 ISBN: 978-81-927230-0-9

Therotical Review of Hybride Network Security

Vidyullata S. Jadhav
VPIMSR,
Sangli
vidyullatap@gmail.com

Dr. S. D. Mundhe
Director, SIMCA-MCA
Narhe, Pune

***Abstract*— Network Security deals with the security problems on networks of any size. It concern to external problems as well as problems from users of computers inside the network. Internet Security is the one most people are concerned with as it deals with malware and hackers. Network security is concern with security of personal computer, network. Different techniques are used for network security.**

Keywords—network security, password, firewall MAC,WAP, Smart Card

I. INTRODUCTION

In Computer science, Security means the methods and procedures involved to keep personal computer, computer network and information secure and assuring its integrity. Personal computer security is security of personal Computer and data stored in it for those computers which is not part of any network but using Internet. Network Security deals with the security problems on networks of any size. It concern to external problems as well as problems from users of computers inside the network. Internet Security is the one most people are concerned with as it deals with malware and hackers. [1]

II. PERSONAL COMPUTER SECURITY

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications) NIST 1995

The key objectives (CIA)

Fig 1: CIA of Computer Security

Confidentiality- confidentiality is assurance that confidential information is not disclosed to Unauthorized individuals. Confidentiality is roughly equivalent to privacy.

Integrity-Integrity is divided into two types data Integrity and system integrity. Data Integrity is assurance that information and programs are changed only in a specified and authorized manner. System integrity- is assurance that a system performs its operations in very effective manner

Availability: For authorized persona system should assure that systems work promptly and service is not denied.

Security option used with personal computer for CIA

1. Personal Computer should be encrypted and secured with a password.
2. The hard drives of desktop computers should be encrypted using software available to stop them being accessed if they are stolen.
3. Use either hardware firewalls or software firewalls.

Fig2 Source: Microsoft website

A firewall is software or hardware that stands between your computer and the internet. It will acts as the gatekeeper for all incoming and outgoing traffic. Firewalls can keep hackers out of personal computer. It also keeps away malware and viruses from personal computer. Basically software firewalls are installed on personal computer. It is part of operating system. This is concern with how applications are communicate with each other on personal computer. [2] The firewall monitors all this information traffic to allow 'good data' in, but block 'bad data' from entering your computer.

III. COMPUTER NETWORK SECURITY

Computer network includes server, workstations, cable if used network and network device. Network security is used to protect data during transmission. It includes protecting server, keeping workstations secure and protecting network device.[3]Internet security is used to protect data during transmission over interconnected network. Following different methods are used for network security.

A. Authentication
B. Firewall
C. MAC Address
D. Wired Equivalent Privacy (WEP)
E. Wi-Fi Protected Access (WPA)

A. Authentication

Authentication is nothing but establishing identity. Authentication establishes our identity so that we can obtain the set of rights Identity [4]. For Authentication following methods where used**.**

1) Passwords

A password is sequence of characters without space used to determine the computer user requesting access to a computer system. Every user has unique id and that can be generally known. In order to verify that user id, a second identification is the password. [5] Most networks require that end users change their passwords on a periodic basis. Good password will be mixture of letters and at least one number.

Algorithm for password
Step 1: accept login name (user id)
Step 2: if login name (user id) is correct then goto step 3 else display message "Wrong user id" and goto step 1
Step 3: Accept password
Step 4: if password is correct then provide access else display message "Wrong password " and stop

2) Smart cards:

Smart cards are not a new technology. Roland Moreno invented and developed the first smart card in 1974. Smart cards are credit card–sized plastic cards that contain integrated circuit cards. Smart cards are tamperproof and can be used to store users' certificates and private keys. Smart cards can perform sophisticated public key cryptography operations, such as digital signing and key exchange.[6]

Fig 3:Smart card(sourse : cis533-authentication.pdf)

Algorithm for smart cards

Step 1: Smart cards communicates with the help of Card Accepting Device (CAD)
Step 2:CAD communicate with small data packets called Application Protocol Data Units (APDUs).
Step 3: The Smart Card and the CAD use a mutual active authentication protocol to identify each other.
Step 4: The card generates a random number and sends it to the CAD
Step 5: CAD encrypt the number with a shared encryption key before returning it to the card.
Step 6: The card then compares the returned result with its own encryption. The pair may then perform the operation in reverse.
Step 7: After communication is established, each message between the pair is verified through a message authentication code.

B. Firewall

A firewall is network security system that will takes care of the incoming and outgoing network traffic hardware or software system which prevents unauthorized access to or from a network. There are different kinds of technique which may be implemented by a firewall. Some of them are as follows: Packet filter , Application gateway, Circuit level gateway, Proxy server [7]

Firewall logic: Firewalls use 3 types of filtering mechanisms:

- Packet filtering or packet purity: Data flow consists of packets of information and firewalls analyze these packets to sniff out offensive or unwanted packets depending on what you have defined as unwanted packets.
- Proxy: Firewalls in this case assume the role of a recipient & in turn sends it to the node that has requested the information & vice versa.
- Inspection: In this case Firewalls instead of sifting through all of the information in the packets, mark key features in all outgoing requests & check for the same matching characteristics in the inflow to decide if it relevant information that is coming through.

Firewall Rules

Firewalls rules can be customized as per your needs, requirements & security threat levels. You can create or disable firewall filter rules based on such conditions as:

IP Addresses: Blocking off a certain IP address or a range of IP addresses, which you think are predatory. What is my IP address? Where is an IP address located?

Domain names : You can only allow certain specific domain names to access your systems/servers or allow access to only some specified types of domain names or domain name extension like .edu or .mil.

Protocols: A firewall can decide which of the systems can allow or have access to common protocols like IP, SMTP, FTP, UDP,ICMP,Telnet or SNMP.

Ports : Blocking or disabling ports of servers that are connected to the internet will help maintain the kind of data flow you want to see it used for & also close down possible entry points for hackers or malignant software.[8]

1) Firewall Algorithm

Following are processes firewall

a) verifying the correctness of server interoperability

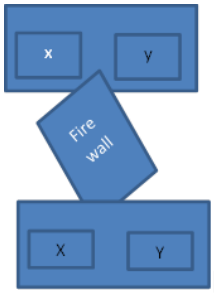
Step 1: x and y are nodes on network which uses I***nternet Protocol version 4(IPv4)***

Step 2: apply for IPv4 address for x and y.

Step 3: nodes x and y establish connections with proxy gateway, virtual external node X,Y;

4) x and y communicate using the IPv4 address;

5) If the communication success, then the configuration is correct on both ends and fails.



[12]

Fig 3: firewall Communication

b) verifying the gateway firewall rules

Step 1: creates x node y in the IPv4 network, configure an IPv4 address;

Step 2: look for an external 64 tunnel-agent, y apply for IPv6 address to external 64 network tunnel proxy;

Step 3: node y connect to 64 tunneling gateway, virtual external networks node y;

Step 4: created node x in the IPv6 network, configure a IPv6 address, and then a establish x connection to y;

Step 5: If x and y can communicate, then firewall blocking rule is not taking effect, or success.

C. MAC Adress:

The Media Access Control (MAC) address is a binary number used to uniquely identify computer network adapters. These numbers (sometimes called "hardware addresses" or "physical addresses") are embedded into the network hardware during the manufacturing process, or stored in firmware, and designed to not be modified. Some also refer to them as "Ethernet addresses" for historical reasons, but multiple types of networks all utilize MAC addressing including Ethernet, Wi-Fi, and Bluetooth. TCP/IP networks use both MAC addresses and IP addresses but for separate purposes. A MAC address remains fixed to the device's hardware while the IP address for that same device can be changed depending on its TCP/IP network configuration.

Format of a MAC Address : Traditional MAC addresses are 12-digit (6 bytes or 48 bits) hexadecimal numbers. By convention, they are usually written in one of the following three formats:

MM:MM:MM:SS:SS:SS
MM-MM-MM-SS-SS-SS
MMM.MMM.SSS.SSS [9]

D. Wired Equivalent Privacy (WEP)

WEP is a security protocol for Wi-Fi networks. Since wireless networks transmit data over radio waves, it is easy to intercept data or "eavesdrop" on wireless data transmissions. The goal of WEP is to make wireless networks as secure as wired networks, such as those connected by Ethernet cables. The wired equivalent privacy protocol adds security to a wireless network by encrypting the data. If the data is intercepted, it will be unrecognizable to system that intercepted the data, since it is encrypted. However, authorized systems on the network will be able to recognize the data because they all use the same encryption algorithm. Systems on a WEP-secured network can typically be authorized by entering a network password.[10]

The security of a wireless LAN is very important, especially for applications hosting valuable information. For example, networks transmitting credit card numbers for verification or storing sensitive information are definitely candidates for emphasizing security. In these cases and others, proactively safeguard your network against security attacks. WEP (wired equivalent privacy) is 802.11's optional encryption standard implemented in the MAC Layer that most radio network interface card (NIC) and access point vendors support. When deploying a wireless LAN, be sure to fully understand the ability of WEP to improve security. It's complicated, but here we go.

WEP in action

If a user activates WEP, the NIC encrypts the payload (frame body and CRC) of each 802.11 frame before transmission using an RC4 stream cipher provided by RSA Security. The receiving station, such as an access point or another radio NIC, performs decryption upon arrival of the frame. As a result, 802.11 WEP only encrypts data between 802.11 stations. Once the frame enters the wired side of the network, such as between access points, WEP no longer applies. As part of the encryption process, WEP prepares a keyschedule ("seed") by concatenating the shared secret key supplied by the user of the sending station with a random-generated 24-bit initialization vector (IV). The IV lengthens the life of the secret key because the station can change the IV for each frame transmission. WEP inputs the resulting "seed" into a pseudo-random number generator that produces a keystream equal to the length of the frame's payload plus a 32-bit integrity check value (ICV).[13]

What's wrong with WEP?

WEP has been part of the 802.11 standard since initial ratification in September 1999. At that time, the 802.11 committee was aware of some WEP limitations; however, WEP was the best choice to ensure efficient implementations worldwide. Nevertheless, WEP has undergone much scrutiny and criticism over the past couple years.

WEP is vulnerable because of relatively short IVs and keys that remain static. The issues with WEP don't really have much to do with the RC4 encryption algorithm. With only 24 bits, WEP eventually uses the same IV for different data packets. For a large busy network, this reoccurrence of IVs can happen within an hour or so. This results in the transmission of frames having key streams that are too similar. If a hacker collects enough frames based on the same IV, the individual can determine the shared values among them, i.e., the keystream or the shared secret key. This of course leads to the hacker decrypting any of the 802.11 frames.

The static nature of the shared secret keys emphasizes this problem. 802.11 doesn't provide any functions that support the exchange of keys among stations. As a result, system administrators and users generally use the same keys for weeks, months, and even years. This gives mischievous culprits plenty of time to monitor and hack into WEP-enabled networks. Some vendors deploy dynamic key distribution solutions based on 802.1X, which definitely improves the security of wireless LANs. The problem, however, is that these types of mechanisms won't be part of the 802.11 standard until the end of 2002 at best.[13]

E. Wi Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) supports a strong encryption algorithm and user authentication. The WPA standard employs Temporal Key Integrity Protocol (TKIP) with Rivest Cipher 4 (RC4) for encryption and Message Integrity Checking (MIC), using 128 bit keys that are dynamically generated for encryption. [11]

Fig 4. Wireless security standards define how data is encrypted across a wireless network link.(Source: http://www.ni.com/white-paper/7376/en/)

One of the simple explanatory devices they used was this equation for WPA:

WPA = 802.1X + EAP + TKIP + MIC

Where

TKIP, MIC and 802.1X parts of the WPA equation each play a part in strengthening the data encryption in WPA-enabled LANs. MIC is Message Integrity Check

[14]

Algorithm for WAP

Step 1: Enter machine password into Access point and Client

Step 2: Access point checks the client's password, If password matches, client connected to network else client not connected to network.

Step 3: Keys are generated and installed. Now client and Access point can exchange data. [14]

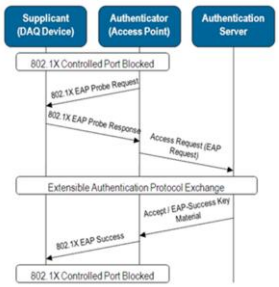


Fig 5: The IEEE 802.1X authentication process involves a layered exchange between the supplicant, authenticator, and authentication server.(Source : http://www.ni.com/white-paper/7376/en/)

REFERENCES

1. Kumar, A. (2011, 11 05). 61722.aspx. Retrieved 11 25, 2016, from http://www.brighthub.com/: http://www.brighthub.com/computing/smb-security/articles/61722.aspx
2. secure-your-computers. (2016). Retrieved November 30, 2016, from www.staysmartonline.gov.au: https://www.staysmartonline.gov.au/computers/secure-your-compute
3. WIRELESS NETWORKING SECURITY(2006)
4. Butler, P. (2011). Computer and Network Security. Oregon: Computer and Information Science.
5. Rouse, M. (2007, june 01). Defination Password. Techtarget, p. http://searchsecurity.techtarget.com/definition/passwo
6. cc962052.aspx. (n.d.). Retrieved dec 05, 2016, from https://technet.microsoft.com: https://technet.microsoft.com/en-us/library/cc962052.aspx
7. Dr. Ajit singh, M. P. (2013). A Review Paper On Firewall. INTERNAT IONA L JOURNA L FOR RE SEARCH IN A P PL I ED S C I ENC E AND ENGINEERING T E CHNOLO GY (IJRA S ET), 4-8.
8. Computer Firewalls. (n.d.). Retrieved 12 12, 2016, from http://www.firewallinformation.com/: http://www.firewallinformation.com/
9. Mitchell, B. (2016, 10 05). introduction-to-mac-addresses-817937. Retrieved 12 12, 2016, from www.lifewire.com: https://www.google.co.in/#q=mac+address+fundamentals
10. wep. (n.d.). Retrieved 12 12, 16, from http://techterms.com/definition: http://techterms.com/definition/wep
11. https://www.staysmartonline.gov.au/computers/secure-your-computers Butler, P. (2011). Computer and Network Security. Oregon: Computer and Information Science.
12. Li Zhou, L. G. (2013). The Firewall Rule Authentication Method Based on 6to4 Tunnel. International Journal of Security and Its Applications, 133-141.
13. Geier, J. (2002, june 01). 80211-WEP-Concepts-and-Vulnerability.htm. Retrieved 12 21, 2016, from http://www.wi-fiplanet.com/: http://www.wi- fiplanet.com/tutorials/article.php/1368661/80211-WEP-Concepts-and-Vulnerability.htm
14. TEAM, T. P. (2003, June 25). wi,review-149.html. Retrieved Dec 21, 2016, from http://www.tomsguide.com/: http://www.tomsguide.com/us/wi,review-149.html