Wireless LAN Security and Management

Luaay Abdul Wahed Shihab

Abstract:-The purpose of the project is to protect the LAN from hackers and make the network security and network is protected using the type of stream encryption is the encryption and one of the systems, encryption of electronic strong because of high security and the difficulty of breaking and stream encryption prevents explicit text to cipher text bit – bit stream encryption key is a sequential or Theorem To generate the key sequence is used to remove recorded value of the given elementary Function and feedback System and network management and security management.

Keywords:- W LAN Security, WI FI protect , SSAD, AP , EBSS

I. INTRODUCTION

In the last decade there has been widespread fast and sophisticated technical networks the wireless different was the use of various techniques and are local networks of the various threats to the growing increasingly been used encryption and that the protection is being from entering the local network and the protection of user and tampering with the computer and find out local area networks has become a major tool to many companies and factories, universities, hospitals and standardization of data and security services that protect the data and means of communication and processing must be distributed across networks of local connections, for send any Public confidential and sensitive to face an official must be protected by the local network one way encryption possible transitions simple networks non-local communication of email and the insured are incomplete files can be stolen or read, or perhaps modify some communication networks within the local encryption codes and digital signatures verify message may help to these problems and can help provide some insurance policies necessary to provide security . One doesn't need to have physical access to your wires to get into your LANs now. Any attacker, even though sitting in your parking lot, or in your neighboring building, can make a mockery of the security mechanisms of your WLAN. In order to design and build a well-secured network, many factors must be taken into consideration, such as the topology and placement of hosts within the network, the selection of hardware and software technologies, and the careful configuration of each component. My paper will be an examination of some of the issues in designing a secure Local Area Network (LAN) and some of the best practices suggested by security experts. I will discuss securing a LAN from the viewpoint of the network architect considering three main areas: the network topology which comprises the physical and logical design of the network; securing the routers and switches which connect segments and hosts to form the network; and, finally, some of the emerging and advanced techniques in network security will be examined .

Manuscript Received on September 2012.

Luaay Abdul Wahed Shihab, University Basrah- Iraq

II. THEORETICAL CONSIDERATION

Point-to-point key distribution this is the basic mechanism of every key distribution Scheme .lf based on symmetric cryptographic technique was, point –to-point key distribution that the two parties involved already share a key that can be used to protect the keying material to be distributed. Based on asymmetric techniques, point –point key distribution requires that each of the two paretic has a public key with its associated secret key and the certificate of the public key produced by a certification.

III. DESIGNING THE PHYSICAL NETWORK

It may seem odd to talk about the physical network when building wireless networks. After all where is the physical part of the network in wireless networks? The physical medium we use for communication is obviously electromagnetic energy but in the context.

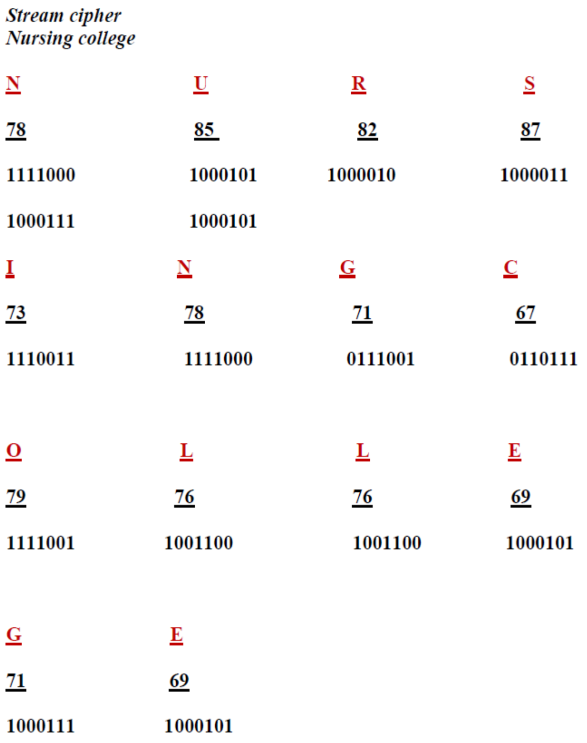
Point-to-point like typically provide an internet connection where such access isn't otherwise available. One side of a point to point link will Have an internet connection while the other Uses the link to reach the internet for example A university may have a fast frame relay or v sat Connection in the middle of campus but can notion Building has an unobstructed view of the remote Sit a point Conn even replace existing dial up likes With proper antennas and clear line of sight Reliable point to point likes in excess in excess of Thirty kilo meters are possible Encryption is one of the sleek and encryption systems, electronic high security because of the strong and difficult to break and therefore the confidentiality of this system depends on the secret key Encryption converts the text flowing to the explicit text of the encrypted beta - beta at the same time. The encryption key is a sequential (serial) binary consisting of a set of zeros and units (1, 0) is called sequential key. Encryption system flowchart includes two parts:

1. Algorithm to generate the key sequence .
2. Gate

* More algorithms that are used to generate the key sequence built using Registered displacement as the main component of the birth of the key sequence is recorded displacement. Secret encryption system depends on the generation of sleek sequential key, where it should be possible.

Stream Ciphers and Block Ciphers

size and performs the XOR function on each block. Each block must be the predetermined size, and leftover frame fragments are padded to the appropriate block size For example, if a block cipher fragments frames into 16 byte blocks, and a 38-byte frame is to be encrypted, the block cipher fragments the frame into two 16-byte blocks and with the plain-text data. The key stream can be any size necessary to match the size of the plain-text frame to encrypt Block ciphers deal with data in defined blocks, rather than frames of varying sizes. The block cipher fragments the frame into blocks of predetermined block is padded with 10 bytes of padding to meet the 16-byte block size.



Stream cipher
Nursing college

N	U	R	S
78	85	82	87
1111000	1000101	1000010	1000011
1000111	1000101		
I	N	G	C
73	78	71	67
1110011	1111000	0111001	0110111
O	L	L	E
79	76	76	69
1111001	1001100	1001100	1000101
G	E		
71	69		
1000111	1000101		

*To generate the key sequence is used to remove are corded value (01010) of the given elementary function and feedback as shown in the table.

T	State	t	State
0	01010	16	11100
1	10101	17	11001
2	01011	18	10011
3	10111	19	00110
4	01110	20	01101
5	11101	21	11010
6	11011	22	10100
7	10110	23	01001
8	01100	24	10010
9	11000	25	00100
10	10001	26	01000
11	00011	27	10000
12	00111	28	00001
13	01111	29	00010
14	11111	30	00101
15	11110	31	01010

A table showing the recorded cases of linear displacement length of (5) and the feedback function

Note**-:**
So = S1
S1 = S2
S2 = S3
S3 = S4
S4 = So S2

Series generated follows :-
near

0101 0111 011 000 11 1 110011 01 001 000 01 0101 011101 1000 11111 0011 0100 1000 01
Combines the key with sequential explicit text using a standard combination (2) to get the cipher text .

N = 1111000 U = 1000101

IV. What is Network Management?

Perhaps the need for network management arises from the difficulty imprecision or complexity that is beyond the capability of automated systems that is we can frame a definition of network management that places emphasis on the need for human intervention by saying that network management is an activity that occurs in situations where automation cannot suffice because human judgment is required we can take a more optimistic approach and argue that the need for network management arises merely from the unknown while this book was being written for example an engineer opined to the author that network management is best described as all the aspects of devising and operating a network that no one knows how to automate the engineer observed that once someone discovers a way to automate a management task vendors incorporate the technology into their products which means that the task ceases to fall into the purview of a network manager.

V. Element and Network Management System

The network management system offered by most equipment venders focus on managing a single network element as a time that is a vender creates each network element independently provides the element with a management interface and allows customers to coordinate multiple element to precisely characterize such system we use the term element management system (EMS) and reserve the more general term network management system(NMS) to refer to a system that is capable of managing and coordinating multiple network elements make them work together consistently .

Why have vendors concentrated on element management system? There are three reasons. first as will see designing a network management system is a non trivial intellectual challenge vendors have tried to design such systems but have not been extremely successful second by restricting attention to a single network element a vendor can eliminate most of the complexity and concentrate on straightforward tasks such as monitoring third because network often contain elements from multiple vendors a network management system must accommodate other vendors products and a given vendor is unlikely to create a system that make it easy to use competitors products the situation can be summarized.

VI. Management issue and security?

The next sections consider several important management issue related to security the descriptions are not meant to serve as a comprehensive list of all security management task or problems instead the discussion pontes out a set of management problems that are particularly significant the sections consider a fundamental question about security as well as more mundane issue and day-to-day task in particular our discussion begin by asking about the overall approach an organization can take regarding security the answer determines how an organization organizations its network security system and selects which security technologies to use .

VII. Management of wireless network

Wireless network pose special problems for the management of security in particular Wi-Fi network that allow multiple computer to share bandwidth create potential security risks a frame transmitted over a Wi-Fi network is subject to eavesdrop ping a third party can obtain a copy of all frames traveling over the Wi-Fi network an encryption technology named wired equivalent privacy (WEP) was developed to encrypt Wi-Fi frames but WEP can be broken given enough time thus even if WEP is used a third party can capture a copy of a conversation break the encryption and read message as a result many managers seek other encryption technologies that can be used with Wi-Fi other security problem in Wi-Fi arise from the use of a32-character string called a serves set identifier (SSID)an SSID is used to identify each wireless LAN-before a computer can became associated with a Wi-Fi access point both the wireless interface in the computer and access point must be configured to have the same SSAD unfortunately SSID alone do not provide security because a third party can monitor the network capture copies of frames and extract the SSID furthermore the default configuration in many access point is open the access point broadcasts its SSID finally managers must contend with a subtle detail in some software when it boots a computer that has been connected to an access point will using the same SSID again which can computer a company s SSID If laptop that was used inside the company is booted outside company the point is . Wireless Local Area Networks are becoming as ubiquitous as wired LANs .Wireless technology is allowing the network to go where wire cannot go. The purpose of this paper is to assist IT Managers in the decision process when implementing a Wireless Network. My intention is to give IT managers a primer on 802.11-based LANs and the potential security risks that an enterprise can open itself to if they do not take appropriate precautions before implementing this technology. This includes conducting an adequate risk analysis before implementing wireless network technologies.

VIII. Types of Wireless LANs

The part of success behind the popularity of WLANs is due to the availability of the 802.11standard from IEEE. The standard specifies operation of WLANs in three ways :

A. ***Infrastructure Mode:*** Every WLAN workstation (WS) communicates to any machine through an access point (AP). The machine can be in the same WLAN or connected to the outside world through the AP.

B. ***Ad Hoc Network Mode*:** Every WS talks to another WS directly Mixed Network Mode: Every WS can work in the above two modes simultaneous .This is also called the Extended Basic Service Set (EBSS).

IX. The LAN Security Problem

The advantages of utilizing a LAN were briefly discussed in the previous section. With these advantages however, come additional risks that contribute to the LAN security problem . LANs share many security problems approaches for their solutions with point-to-point conventional communications systems. In addition , they have some unique problems of their own. This section surveys these problems and leads into the section that discusses selected approaches for solution.

X. Distributed File Storing – Concerns

File servers can control users' accesses to various parts of the file system. This is usually done by allowing a user to attach a certain file system (or directory) to the user's workstation, to be used as a local disk. This presents two potential problems. First, the server may only provide access protection to the directory level, so that a user granted access to a directory has access to all files contained in that directory. To minimize risk in this situation, proper structuring and management of the LAN file system is important. The second problem is caused by inadequate protection mechanisms on the local workstation. For example, a personal computer (PC) may provide minimal or no protection of the information stored on it. A user that copies a file from the server to the local drive on the PC loses the protection afforded the file when it was stored on the server. For some types of information this may be acceptable. However, other types of information may require more stringent protections. This requirement focuses on the need for controls in the PC environment.

XI. Other LAN Security Concerns

Other LAN security problems include (1) inadequate LAN management and security policies, (2)lack of training for proper LAN usage and security, (3) inadequate protection mechanisms in the workstation environment, and (4) inadequate protection during transmission. A weak security policy also contributes to the risk associated with a LAN. A formal security policy governing the use of LANs should be in place to demonstrate management's position on the importance of protecting valued assets. A security policy is a concise statement of top management's position on information values, protection responsibilities, and organizational commitment. A strong LAN security policy should be in place to provide direction and support from the highest levels of management. The policy should identify the role that each employee has in assuring that the LAN and the information it carries are adequately protected .The LAN security policy should stress the importance of, and provide support for, LAN management. LAN management should be given the necessary funding, time, and resources. Poor LAN management may result in security lapses. The resulting problems could include.

XII. GOALS OF LAN SECURITY

The following goals should be considered to implement effective LAN security:

- Maintain the confidentiality of data as it is stored, processed or transmitted on a LAN.
- Maintain the integrity of data as it is stored, processed or transmitted on a LAN.
- Maintain the availability of data stored on a LAN, as well as the ability to process and transmit the data in timely fashion.
- Ensure the identity of the sender and receiver of a message.

Adequate LAN security requires the proper combination of security policies and procedures, technical controls, user training and awareness, and contingency planning. While all of these areas are critical to provide adequate protection, the focus of this document is on the technical controls that can be utilized. The other areas of control mentioned above are discussed in the appendices.

XIII. CONCLUSION

Protect the local network using encryption flow and prevent hackers from penetrating the network And how to use the network your local network in order to design and build a good network and network insurance.

REFERENCE

[1]. Wireless networking in the developing / first edition / 2006

[2]. Cipher system te protection of communication by BEKER . H and PIPER. F

[3]. Communication network / SHARAM HEKMET

[4]. Concept of networking / IHT/ first edition / 2000-2001

[5]. Automated network management system by DOUGLAS E. COMER

[6]. Wireless LAN security – challenges and solution / PROF. RATHNAKAN . DR. NATHAN.

[7]. Internet working with TCP/ IP / FIFTH EDIYION / by DOUGLAS E . COMER.