SECURITY PROBLEMS IN 802.11 WIRELESS NETWORKS STANDARD DUE TO THE INEFFECIENCY OF WIRED EQUIVALENT PRIVACY PROTOCOL

Varma Samanthapudi, B.E.

Problem in Lieu of Thesis Prepared for the Degree of

MASTER OF SCIENCE

UNIVERSITY OF NORTH TEXAS

May 2003

APPROVED:

Roy Tom Jacob, Major Professor
Steve Tate, Committee Member
Robert Brazile, Committee Member
Krishna Kavi, Chair of the Department of Computer Science
C. Neal Tate, Dean of the Robert B. Toulouse School of Graduate Studies

Samanthapudi, Varma, Security problems in 802.11 wireless networks standard due to the inefficiency of wired equivalent privacy protocol. Master of Science (Computer Science), May 2003, 41 pp., 1 table, 5 figures, references, 25 titles.

Due to the rapid growth of wireless networking, the fallible security issues of the 802.11 standard have come under close scrutiny. Nowadays most of the organizations are eager to set up wireless local area networks to reduce the hassles of limited mobility provided by conventional wired network. There are serious security issues that need to be sorted out before everyone is willing to transmit valuable corporate information on a wireless network. This report documents the inherent flaws in wired equivalent privacy protocol used by the 802.11 standard and the ensuing security breaches that can occur to a wireless network due to these flaws. The solutions suggested in this report might not actually make the 802.11 standard secure, but will surely help in the lead up to a secure wireless network standard.

TABLE OF CONTENTS

Page

LIST OF FIGURES AND TABLES ……..iii

Chapter

1. INTRODUCTION……..…….1

   Organization of the Problem in Lieu of Thesis

2. WIRELESS NETWORKING AND 802.11 STANDARD……..…….3

   How Does Wireless Networking Work?
   Types of Communication Methods in Wireless Networks
   802.11 Standard

3. WIRED EQUIVALENCY PROTOCOL (WEP)……21

   Introduction to WEP Protocol
   WEP Protocol Implementation
   Major WEP Security Flaws
   Attacks on 802.11 Wireless Networks Due to Inefficient WEP Protocol

4. PROPOSED SOLUTIONS AND CONCLUSIONS……..…….. 35

   Counter Measure for Improving WEP's Security
   Conclusions

5. REFERENCES……..…….39

.

LIST OF FIGURES AND TABLES

Page

Figure

1. Classifications of Wireless LANS……..……4
2. An Ad Hoc Wireless Network……..……13
3. An Infrastructure Wireless Network……..……14
4. Transmission in WEP Protocol…..……24
5. WEP Frame Transmission Format……..…….25

Table

1. Extensions in 802.11 Standard and Their Specifications……9

1. INTRODUCTION

"Networking" refers to the way computers and other devices are connected together to share information and hardware resources. There has been tremendous growth in wireless networks over the last decade. There are whole lot reasons as to why wireless networking is being adopted in place of traditional wired networking. Dealing with cabling problems has been one of the primary jobs of a network administrator. Troubleshooting cables for breaks bad connections and overseeing the relocation of computers is not only time consuming, but frustrating as well.

As a result, some of the network managers turn to wireless networking, rather than cable. The major motivation factor for moving to wireless networks has been mobility. The increase in the number of laptop personal computers and the personal digital assistants has brought about a wide range of places where people need to be connected and this has been a limitation for wired networks. Network users can access the local area network (LAN) literally from anywhere, as they are not limited by the wired connections.

Flexibility is another aspect that has been driving people towards wireless technology. Using the ad hoc network it is very easy to set up a network among a set of clients so that they can communicate with relative ease, say at a meeting where you expect people to share data through their laptops, which are easier to carry around. It is very easy to set up a wireless network in places, which are not easily accessible or not viable enough to set up a wired network.

Cost of installation is the other reason, which supports establishment of a wireless network. Installing network cable can be expensive proposition, costing

hundreds or even thousands of dollars per network connection. It is relatively cheap to set up a wireless network rather than drilling holes through the wall. [9]

Though it may sound wireless networking is the next thing in the field of networking but there are tradeoffs that make one think if it is worth changing to a wireless environment. By the nature of medium, wireless networks transmit at slower data rates than wire-based networks. Wireless network also has a limitation on the number of connected nodes and how far apart those nodes can be placed from each other.

The major drawback in wireless networks has been the security being offered for the data being transmitted. Various organizations are implementing wireless networks based on the institute of electrical and electronics engineers (IEEE) (IEEE is a non-profit association of technical professionals - www.IEEE.org) 802.11 standard, which provide confidentiality through wired equivalent privacy (WEP) protocol that have significant flaws. These flaws give rise to a number of attacks, both passive and active, that allow eavesdropping on, and tampering with the connected resources. [2]

1.1 Organization of the Problem in Lieu of Thesis

Having presented a brief introduction to wireless LANs and terminology associated with them in this chapter, the next chapter explains wireless networking and 802.11 standard in detail. The WEP protocol set up is described in chapter 3. This chapter also gives an insight into the various flaws in WEP security and also the documents the various attacks on 802.11 wireless networks. The fourth chapter includes the recommendations suggested for the improvement of security in wireless networks and conclusions.

2. WIRELESS NETWORKING AND 802.11 STANDARD

2.1 How Does Wireless Networking Work?

Wireless networking refers to the transmission of signals, which are transmitted and received via antennae through a wireless medium such as air or space instead if through a physical cable. Strictly speaking, any technology that does this could be called wireless networking. But nowadays the term wireless networking generally refers to Wireless Local Area Networks (WLANs). Using electromagnetic waves, WLANs transmit and receive data over air minimizing the need for wired connections. [6][7]

Since there is no physical connection involved so the data communication is done via electromagnetic airwaves (radio and infrared). Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that I can be accurately extracted at the receiving end. This is generically referred to as modulation of the carrier by the information being transmitted. Once data is modulated onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier.

As the communications are being done through radio waves there is a very good chance that multiple radio carriers can exist in the same space at the same time. It is possible to avoid the radio carriers from interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in (or selects) one radio frequency while rejecting all other radio signals on different frequencies. [2][3][6]

An access point that acts as a transmitter/receiver (transceiver) device connects to the wired network from a fixed location using standard Ethernet cable. At minimum, the access point receives, buffers, and transmits data between the WLAN and the wired network infrastructure. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet. [5]

2.2 Types of Communication Methods in Wireless Networks

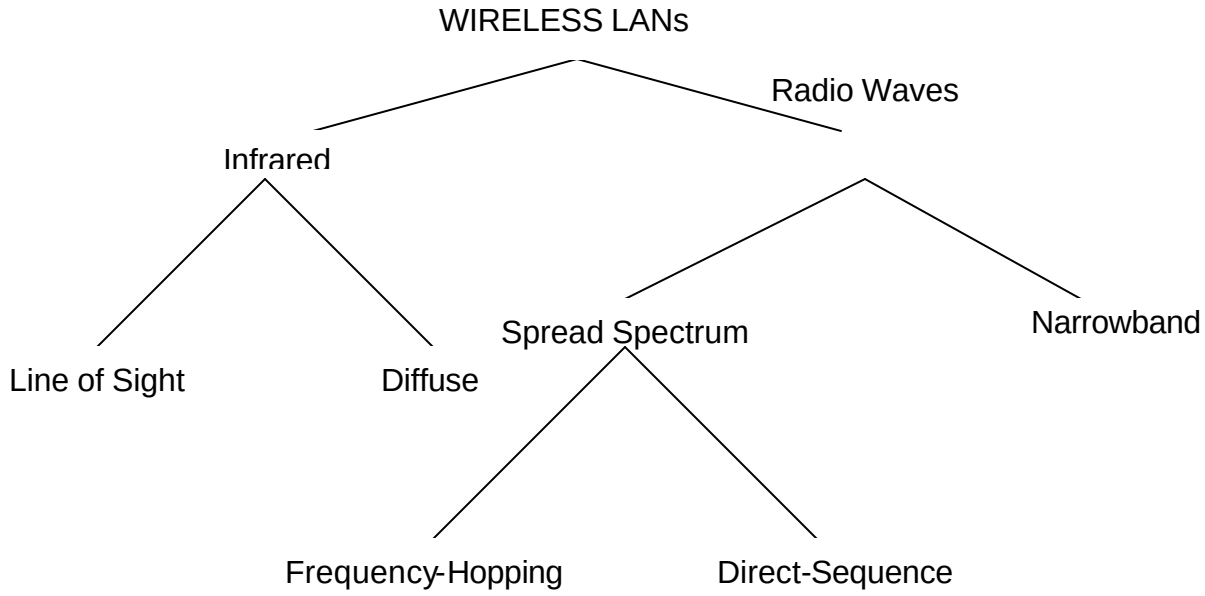

Figure 1: Classifications of Wireless LANs [5][13]

From figure 1 it's quite evident that modes of communication within wireless networks can be classified under either radio wave or infrared technology. There are various technologies to choose from to carry data when designing a wireless network. The following section describes the basics of how each of these technologies operates and what are their operational characteristics. [5][9]

2.2.1 Infrared Technology

In this technology data is transferred through infrared (IR) light band of the electromagnetic spectrum. It operates between 1000GHz and higher range, radio wave and visible light. Infrared waves cane be reflected off, but cannot penetrate opaque objects such as walls. The primary advantage of infrared technology is its great bandwidth, allowing it to carry hundred of megabits of data per second.

The technology used with infrared networks is almost similar to the one used for remote-control units that come with home electronics equipment, such as TV's and stereos. Receivers for wireless networks, like the channel changer and TV, must be visible to the transmitter, either directly or via reflection. Infrared networks can be implemented with mirrors that focus the light signal to an extremely tight beam. High-speed communication can be achieved as focusing delivers essentially the entire transmitted signal to the receiver.

Mirror-based systems are well suited for point-to-point applications where transceivers are seldom moved. High performance directed infrared is impractical for mobile users and is therefore used only to implement fixed sub networks. Infrared transmission is used for short and medium range communications and control. Generally, infrared transmission is restricted to LANs within or between buildings because of limited distances and incapability to penetrate walls. [3][5]

There are two ways to transmit infrared waves in a wireless network setting.

Directed infrared. In this mode of transmission the receiver must have a direct, unobstructed view of the sending unit, and any movement in either unit can break the connection. There shouldn't be any obscurity between transmitter and the receiver.

Diffused or reflected infrared. To work around the line-of-sight requirement of directed transmission, the transmitter will spread a strong infrared signal over a wide angle. A single transmitter can reach multiple receivers, while reducing the effects of the transmitter or receiver being moved. A more diffused signal, however, reduces date rates and shortens the distance over which the signal can be reliably sent.

Infrared technology is little used in commercial wireless LAN's as it has its own set of limitations. High performance directed infrared is impractical for mobile users and is therefore used only to implement fixed sub-networks. Diffused infrared wireless LAN systems do not require line-of-sight, but cells are limited to individual rooms. Another disadvantage of infrared networks is their susceptibility to interference from other light sources, including sun and some lighting fixtures. [5]

2.2.2 Radio Transmission Technology

Radio transmissions use radio frequencies (RF) to transmit information. There are many different radio frequency ranges in the electromagnetic spectrum that are assigned to different services. From 800 MHz to 2.5 GHz range of the electromagnetic spectrum, is used for various services such as digital cordless phones, pagers, personal digital assistants (PDAs), laptops and personal computer memory card international association (PCMCIA) cards, and so on. There are three predominantly used technologies to transmit data using radio frequencies. [5][7]

Narrowband technology. In this technology the date is transmitted directly on a center frequency, much like a radio broadcast, so the transmitter and receiver must be tuned to the same bandwidth. Narrowband radio keeps the radio signal frequency as

narrow as possible just to pass the information. Interception can be avoided by carefully coordinating different users on different channel frequencies.

Like the signals from radio and TV stations, narrowband signals are subject to interference from signal reflections. This interference is caused when signals reflected off walls and other objects arrive at different intervals. Such interferences make communication unreliable. Unlike the human eye, communications equipment is not sophisticated or intelligent enough to discern the difference between reflections and the real transmission. In order for the narrowband technology to work properly a clear channel for communications has to be ensured. This can be achieved by carefully allocating each available frequency band to make sure that no nearby networks share the same frequency. [7][12]

Spread spectrum technology. Spread spectrum simply means that data is sent over a number of discrete frequencies available for use at any time in the specified range. There are two different implementations for spread spectrum technology. Spread spectrum technology is most widely used data communication system in wireless LANs. This technique has been designed to increase the efficiency in bandwidth even though there are some tradeoff's associated with it. The frequency range for transmission using spread spectrum technology is 902Mhz to 928Mhz, which has been set-aside for wireless data communications. Even though the bandwidth consumed with spread spectrum technology is more than in case of narrowband transmission, it produces a signal that is, in effect, louder and thus easier to detect. Using spread spectrum technology it is highly unlikely that one spread spectrum network user will interfere with another. The original Institute of Electrical and Electronics Engineers wireless-ethernet

specification, known as IEEE 802.11, designated two kinds of spread spectrum frequencies for communicating between devices: frequency hopping and direct-sequence. [7][9][12]

Frequency-hopping spread spectrum technology. In this method of communication short burst of data is sent and then frequencies are shifted and then another short burst is transmitted. It uses a narrowband carrier than changes frequency in a pattern known to both transmitter and receiver. The frequencies are synchronized in a fashion such that a single logical channel is maintained. The devices that are communicating using frequency-hopping technique agree on which frequencies to hop to, and use each frequency for a brief period of time before interfering with each other. In frequency-hopping the date is generally sent on just two to four frequencies simultaneously, they use 1 MHz or less of the available bandwidth. Because they use any given frequency for such short time they are less prone to interference. Frequency-Hopping based devices are easier and cheaper than devices using infrared. [6][7]

Direct-sequence spread spectrum technology. Using this technology, Communication is done by splitting each byte of data into several parts and sending them concurrently on different frequencies. Direct-sequence spread spectrum generates a redundant bit pattern for each bit to be transmitted. Direct-sequence unlike frequency-hopping uses a lot of available bandwidth, about 22 MHz. The transmissions in sequence-sharing are suitable for bandwidth sharing because they offer an improved signal-to-noise ratio compared with narrowband transmissions. Even if some of the bits are lost during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. Direct-sequence spread spectrum

is capable of much greater speed than frequency-hopping but is more prone to interference. [5][6][7]

2.3 802.11 standard

2.3.1 what is 802.11 Standard?

In order for wireless networks to function they require the use of underlying technology that deals with radio frequencies as well as data transmission. Though there are different technologies available, but 802.11 standard produced by the Institute of Electrical and Electronics Engineers is the most widely used underlying technology for corporate internal wireless LANs. Most of the airports and hotels are using the 802.11 standard so people can wirelessly browse the Internet with their laptops. [7]

Table 1: Extensions in 802.11 standard and their specifications. [4][6][12][25]

Standard	Operational Characteristics and specifications
802.11a	This standard was published in 1999, and it uses orthogonal frequency division multiplexing (ODDM) to provide data rates up to 54 Mbps in 5GHz bands
802.11b	This has become the standard for wireless LANs and is also referred to as Wireless Fidelity (Wi-Fi) standard. This standard uses the direct-sequence spread spectrum and provides data rates up to 11 Mbps at 2.4GHz.
802.11d	This standard works at a frequency of 2.4GHz, which is the same bandwidth as that of Wi-Fi standard. The domains of the wireless network are updated regularly in this standard.
802.11e	802.11e was designed especially for someone looking for quality of

	service (QoS). The 802.11e standard has created a QoS baseline document that proposes the methods for handling time-sensitive traffic. It is highly suitable for transmitting multimedia applications.
802.11f	This standard uses a new protocol know as inter access point protocol (IAPP). The main aim of this standard is to make sure that mobile devices can still remain connected to the network even when they are moved between different access points.
802.11g	The 802.11g standard defines a technology for operations at 2.GHz (like the 802.11b) that offers high data rates, which can reach up to 22Mbps using orthogonal frequency division multiplexing (OFDM). 802.11g was designed to create a standard that had less path loss than 802.11a and was compatible with 802.11b.
802.11h	This standard was designed to enhance the physical layer and medium access control layer specifications of 802.11a. The other motivation for coming up with this standard was to enable the regularity acceptance of 802.11a products in Europe.
802.11i	The major aspect of this standard is to come up with a wireless networking standard that is secure. All the security flaws in 802.11a, 802.11b and other standards have been addressed. The authentication process in this standard is going to be done at the server side. The security encapsulation in 802.11i is based on advanced encryption standard (AES).

The IEEE 802.11 standard was published first in 1999 and it was designed to provide data rates up to 2 Mbps at 2.4GHz. It was designed to use either frequency-hopping speed spectrum or direct sequence speed spectrum. At present task groups numbered a through i are working on various methods to standardize improvements to the 802.11 standard and their specifications are mentioned in table 1. The two major standards being widely used to deploy wireless networks are: 802.11b and 802.11 a. [9]

802.11b. 802.11b is also known as wireless fidelity (Wi-Fi), or wireless ethernet. It has become the standard for WLAN's. 802.11b standard uses direct sequence spread spectrum. The current speed of wireless networks stands on 11 Mbps, but it can reach much higher data rates in the nearest future. Wi-Fi networking products transmit data at the 2.4 GHz frequency, much like newer cordless phone. When there is a strong signal, data moves between computers at 11 Mbps that is almost 20-40 times faster than most high-speed Internet connections. When the signal gets weaker (as the computers are moved farther apart or have more wall in between), the transmission sped gradually decreases to 1 Mbps, which is still quite fast. Using 802.11b standard the data can be transmitted up to distances of 1000 ft, so it is quite suitable to an office setting. The number of access points needed is determined by distance and the number of computers to be connected to the network. For large, such as a warehouse or a department store, 802.11 will provide the least costly solution because of fewer access points. 802.11b products are prone to radio frequency interferences as nowadays most of the cordless phones use 2.4GHz. [1][7][12]

802.11a. 802.11a is the newer and faster version of 802.11b, developed by IEEE, but is still yet to being accepted as a replacement for 802.11b. Using 802.11a

products transmit data at speed s up to 72 Mbps at the frequency of 5GHz. It uses orthogonal frequency division multiplexing (OFDM). 802.11a products are more expensive than 802.11b products, but they offer faster transmission rate and are less prone to interference from microwave ovens and cordless phones. The problem with this standard is that at 5GHz, data doesn't get transmitted to longer distances as path loss incurs due to increased absorption of the radio frequency energy by walls and other solid objects. Of course the superior performance of 802.11a offers excellent support for bandwidth hungry applications, but the higher operating frequency equates to relatively shorter range. Having more access points to handle the higher bandwidth can solve this problem. 802.11 can support higher end applications involving video, voice, and the transmission of large images and files. [1][7][9]

2.3.2 802.11 Wireless Network Topologies

There are two modes of wireless LAN configurations defined in 802.11 standard: Ad hoc mode and Infrastructure mode.

Ad hoc mode. This kind of configuration is also referred to as peer-to-peer mode or an independent basic service set (IBSS). In ad hoc configuration wireless stations communicate directly with one another without using an access point or any connection to a wired network. In ad-hoc networks the infrastructure is build up of mobiles, which establish wireless links between them and build a network topology allowing multi-hop connectivity. Its key characteristics are that there is no fixed infrastructure, and that there is wireless multi-hop communication, dynamically set up and re-configurable as mobiles move around.

As shown in figure 2 any time two or more wireless adapters are within range of each other, they can set up an independent network. Ad hoc networks are characterized by dynamic, unpredictable, random, multi-hop topologies with typically no infrastructure support. The mobiles must periodically exchange topology information, which is used for routing updates. Ad hoc networks are helpful in situations, in which temporary network connectivity is needed. [2]

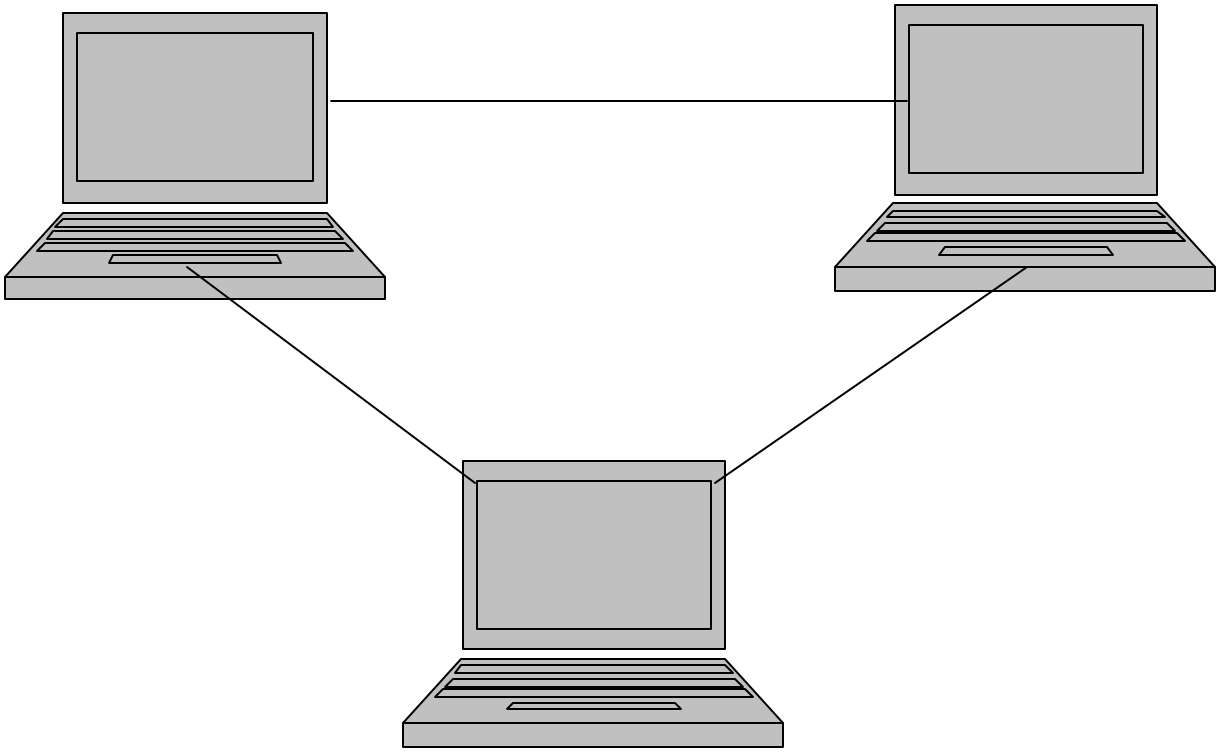

Figure 2: A peer-to-peer or independent or ad hoc wireless network. [2]

Infrastructure wireless LANs: In infrastructure WLANs, multiple access points link the WLAN to the wired network and allow users to efficiently share network resources. Infrastructure network is also referred to as centralized WLAN as the wireless devices try to access the resources of central server rather than the client. In this mode of

wireless network at least one access point is connected to the wired network infrastructure and a set of wireless end stations. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building.

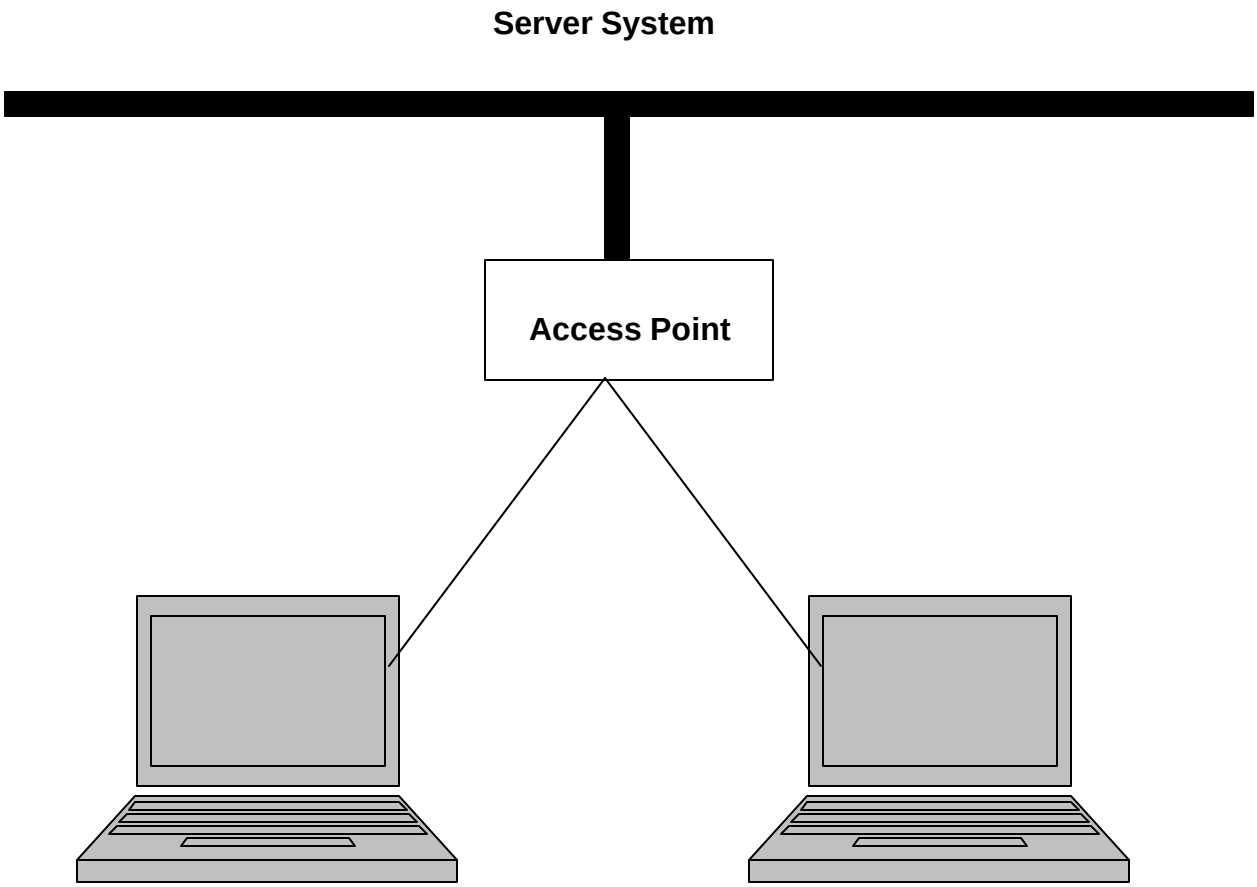

Figure 3: An infrastructure wireless network. [5][6]

The key characteristic of centralized WLANs is that there is some fixed wired infrastructure, which is always accessible through a single hop wireless link. The base stations are connected to the fixed network and support the communication of the

mobiles in range of the base station's radio. Wireless networks often extend, rather than replace, wired networks, and are referred to as infrastructure networks. [5][6]

2.3.3 IEEE 802.11 Layers

Though there are many layers involved for the actual transmission of data over a wireless network the IEEE 802.11 standard places specifications on the parameters of the physical (PHY) and medium access control (MAC) layers of the network. This section details the significance and the standards of the two essential (PHY and MAC) layers of wireless networking.

Physical layer. The physical layer, which actually handles the transmission of data between nodes, can either use direct-sequence spread spectrum, frequency-hopping spread spectrum, or infrared pulse position modulation. IEEE 802.11 makes provisions for date rates of either 1 Mbps or 2 Mbps, and calls for operation in 2.4 – 2.4835 GHz frequency band in case of spread spectrum transmission a 300 – 428,000 GHz for infrared (IR) transmission. Infrared is generally considered to be more secure to eavesdropping, because infrared transmissions require absolute line-of-sight links, as opposed to radio frequency transmissions, which can penetrate walls and be intercepted by third parties unknowingly. However, infrared transmissions can be adversely affected by sunlight, and the spread spectrum protocol of 802.11 provides some rudimentary security for typical data transfers. [5][7]

Medium access Control (MAC) layer: The 802.11 MAC layer provides functionality to allow reliable data delivery for wireless physical layer media. The data delivery itself is based on an asynchronous delivery of MAC layer data. It contains a set

of protocols, which is responsible for maintaining order in the use of a shared medium. The 802.11 MAC layer provides a controlled access method known as carrier sense multiple access with collisions avoidance (CSMA/CA).

In this protocol, when a node receives a packet to be transmitted, it first listens to ensure no other node is transmitting. If the channel is clear, it then transmits the packet. Otherwise, it chooses a random backoff factor, which determines the amount of time the node must wait until it is allowed to transmit its packet. During periods in which the channel is clear, the transmitting node decrements its backoff counter. When the backoff counter reaches zero, the node transmits the packet. Since the probability that two nodes will choose the same backoff factor is small, collisions between packets are minimized.

Collisions detection, as is employed in ethernet, cannot be used for the radio frequency transmissions of IEEE 802.11. The reason for this is that when a node is transmitting it cannot hear any other node in the system which may be transmitting, since its own signal will drown out any others arriving at the node. Whenever a packet is to be transmitted, the transmitting node first sends out a short ready-to-send (RTS) packet containing information on the length of the packet. If the receiving node hears the RTS, it responds with a short clear-to-send (CTS) packet. After this exchange, the transmitting node sends its packet. When a packet is received successfully, as determined by a cyclic redundancy check (CRC), the receiving node transits and acknowledgment (ACK) packet. This back-and-forth way of communication avoids any chance of packet being lost or miscommunication. [5][7][12]

2.3.4 Security flaws in 802.11 standard

Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications. However, many organizations are rapidly deploying wireless infrastructures based on IEEE 802.11 standard, even though it is a known fact that there are serious security concerns associated with it. How these security problems affect an organization depend on their goals and type of wireless network employed within. The perceived insecurity of wireless networks has been a major inhibitor for its worldwide acceptance. Network architects are now faced with the challenge of designing secure networks in the light of the known security attacks and problems. Before describing some of the security risks and attacks associated with 802.11 standard, it would help to know how the communications process happens in a wireless network. [19]

Prior to communicating data, wireless clients and access points must establish a relationship, or an association. Only after an association has been established can the two wireless stations exchange data. The association process is a two-step process involving three states: Unauthenticated and unassociated, authenticated and unassociated, and authenticated and associated. To transition between states, the communicating parties exchange messages called management frames.

To begin with any client that wants to exchange information is in the unauthenticated and unassociated state of association process. All access points send a beacon management frame at fixed intervals. A client that wants to communicate with the access point keeps listening to the beacon management frame from the closest

access point available. The client then selects the access point to associate with and then sends a probe request management frame. After identifying the access point mutual authentication process is performed between the client and the access point and then the client moves from the first state to authenticated and unassociated state. The client now sends an association request form and then the access point responds whereby the client moves to the final state i.e. authenticated and associated state. After the above mentioned process is fulfilled a client becomes a peer of the wireless network that its trying to associate and can hence transmit data frame son the network. The following section documents some of the security risks associated with 802.11 wireless networks standard. [9][19]

Easy access. With the right kind of equipment wireless network are easy to detect. As explained earlier all the access points need to send a beacon management frame to announce their existence so that clients can connect to them. By monitoring beacon frames, wandering users with an 802.11 receiver can find out about wireless networks in the area simply by putting an antenna. This leads to insertion attacks, as information needed to join a network is also the information needed to launch an attack on the network. [9]

Insertion attacks. Insertion attacks are illegal use of wireless network resources without having to go through the security process. Insertion attacks can be done in two ways, either as unauthorized client or as unauthorized access point. In insertion attack by unauthorized client the attacker get connected to the internal network without being authorized. If the access point doesn't ask for a password then the attacker can get direct access to the network. There is a second kind of insertion attack in which the

attacker who has access to a wired network can set a base station (access point) to the network internally. Attacks can be done on the wired network through the access point in just the same way as unauthorized client using the access point that has been placed in the network does insertion attacks. [5][9]

Interception and session hijacking attacks: The frames that and transmitted in 802.11 networks are not authenticated. Even though every frame has an address it doesn't guarantee that the same station sends the packet received. Attackers can use spoofed frames to redirect traffic. If the access point is connected to a hub rather than a switch there is every chance that the attacker can monitor all the data being transmitted out of the hub. If an attacker can manage to sniff into the network then he can inject false traffic into a network. The attacker may even be able to issue commands on behalf of a authorized client and hijack a session. [5][9[19]

Misconfigurations: The access points or base stations are set in the least secure mode initially. t is the work of the network administrator to set the required settings based on the level of security required. A major concern with this aspect of 802.11 is that the base station maybe be misconfigured, by the system administrator, and thereby leading to various kinds of attacks. [3][8]

Jamming: As the name itself suggests is that kind of an attack in which the whole network is jammed so that there wont be any further service from the network. It is easy for an attacker with proper equipment to flood the 2.4Ghz frequency with illegitimate material so that the network stops functioning as it cannot differentiate between the legitimate requests and the ones sent by the attacker. This kind of attack can be

achieved by staying outside the range of the network by the access point or by staying within the wireless network. [3][8][9]

Brute force attacks: Even after having been properly configured with enough security setting the access point is still liable to be attacked by brute force dictionary attempts to find out the key by trying out all the possible passwords. The major reason for this kind of attack to be possible is the fact that most of networks share a common key among its clients so this way its is much easy to be able to crack it as it stays the same for a while. The intruder can gain access to the network if the attacker guesses the password once. [8][9]

Client-to-client attacks: The wireless clients can communicate with each other by-passing the access point. Therefore each client should be able to protect itself from other clients. One mode of client-to-client attack is transmission control protocol/Internet protocol (TCP/IP) service attack. In this kind of attack if the wireless client is running TCP/IP services then the attacker can exploit its settings through another client. In another type of client-to-client attack the attacker can cause the clients system to jam by sending bogus packets and thereby causing denial of service. [3][8]

Attacks against encryption: 802.11 provide no protection against attacks that passively observe traffic. The main risk is that 802.11 does not provide way to secure data in transit against eavesdropping. Frame headers are always in the clear and are visible to anybody with a wireless network analyzer. Security against eavesdropping was supposed to be provided by the much-maligned wired equivalent privacy protocol. WEP encryption and the security concerns associated with it are explained in detail in the next section. [8][18]

3. WIRED EQUIVALENCY PRIVACY (WEP)

3.1 Introduction to WEP Protocol

WEP, short for wired equivalent privacy protocol, is a protocol defined in 802.11 standard for wireless LANs. As the name suggests WEP was designed to make sure that security levels in wireless LANs are maintained at the same level as the wired LAN. WEP's aim is to protect data as it's transmitted from one point to another point by encrypting data over radio waves. The WEP algorithm was designed to protect wireless networks from eavesdropping by maintaining the confidentiality of link layer communications and also to prevent unauthorized access to a wireless network. The WEP protocol also does integrity checksum to eliminate tampering of transmitted date.

The WEP algorithm relies on a secret key that is shared within the wireless network. The secret key is used to encrypt the packet of data before they are transmitted. The WEP standard specifies the use of 40-bit keys. Unencrypted data is called plain text and the cipher text refers to encrypted data. WEP also uses an integrity check to make sure that the data is not modifies during transmission. Most wireless networks use single WEP key rather than multi WEP key techniques, which will make the data transmission much more secure. [5][7][16]

WEP encryption is the translation of data into a secret code. In an IEEE 802.11 standard the WEP encryption key is used to provide wireless clients with confidentiality and authentication. A WEP encryption is decrypted using the secret key or password. The 802.11 standard does not discuss how the shred key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. WEP encrypts plain text by RC4 (RC4 stands for Ron's code # 4, it is a

stream cipher developed by Ronald Rivest for RSA Data Security©) encryption method, which uses the shared key and an initialization vector (IV). The receiving client or access point decrypts the text in a similar fashion as it was encrypted using the RC4 algorithm.

Although the WEP protocol was designed to meet the security standards of wired networks, it was seriously hampered due to the regulations set by the government for cryptographic systems. The WEP key lengths were limited to 40 as strong cryptographic systems fell under the same export regulations as that of weapons for mass destruction. There are serious flaws that emerge with the usage of this protocol due to misapplication of the cryptographic primitives. These flaws lead to a number of attacks that prevent WEP from meeting its goal. The following sections depict the working of WEP protocol and the inherent flaws and attacks associated with it. [5][7]

3.2 WEP Protocol Implementation

Before explaining the process of exchanging data in a wireless network using WEP security standard, it is pertinent to know how the key stream or the per-packet-key is generated using the RC4 algorithm.

3.2.1 RC4 Encryption Algorithm

RC4 stands for Ron's code # 4 and is a stream cipher symmetric key algorithm. The RC4 algorithm uses a variable key length and a state table also known as initialization vector (IV). The state table is used along with the key to generate a key stream, which is XORed (exclusive-or) with the plain text to get the cipher text. The length of the variable key was limited to 40 bits because of the restrictions put forth by the government on all cryptographic techniques. But nowadays with the restrictions

being softened the 128-bit key is also in use. The RC4 algorithm works in two phases: key stream generation and ciphering. [17]

Key stream generation using RC4. This key stream generation phase is the most complex phase involved in the working of RC4 algorithm. In this phase the key stream is generated using the key and the state table (IV), with N number of mixing operations, with N being the key length. These mixing operations consist of swapping bytes, modulo operations, and other formulas. [17]

Ciphering. Once the key stream or the encrypting variable has been generated, it enters the ciphering phase, where it is XORed with the plain text to create an encrypted text. XOR is the logical operation of comparing two binary bits. Since the key stream and the text to be encrypted are of the same size so each individual bits of both are compared. If the bits are different, the result is 1. If the bits are the same, the result is 0. Once the receiver gets the encrypted message, it can be decrypted by XORing it with the same key stream. [23]

3.2.2 WEP Set up

Every peer connected to the wireless network is initialized with the secret or shared key via a mechanism that is undisclosed by the 802.11 standard. After the initial association process is completed, the data is transmitted from a client or access point to its peer connected on the wireless network in a sequence of three steps:

Checksumming. It is the first step in data transmission. The client willing to send data over the wireless network computes the check sum of the plain text. Cycle redundancy check (CRC) 32 is a kind of checksum in which an integer value obtained using the numerical value of the bits of the message is sent along with it. The sender

calculates the CRC value of the plain text and is appended to the plain text to be transmitted and the resultant frame is ready for encryption. [22]

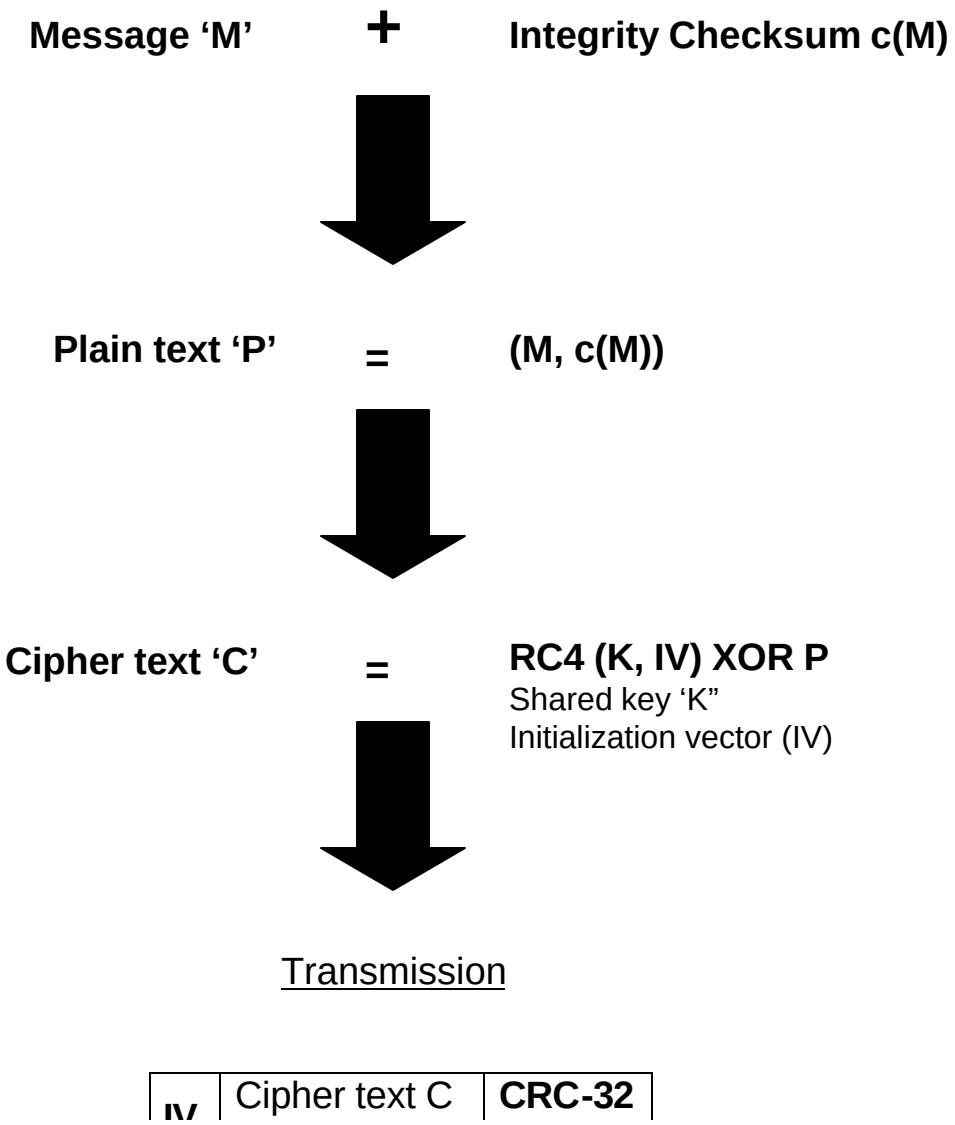

Figure 4: Transmission of data from sender to receiver in WEP protocol. [17][25]

Encryption. The intermediary packet obtained from the first stage is encrypted using the derived key stream obtained by using RC4 algorithm. An initialization vector is generated and then using the RC4 algorithm a key stream is generated. The sender

XORs the intermediary frame containing the plain text with the key stream generated. The resultant cipher text is ready to be transmitted on to the network. [7][25]

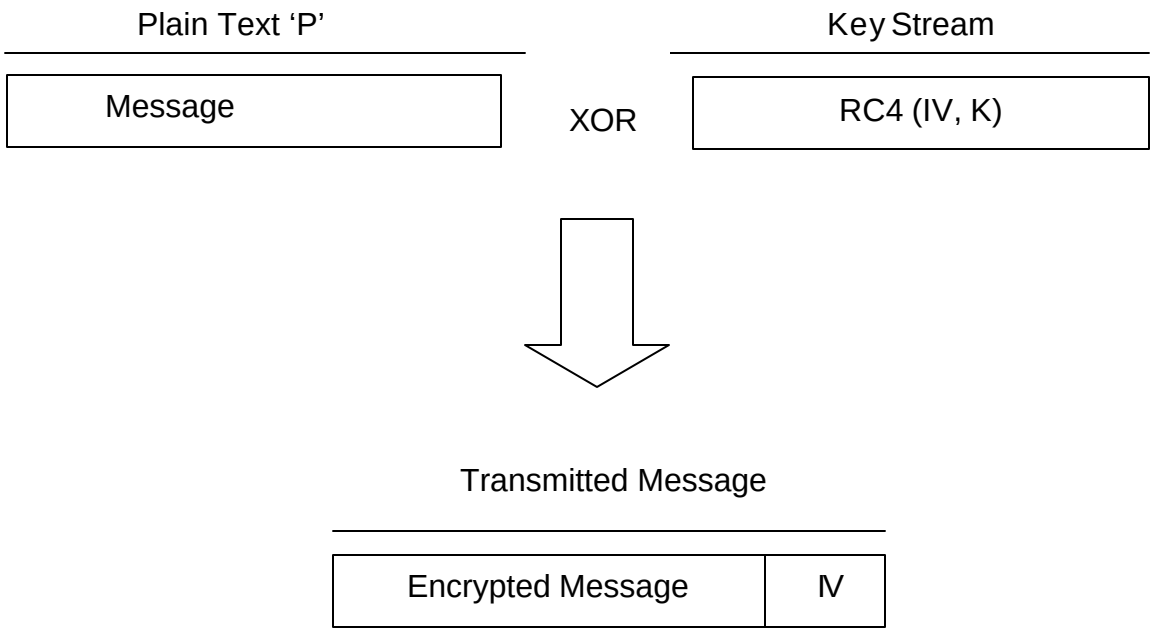

Figure 5: WEP frame transmission format. [17][25]

Transmission. The encrypted text obtained from stage 2 is appended with the initialization vector and is transmitted over the wireless network by the sender. The final frame is sent over radio links to the concerned receiver.

To decrypt the received frame the receiver just reverse engineers the steps done to encrypt the message. Using the initialization vector that has been sent along with the message and the shared key, which is already known the receiver, generates the key stream by implementing the RC4 algorithm. The receiver then decrypts the cipher text message by XORing it with the key stream obtained. The recipient then splits the plain

text message into two constituent parts: message and CRC. Computing its checksum and comparing it with the CRC value can confirm the validity of the message.

3.3 Major WEP Security Flaws

WEP was initially designed to focus on three security aspects of wireless networks, which are confidentiality, access control and data integrity. But in practice it barely manages to accomplish any of the three goals that it had aimed to achieve. The following section describes the security flaws and the relevant attacks associated with the WEP protocol.

3.3.1 Key Stream Reuse

The key stream is generated giving the secret key and the initialization vector as an input to the RC4 stream cipher algorithm. RC4 algorithm is also known as a stream cipher algorithm. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plain text to produce the cipher text. The receiver has the same secret key and using the IV, which in plain text format is sent along with the cipher text, decrypts the message. This mode of transmission works securely if the stream cipher key stream is never reused.

The RC4 algorithm repeats the key stream if the same key and IV are given as inputs. It is a known fact that the secret is changed very rarely as it is very troublesome to update the key for all the peers connected on the network. Hence the key stream reuse occurs due to repetitions of the initialization vector. The WEP IV is 24 bits long so there are a total of 2^{24} key streams possible as we use a secret key with varying the values of IV. So for each transmission, the sender uses one of these 2^{24} key streams to encrypt the data and therefore there is a very good chance of multiple reuses of IV.

Since the length of the initialization vector is set to 24 so this vulnerability is inherent and no compliant implementation can avoid it.

There is no such algorithm in 802.11 standard that prevents the reuse of IV. The only way WEP tries to prevent this attack is by generating a per-packet key stream instead of using a single key stream for the entire data being transmitted i.e. it increments the value of IV by 1 for every packet so that reuse of IV doesn't happen. Even the per-packet key stream mechanism doesn't serve the purpose as the IV generator is reset to zero every time its initialized so there is a very good chance that the lower end values of IV will be reused. [8][19][15]

3.3.2 Linear Checksum

The WEP protocol uses an integrity checksum of the message being transmitted using CRC-32 checksum, which is encrypted while it is sent along with the message on radio links. The problem with CRC-32 is that it is linear, which means that it is possible to compute the bit difference of two CRC's based on the bit difference of the messages over which they are taken. In other words, flipping bit n in the message results in a deterministic set of bits in the CRC that must be flipped to produce a correct check sum on the modified message. Because even after RC4 decryption the flipping bits are carried through, this allows the attacker to flip arbitrary bits in an encrypted message and correctly adjust the checksum so that the resulting message appears valid.

The CRC checksum is not a cryptographically secure authentication code as it is insufficient to ensure that an attacker cannot tamper with the message. CRC checksum's are designed to detect random errors in the message and they cannot

withstand against malicious attacks. The vulnerability of CRC is exacerbated by the fact that the message payload is encrypted using the stream cipher. [22]

3.3.3 Flaws in RC4 Key Scheduling Algorithm

One in every 256 keys generated by the RC4 algorithm can be a weak key. Weak keys are the keys identified by cryptanalysis that is able to find circumstances under which more one or more generated bytes are strongly correlated with a few bytes of the key. The key schedules for the keys generated by RC4 are less correlated with the key than they ought to be. This makes it far easier to crypt analyze data encrypted under these keys.

Once it's know that there class of weak keys in the RC4 algorithm, the obvious practical attack would be to search for potential weak keys first during an exhaustive search. However since only one in every 256 keys is weak, the effective reduction in search space is not particularly significant. The presence of weak keys can be a big drawback if the attacker is satisfied with recovering only a percentage of the keys subjected to analysis. In particular circumstances the relationship between weak keys may provide a much more significant reduction in the workload of the attacker.

The other concern with the RC4 algorithm is that it imperfectly hides correlation in the encrypted data. This property is also known as empirically measurable bias. This problem is inconsequential as long as WEP uses only an infinitesimal part of the generated key stream and far easier attacks against WEP's use of RC4 exist. [19][14]

3.2.4 Message Decryption

As described in the earlier section that it is very easy to modify messages being transmitted over the wireless network without even letting the receiver know about it.

This flaw leads to a new kind of problem, as it is easy to decrypt messages just as it is possible to modify the content of the message and direct it to the access point instead of sending it to the intended receiver. Even if the attacker cannot decrypt the message, it is possible to make the access point decrypt the message. The attacker can intercept a message and send a modified message, which the attacker is aware of to the access point. Since the access point has the shared key therefore it responds back after decrypting it.

3.4 Attacks on 802.11 Wireless Networks due to inefficient WEP protocol

Though the attacks being mounted on 802.11 are basically dependent on it's cryptographic vulnerabilities, in order for these to succeed the attacker should be able to get access to the transmitted data. The messages in wireless networks using 802.11 standard are sent through radio waves. It takes lot of infrastructure to get access to data that is being transmitted at 2.4GHz and also to inject messages at the same frequency. The attacker must also have an understanding of how the physical layer works in 802.11. The major problem with wireless networks being the fact that equipment supporting 802.11 standard is readily available in the form of wireless ethernet interfaces. Once an attacker gains access to the encrypted frame then based on the flaws associated with WEP protocol, there are various kinds passive and active attacks that the wireless networks can be subjected to. Here are some attacks on wireless networks, which are incurred due to inefficient WEP protocol. [18]

3.4.1 Passive Attack to Read Encrypted Traffic

This attack stems from the key stream reuse. Key steams are repeated every time the initialization vector is reused. Since the WEP IV is transmitted in plain text

along with the encrypted message so if the attacker can get hold of two encrypted messages with the same IV then it is possible to know the content of the message without having to decrypt it. XORing the two encrypted messages cause the key stream to cancel out thereby leaving the attacker with an XOR of the two plain texts.

It becomes very easy for the attacker to decipher the contents of the message by making educated guesses as the IP traffic has lot of redundancy, since protocols use well-defined structures in messages. Once a plain text for a specific IV has been detected form there onwards the plain texts for all other messages with the same IV is easy to attain, since all the pair wise XORs are known. Even if the attacker is not able to get hold of the plain text with the two encrypted texts available, further collisions for the same WEP IV value increase the chances of understanding the message being transferred in a specific wireless network. With only a small factor of time necessary, it is possible to recover a modest number of messages encrypted with the same key stream.

Even if the attacker is not able to decipher the pair wise XORs of the plain text, there is another means by which plain text can be recovered. The attacker can get hold of the information regarding where the message is being directed to, since the fields of IP traffic are very much predictable. Using this knowledge the attacker can send IP traffic directly to a mobile host under the attacker's control. The attacker sends a known plain text to the access point without raising any alarms as the access point thinks that it came from one of its peers on the network. The access point decrypts the message and sends it back to the attacker whereby it is easy to get the key stream. [15][19]

3.4.2 Decryption Tables

The reuse of key stream is caused by the small space of 24 bits provided for the initialization vector. While monitoring the traffic over a specific wireless network, which shares a common secret key for a considerable amount of time, if the attacker can get hold of a plain text then he can derive the key stream using the IV used. The plain text can be achieved by a thorough analysis of collision of encrypted messages with the same IV. The key stream obtained can be used to decrypt all other messages that use the same IV. Over a period of time the attacker can build a table or dictionary, which contains the key stream for each particular IV possible.

The maximum possible values for the initialization vector are 2^{24} since out the 64 bits available for encryption the secret key takes up 40 bits and the remaining 24 are allocated to the initialization vector. In order to set up a table with all possible value for IV it roughly takes about 24 GB, which is affordable when considered that the attacker might intend to misuse some valuable corporate information. Even if the attacker cannot afford the space and the time involved in monitoring for all the possible values of IV, it might as well be beneficial to set up a table for lower end values of IV. Since the wireless devices reset the value of IV to zero every time they are initialized so there is a very good chance that most of the collisions occur for the lower end values of IV. [18]

3.4.3 Active Attacks by Modifying Messages

This attack is based on the fact that the CRC-32 checksum used to check the integrity of message being transmitted does not serve the purpose. The checksum is linear, which means that the checksum is distributed over the entire XOR so therefore even if we flip some of the bits the resultant checksum can still be the same as the

original one. If the attacker can get hold of a plain text then he can make modifications in the plain text to get a corrupt message with the same checksum and start injecting the corrupt message over the wireless network. The recipients of the corrupt message sent by the attacker cannot notice any malpractice as they find that the checksum associated with the message keeps its validity in good stand.

The attacker will be able to inject corrupt messages even without complete knowledge of the packet. The attacker only needs to know the cipher text and the desired plaintext difference to create a new message with the same checksum value. If the attacker has partial knowledge of the contents in the message, it is possible to make selective alterations with the information available to create a new message with the same checksum value. [15][18][19]

3.4.4 Message Injection by Reusing IV

It was explained in section 3.2.1 that the collision of messages occurring for those using the same IV, leads to number of complex attacks on the wireless network. The 802.11 standard does not provide a mechanism to prevent repetitions of IV so it obviously an 802.11 device accepts messages even though they are encrypted using the same key stream. So it is possible to use already monitored IV values without letting the receiver detect the discrepancy.

It is easy to get the value of the initialization vector since it is transmitted in plain text over the wireless network. The attacker can inject corrupt messages with same IV values. Every receiver must accept messages even if they have repeated IV's or risk non-interoperability with compliant devices. The attacker can sometimes end up

jamming the network traffic for a client by sending many illegal messages based on the repeated IVs. [16][18]

3.4.5 Active Attacks by IP Redirection

These kinds of attacks use the ability to modify encrypted data without knowing the content as explained in section 3.2.3. By monitoring the wireless network traffic and intercepting a message we can determine the IP address of the designated receiver. As all the packets from the client's head towards the access point, it sometimes acts as IP router with Internet connectivity. A packet transmitted in 802.11 wireless networks follows certain standard format for packet headers, whereby the location for destination IP address is easy to decipher. Once the IP address is obtained the header information in the packet can be carefully manipulated by changing the bits in such a way that the new IP address in the packet is that of the system owned by the attacker. The attacker then directs the IP address modified packet to the access point, which is unable to detect any changes as the checksum tallies even with the new IP address. The access point then decrypts the packet and then sends it in plain text to the designated IP address that is owned by the attacker.

This kind of attack becomes tougher if the attacker doesn't know the original IP checksum. In this case the attacker tries to make educated guesses of the difference in IP checksum and tries to forward the packet to the access point. The access point just ignores the packet if the checksum doesn't match, as it has no mechanism to realize if an authorized client had sent the illegal packet or if it was a foul play by an attacker. [15][16[18][19]

3.4.6 Attacks On The Weak Keys In RC4

The key schedules for the keys generated by RC4 are less correlated with the key than they ought to be. This makes it far easier to crypt analyze data encrypted under these keys. Once it's know that there class of weak keys in the RC4 algorithm, the obvious practical attack would be to search for potential weak keys first during an exhaustive search. However since only one in every 256 keys is weak, the effective reduction in search space is not particularly significant. The presence of weak keys can be a big drawback if the attacker is satisfied with recovering only a percentage of the keys subjected to analysis. In particular circumstances the relationship between weak keys may provide a much more significant reduction in the workload of the attacker. [16][17]

3.4.7 Attacks Against TCP/IP Traffic

There are situations in which the wireless networks are used as a data link to TCP/IP network. An attacker can misuse the TCP/IP protocol in which the response to an accepted packet is an ACK acknowledgement. The attacker sniffs a packet on the wireless network and flips a few bits and adjusts the encrypted CRC accordingly to obtain a new cipher text with valid WEP checksum. The attacker then sends it to the access point, which is connected to the TCP/IP layer and waits for its response. The acknowledgement packets are easily identified by their size, without needing to be decrypted. Every data frame contains known plain text therefore the attacker can recover partial key stream with every frame sent. The bits to be flipped should be carefully chosen so that that the TCP checksum remains undisturbed. [16][18][19]

4.0 PROPOSED SOLUTIONS AND CONCLUSIONS

4.1 Counter Measure For Improving WEP's Security

Trying to improve WEP security is not an easy task. The major factor being that the 802.11 standard has been widely deployed in most of the wireless networks and now any improvements made to the standard should be interoperable with the previous standards. The future work regarding the security aspects of wireless networks should make sure that the security is enhanced without reducing the line rates. Systems already deploying 802.11 standard should not be made to upgrade any further hardware. The new standard with the improvements should allow for incremental deployment rather than being asked to change to a new standard all of a sudden. Keeping all the above aspects in the mind the following recommendations should help in eliminating the discrepancies in WEP security.

4.1.1 Encrypting The Initialization Vector With The Secret Key

Most of the passive attacks stem from the fact that the initialization vector used by the RC4 algorithm is sent in plain text along with the encrypted message. The value of IV is being sent in plain text, as the receiver needs it to decrypt the encrypted message using the RC4 algorithm again. The security of WEP can significantly be improved by encrypting the initialization vector as well. The initialization vector can be encrypted using the secret key, as all the peers on the wireless network are aware of it.

The initialization vector can be encrypted using a simple and effective algorithm such as tiny encryption algorithm (TEA). TEA is one of the fastest and most efficient cryptographic algorithms. TEA encrypts 64 bits at a time and can use a 128-bit key. If the initialization vector is encrypted using TEA, even a one-bit difference in IV will cause

a 32-bit difference in cipher text. Even decryption of the TEA encryption technique is quick and easy. Two different kinds of encryption schemes one for the message and one for the initialization vector are going to make the transmission process a bit complex, but as security is of utmost importance may be it is worth it. [24]

4.1.2 Using A New Stream Cipher:

Most of the drawbacks associated with the stream cipher RC4 have been already explained. Even expanding the length of the key size to 128 bits does not bring about any major improvement in the security aspect of WEP, since the initialization vector, which doesn't vary even if the key size has been changed, has caused the problems described so far. So the problem hasn't been with the key but the cryptographic algorithm RC4, which is being used. It would be beneficial to replace the encryption technique with newer encapsulations schemes such as advanced encryption standard (AES) or use probabilistic encryption techniques. The problem associated with changing the stream cipher is that the standard with the new encapsulation scheme should be interoperable with the previous standards, which are already in operation using RC4 stream cipher.

4.1.3 Changing WEP Keys Frequently

One of the major problems with WEP has been the fact that most of the wireless networks use the shared key for a considerable length of time. If an attacker gets hold of the key then all of the data being transmitted on the network is easy to encrypt with the key and the initialization vector, which is available in plain text. Frequent re-keying makes it harder to recover the encryption key. By refreshing the key after a set intervals or after sending specific number of frames can greatly reduce the rate of encrypted key

being derived. Changing the key does not give the attacker enough time to intercept sufficient data to crack the key. Even if the attacker manages to do so due to the refreshing there is a very good chance that key would have changed by then. Authenticated key refresh in MAC layer provides a secure and synchronized mechanism for re-keying.

4.1.4 Random Generation And Increase In Bit Size For The Initialization Vector

Reuse of the initialization vector has been a big concern for WEP security. The only way WEP tries to prevent this attack is by generating a per-packet key stream instead of using a single key stream for the entire data being transmitted. Even the per-packet key stream mechanism doesn't serve the purpose as the IV generator is reset to zero every time its initialized so there is a very good chance that the lower end values of IV will be reused. Generating random values for IV, using a pseudo-random number generator might avoid the problem. [20]

The WEP IV is 24 bits long so there are a total of 2^{24} key streams possible with a secret key with varying values of IV. So for each transmission, the sender uses one of these 2^{24} key streams to encrypt the data and therefore there is a very good chance of multiple reuses of IV. Since the length of the initialization vector is set to 24 so this vulnerability is inherent and it can be avoided by using a much bigger IV. It is tough to end up building a decryption dictionary for a 128-bit initialization vector.

4.1.5 Eliminating The Weak Keys In RC4 Stream Cipher

As already described the presence of weak keys reduces the workload on the attacker to crack the key stream. The weak keys occur due to inadequate mixing of the key bytes during the generation of the RC4 state table. Discarding the number of bytes

generated, because the algorithm used to generate bytes introduces additional non-linear dependencies into the state table, can eliminate the weak keys. Ensuring that multiple session keys are not linearly related also reduces the chances of having weak keys. [17]

4.2 Conclusions

I have documented serious flaws and attacks associated with the implementation of wired equivalent privacy protocol in 802.11 wireless networks standard. Though WEP tries to attain the security standards of wired LANs, frankly it falls way short of its goal. The recommendations suggested in this document may not necessarily make WEP an acceptable standard because it has many inherent discrepancies that are vulnerable to be attacked in future. In order for wireless networks to be accepted as a secure networking medium, 802.11 has to rethink about WEP protocol and see if it can build a secure link layer transmission protocol from scratch rather than trying to work around it. Though it may sound as a sensible thing to do, there are strings attached to it that make one rethink if it is possible, because it might not be possible to make a new security protocol interoperable with so many deployed wireless network infrastructures and ones being deployed. Hopefully wireless networks in the future are going to be as secure as the wired networks.

REFERENCES

1. R. Bagrodia, W.W.Chu, L. Kleinrock, and G. Popek, “Vision, Issues, and Architecture for Nomadic Computing,” institute of electrical and electronics engineers (*IEEE) Personal Communications*, December 1995, pp. 14-27.

2. K. Pahlavan, A. Zahedi, P. Krishnamurthy, “Trends in Local Wireless Networks,” *IEEE Communications Magazine*, March 1995, pp. 88-95.

3. G. H. Forman and J. Zahorjan, “The Challenges of Mobile Computing,” *Computer Networking*”, April 1994.

4. P. Lettieri and M.B. Srivastava, “Advances in Wireless terminals,” *IEEE Personal Communications*, (1999), pp. 6–19.

5. N. Vaidya, Tutorial: “Mobile ad hoc networks: routing, MAC and transport issues,” *ACM MobiCom Tutorials*, Boston, MA (2000).

6. D. Buchholz, P.Odlyzko, M. Taylor, R. White, “Wireless In-Building Network Architecture and Protocols,” *IEEE Network Magazine*, November 1991, pp. 31-38.

7. IEEE, “ Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,” Std 802.11D6.2, December 1997.

8. H. Ahmadi, A. Krishna, and R. O. Lamaire, “Design Issues in Wireless LANs,” *Journal of High Speed Networks*, Vol. 5, 1996, pp. 87-104.

9. C. A. Rypinski, “Standard Issues for Wireless Access,” *Business Communications Review*, August 1992, pp. 40-45.

10. A.J. Menezes, P.C. van Orschot, and S. A. Vanstone, “Handbook of Applied Cryptography,” chemical robber company (CRC) press 1996.

11. L. Goldberg, “Wireless LANs: Mobile Computing’s Second Wave,” *Electronic Design*, Issue 26, June 1995.

12. K. Chen, “ Medium Access Control of Wireless LANs for Mobile Computing,” *IEEE Network*, September/October 1994.

13. B.E. Mullins, N.J. Davis IV, and S.F. Midkiff, “An Adaptive Wireless Local Area Network Protocol That Improves Throughput Via Adaptive Control of Direct Sequence Spread Spectrum Parameters,” to appear in *ACM Mobile Computing and Communication Review*, Vol. 1, No. 3, 1997.

14. S. Kent and R. Atkinson, RFC 2401, “Security Architecture for the Internet Protocol,” IETF, November 1998.

15. Borisov, Nikita, and David Wagner. “Intercepting Mobile Communications: The Insecurity of 802.11.” Published in the proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, July 16-21, 2001.

16. Mishra, Arunesh, and William Arbaugh. “An Initial Security Analysis of the IEEE 802.1x Security Standard.” February 6, 2001. http://www.cs.umd.edu/~waa/1x.pdf

17. A.W. Arbaugh, “An Inductive Chosen Plaintext Attack Against WEP/WEP2.” IEEE Document 802.11-01/230, May 2001.

18. Fluhrer, Scott, Itsik Mantin, and Adi Shamir, “Weakness in the Key Scheduling Algorithm of RC4.” Presented to the Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

19. Stubblefield, Adam, John Ioannidis, and Aviel D. Rubin. “Using Fluhrer, Mantin, and Shamir Attack to Break WEP,” *AT&T Labs Technical Report* TD-4ZCPZZ. Revision 2, August 2001. http://www.cs.rice.edu/~astubble/wep

20. D. B Johnson and D.A. Maltz, “Protocols for Adaptive Wireless and Mobile Networking,” *IEEE Personal Communications Magazine*, February 1996, pp. 34-41.

21. L. Blunk and J. Vollbrecht, “PPP Extensible Authentication Protocol (EAP),” Tech. Rep. RFC2284, Internet Engineering Task Force (IETF) March 1998.

22. B. Braden, D. Borman, and C. Patridge, “Computing the Internet Checksum.” Internet Request for Comments RFC 1071, Internet Engineering Task Force, September 1988.

23. E. Dawson and L. Nielsen, “Automated Cryptanalysis of XOR Plaintext Strings,” *Cryptologia*, (2): 165-181, April 1996.

24. P. Kocher, “Cryptanalysis of Diffie-Hellman, RSA, DSS and Other Cryptosystems Using Timing Attacks,” Advances in cryptology, CRYPTO ’95: 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27-31, 1995: proceedings, pages 171-183, Springer-Verlag, 1995

25. S.G. Stubblebine and V.D. Gilgor, “On Message Integrity in Cryptographic Protocols,” In Proc. IEEE Symposium on Research in Security and Privacy, pages 85-105, 1992.