (at one time). For encryption, the 64-bit plain text is divided into four 16 bits sub-blocks. In our discussion, we denote these four blocks as P1 (16 bits), P2 (16 bits), P3 (16 bits) and P4 (16 bits). Each of these blocks goes through 8 ROUNDS and one OUTPUT TRANSFORMATION phase. In each of these eight rounds, some (arithmetic and logical) operations are performed.

Throughout the eight ROUNDS, the same sequences of operations are repeated. In the last phase, i.e., the OUTPUT TRANSFORMATION phase, we perform only arithmetic operations. At the beginning of the encryption process, the 64 bit plain text is divided in four equal size blocks and ready for ROUND1 input. The output of ROUND1 is the input of ROUND2. Similarly, the output of ROUND2 is the input of ROUND3, and so on. Finally, the output of ROUND8 is the input for OUTPUT TRANSFORMATION, whose output is the resultant 64 bit cipher text (assumed as C1 (16bits), C2 (16 bits), C3 (16 bits) and C4 (16 bits)).

RC4

RC4 generates a pseudorandom stream of bits (a keystream). As with any stream cipher, these can be used for encryption by combining it with the plaintext using bit-wise exclusive-or; decryption is performed the same way.

III. CONCLUSION

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. The salient features of WSNs make it very challenging to design strong security protocols.Algorithms have been developed as a measure to secure the system. All the algorithms are Useful based on the on the requirement as and when needed. Various security mechanisms and security Protocos are available for each of the attacks and algorithms.

REFERENCES:

1. L. Yuan and G. Qu, G, "Design space exploration for energy-efficient secure sensor network", Proc. The IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2002, 1719 July 2002, pp. 88 – 97. 32.
2. G. Jolly, M.C. Kuscu, P. Kokate, and M. Younis, "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340. 33.
3. M. Younis, M. Youssef, and K. Arisha, "Energy-aware routing in cluster-based sensor networks" Proc. 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 1-16 Oct. 2002 pp. 129 – 136. 34.
4. A.D. Wood, J.A. Stankovic, and S.H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks", 24th IEEE Real-Time Systems Symposium, (RTSS), 2003, pp. 286-297. 35. M. Cagalj, S. Capkun, and J.P. Hubaux, "Wormhole-based AntiJamming Techniques in Sensor Networks" from http://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf
5. Second Edition, Vol 2.2003, , Tata MCGrawHil, pg: 01 – 255 "Cryptography and Network Security" – Atul Kahate
6. Cheung O.Y.H., Tsoi K.H., Leong P.H.W., and Leong M.P. "Tradeoffs in Parallel and Serial Implementations of the International Data Encryption Algorithm IDEA"