ENHANCING WLAN SECURITY THROUGH IEEE 802.1X AND RADIUS

Himanshu[1], Mr. Rakesh Joon[2]
[1]M.Tech (ECE), [2]Asst. Prof. ECE
Ganga Institute of Technology and Management, Village Kablana, Jhajjar

ABSTRACT: WLANs are become popular due to their completely different advantages. Beside of these advantages, WLANs also are facing the most important drawback of security, therefore that's why a lot of folks do analysis on wireless local area network to boost the safety as a result of several firms wish to transfer their smart information over wireless local area network. This report discusses the safety problems with wireless local area network supported IEEE 802.11 normal, such variety of networks are brought up as Wi-Fi network. Wireless local area network is deployed as associate degree extension of already existed wired-LAN. So it's necessary to supply the safety of wireless local area network equals to Wired-LAN. We tend to worked during a research lab atmosphere so as to piece the 3 completely different security solutions (WEP, WPA &amp; WPA2 exploitation IEEE 802.1X) on infrastructure mode for personnel and enterprise design of wireless local area network. For every security resolution we tend to used the 'Backtrack' as a security cracking tool. so as to interrupt the WEP (64 and 128 bit long) security key of wireless local area network, build comparison between sixty four and 128 bit long WEP key and additionally analyzed the various quite attacks and a few problem of exploitation WEP security in wireless local area network. within the same means piece the WPA and WPA2 (using IEEE 802.1X) security resolution in infrastructure mode of wireless local area network and used identical security cracking tool double back so as to interrupt the safety of wireless local area network and analyze the various attacks on the network in these design and downsides of exploitation WPA and WPA2 security solutions. By exploitation IEEE 802.1X and RADIUS server we are able to improve the safety of enterprise network. Within the finish we tend to escort several conclusions and suggestions which will facilitate so as to supply higher security whereas deploying Wireless local area network.

Keywords: WLAN, WEP, WAP, Ad Hoc Network, Security, Attacks, etc.

I. INTRODUCTION

1.1 Introduction

Now days WLANs area unit more and more famous attributable to their reduced value of parts, simple to deploy at anytime and anyplace within the world. finish purchasers area unit in an exceedingly position to send big files through the communication medium that's air and liberated to move within the boundary of wireless local area network, ready to access the web and big information measure activities while not the necessity of any cable or property with a switch or a hub. Beside all of those advantages WLANs face the matter of security as a result of several firms area unit transferring their wise knowledge across the WLANs. thus numerous individuals do analysis on the wireless local area network security. WLANs area unit created for a wise transfer of knowledge. at first the aim of making wireless local area network as associate degree addition for the already put in wired LAN. During the history of the WLANs it faces solely single downside that's of Security. Still heap of analysis goes thereon the way to improve the safety so as to create the network safer and reliable then the Wired LAN. The breach within the security of wireless local area network can mechanically hurt the wired LAN as a result once RFs started acquiring the air than there's an opportunity of hazard of special attacks that we are going to discuss in next chapters. Our main goal of the study is to create our network more secure and reliable. There area unit 5 basic predefined goals for WLANs and there area unit completely different security solutions out there which can facilitate to supply the 5 basic goals. we tend to area unit getting to analyze that security resolution is totally providing the goals. once any security resolution is prepared to supply the higher than five goals, security is mechanically achieved for the WLANs. {we will|we'll|we area unit going to} additionally analyze that what number completely different attacks are potential and the way to mitigate them likewise represented additional. We area unit getting to put together the various security resolution like WEP, WPA and WPA2 in an exceedingly research lab surroundings. From the two labs we tend to area unit getting to analyzed that security resolution is best amongst beat order to supply the higher security and which sort of general attacks area unit potential and the way to mitigate all of them with their solutions in next chapters.

1.2 WLAN Basics

The WLAN could be a wireless technology regarding that terribly restricted variety of individuals is aware of within the previous couple of years. It grew chop-chop in an exceedingly tiny amount of your time a bit like a mobile communication and net technology. This development is simply owing to the WLANs, which give low value, flexibility, measurability and simple development. nevertheless this technology additionally brings heap of great problems like security, calibre of service.

1.3 Types of WLAN

WLAN operates in 2 modes, that are given below.

- Ad Hoc Mode.

- Infrastructure Mode.

1.3.1 Ad Hoc Mode

Ad hoc mode is additionally called peer to peer or IBSS (Independent Basic Service Set). it's a kind of local area network within which the network is formed solely by the wireless devices while not the necessity of any centralized controller or AP. during this design the wireless network is relatively simple to form and every and each device will communicate with one another instrumentality within the network with facilitate of NICs. this kind of network is extremely helpful for little organization wherever computers aren't interested to examine the data of alternative computers. In accidental mode there's no would like of Access purpose as a result of all of the digital computer and computers are connected with a wireless NIC card which may communicate with one and alternative via Radio waves. The accidental mode is appropriate for chop-chop fixing a wireless network in an exceedingly building conference centre, meeting space or anywhere else wherever enough wired infrastructure mode doesn't exist.

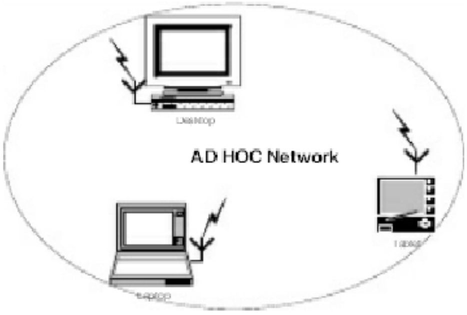


Figure 1.1: Adhoc Mode design

1.3.2 Infrastructure Mode

The purpose of victimisation the infrastructure design in WLAN is to expand the wired network by victimisation the wireless instrumentality i.e. base station additionally called access point (AP). AP is perform as a bridge between wireless and wired network and additionally performs sort of a centralized controller in an exceedingly wireless network for all wireless shoppers. The AP is answerable for manage the transmission andreception of many wireless equipments at intervals a restricted boundary of the network. totally different vendor's product will support the various ranges and variety of wireless instrumentality based mostly onthe wireless normal. Network administrator will use the many APs within the infrastructure modein order to extend the scale of the network. This project relates with the infrastructure mode, all the work wiped out this design.

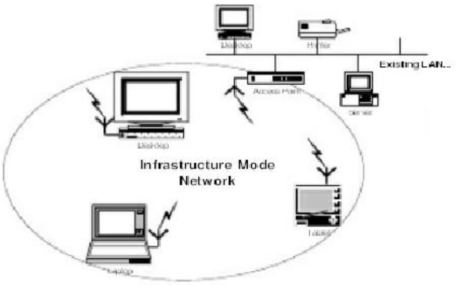


Figure 1.2: Infrastructure Mode Architecture

II. LITERATURE REVIEW

Martin Beck and Erik Tews (8 November 2008) described two attacks on IEEE 802.11 based wireless LANs. The first attack is an improved key recovery attack on WEP, which reduces the average number of packets an attacker has to intercept to recover the secret key. The second attack is (according to our knowledge) the first practical attack on WPA secured wireless networks, besides launching a dictionary attack when a weak pre shared key (PSK) is used. The attack works if the network is using TKIP to encrypt the traffic. An attacker, who has about 12-15 minutes access to the network is then able to decrypt an ARP request or response and send 7 packets with custom content to network. They finally concluded that the TKIP protocol used by WPA is not much different from WEP, so that attacks on WEP can affect the security of networks using TKIP, as seen in the paper. Even WPA with a strong password is not 100% secure and can be attacked in a real world scenario. Although this attack is not a complete key recovery attack, they have suggested that vendors should implement Counter measures against this attack. Because the problem can be fixed in a high level part of the protocol.

Frank H. Katz (July 2010) investigated the differences between WPA and WPA2, the vulnerabilities and limitations of each, the reasons why WPA2 is considered to be a more robust and secure standard than WPA.Significant weaknesses in the Wired Equivalency Protocol (WEP) led to the creation of the Wi-Fi Protected Access (WPA) Wired Local Area Network (WLAN) security protocol and the amendment to that protocol, WPA2. Recent work by Eric Tews of the Technical University of Darmstadt and fellow German security researcher Martin Beck indicate that WPA can be cracked in 15 minutes. Their work tends to confirm that it was necessary to replace WPA with WPA2.

They finally concluded that WPA encryption protocol can be cracked due to vulnerabilities in the TKIP encryption algorithm. After analyzing the WPA and WPA2 wireless encryption protocols and enumerating their differences, it is clear that the Advanced Encryption Standard, which is an integral component of the WPA2 protocol, is a significant improvement over WPA'sTKIP. Current technology is adequate to ensure that organizations can implement WPA2, and organizations that useWPA should consider implementing WPA2.

S.Chandramathi, K.V. Arunkumar, S.Deivarayan and P.Sendhilkumar (April 2006) explained that a wireless local area network (WLAN) is a flexible data communication system implemented as an extension to or as an alternative for a wired local area network (LAN). The 802.11 standard defines the Wired Equivalent Privacy (WEP) protocol and encapsulation of data frames for the purpose of security of the wireless LAN systems. It is intended to provide data privacy to the level of a wired network. WEP suffered threat of attacks from hackers owing to certain security shortcomings in the WEP protocol. Despite its short comings one cannot undermine the importance of WEP as it still remains the most widely used system.WEP suffers security pitfalls due to weak key management of the shared secret key and initialization vector (IV) repetitions. To overcome these problems, the existing WEP protocol is modified in this project to enhance the security of WLAN systems by dynamically changing the WEP key based on the network traffic intensity and updating it frequently based on the number of frames transmitted by using fuzzy logic which ensures message privacy as the encryption is not breached.

Maocai Wang, Guangming Dai, Hanping Hu and Lei Pen (2008) analyzed the security of IEEE 802.11. Based on the discussion of IEEE 802.11 security requirement, the three security technologies—SSID (Service Set Identifier), MAC(Media Access Control), WEP(Wired Equivalent Privacy) in WLAN standard IEEE802.11 are introduced, especially the encrypting algorithm and the integrity check algorithm in WEP. The security flaws caused by RC4 algorithm, key management, initialization vector Space, CRC algorithm and authentication mechanism in WEP are analyzed mainly in this paper. At the end of the paper, some advices and strategies to these flaws are given.

Olli Vihervuori (27 April 2009)evaluates wireless local area network security standards WEP, WPA and WPA2 with an emphasis on recent research findings concerning new attack methods and proposed improvements to counter those attacks. This paper concludes that WEP must be considered totally insecure because the best implemented attack techniques are fast and widely available. WPA is much safer but increasing number of attacks exploiting its vulner abilities exists. Thus far, a partial break of the algorithm has been successful but only in specific conditions. The newest security standard, WPA2, is generally secure enough in practice, because there are no publicly known attacks threatening data confidentiality and integrity. The standard may still need some minor changes because several denial-of-service attacks against it have been devised. This paper also discusses Wi-Fi Protected Setup which is the newest wireless LAN related security standard by Wi-Fi Alliance. It turns out to be helpful to the users, but it brings along some difficult to exploit but very serious security issues.

Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen (5 November 2007) have given a comparative study of the different wireless protocols. Bluetooth, ultra-wideband (UWB, over IEEE 802.15.3), ZigBee (over IEEE 802.15.4), and Wi-Fi (over IEEE 802.11) are four protocol standards for short range wireless communications with low power consumption. From an application point of view, Bluetooth is intended for a cordless mouse, keyboard, and hands-free headset, UWB is oriented to high-bandwidth multimedia links, ZigBee is designed for reliable wirelessly networked monitoring and control networks, while Wi-Fi is directed at computer-to-computer connections as an extension or substitution of cabled networks. In this paper, we provide a study of these popular wireless communication standards, evaluating their main features and behaviors in terms of various metrics, including the transmission time, data coding efficiency, complexity, and power consumption. It is believed that the comparison presented in this paper would benefit application engineers in selecting an appropriate protocol.

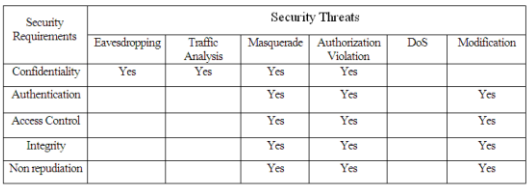
III. CONCEPT AND THEORY PROBLEM

3.1 The WLAN Security Problem

Problems that WLAN Security is facing as a result of the quantifiability, simple &amp; giant readying of the network and these characteristics starts a various variety of issues that require some solutions. If someone compromise the protection then network is useless. each AP out there within the network is information processing based; want some management, oversight and management. This action produces the additional load, creates problem for the wireless technologies throughout the implementation this can be as a result of each AP has identical configuration this similarity between the APs can tend to some misconfiguration and inappropriate action of the WLAN and a giant headache to distribute &amp; maintain quick configuration for all APs out there within the WLAN. It’s terribly onerous to supply the physical security to every AP within the network as a result of there location is usually outside from a server space or bolted space. The taken of that AP with its secrets, interloper will build use of these secret resources. to mend the on top of aforementioned issues, completely different vendors started work along so as to supply the answer by combination the various network change techniques, centralized, management and share wireless access in a very new style. therefore mixed answer provides a profit and friendly interface among the AP and a controller to mend all the issues appears undesirable. By use of ACs the threat of taken information processing is totally solved . the various WLANs victimization the devices for the management network access so as to supply packet delivery among the host to host for the various WLAN that additionally accumulated responsibleness. so as to supply the higher security to the WLAN, the APs area unit put in at anywhere wherever there's a less physical security out there, thus CAPWAP style will decrease the importance of taken AP. Let suppose all the high price secrets of AP area unit saved within the AC just like the RADIUS shared secrets, when the taken of AP won't turn out any threat for the network. therefore AC may be a device which will be place at a foothold wherever there's a physical security out there.

3.2 Security demand of WLAN

To provide the protection to WLAN, It needs 5 main security necessities to be achieved that area unit knowledge integrity, confidentiality, authentication, access management &amp; Non repudiation [5 –9].This section explains the aim of every security demand in terms of the protection threats, suggests that that security demand is employed to defend that security threat [5-9]. generally security threats area unit Eavesdropping and traffic analysis, Masquerade, Authorization violation, DoS &amp; Modification of forgery of knowledge [5-9]. therefore the below table best describes the aim of every security demand, suggests that that security demand is employed to mitigate that threat so as to supply the higher security to the wireless network.



Security Requirements	Security Threats					
	Eavesdropping	Traffic Analysis	Masquerade	Authorization Violation	DoS	Modification
Confidentiality	Yes	Yes	Yes	Yes		
Authentication			Yes	Yes		Yes
Access Control			Yes	Yes		Yes
Integrity			Yes	Yes		Yes
Non repudiation			Yes	Yes		Yes

Table 3.1: Security Goals w.r.t. Security Threats

Each security answer (WEP, WPA and WPA2) has got to offer the on top of 5 security demand to form a secure WLAN. so to stay removed from the various attacks in little or larger WLAN, the network administrator should use the particular security mechanism within the WLAN so as to form the network a lot of and a lot of consistent and ascendable. presently wireless web is growing terribly quick; as a result there's an excellent have to be compelled to build communication safer else this fast speed of knowledge flow becomes useless for everyone.

3.3 Attacks on WLAN

Currently WLAN faces many security threats and attacks because of its nature as a result of the data is broadcast into the air through that one will break the protection of WLANs having very little understandings regarding the network.
Different types of attacks and threats are classified in to 2 main components. These kind of attacks are thought of to be general in context for each WLANs and can delineate more thoroughly with their problem and solutions.

- Logical Attacks
- Physical Attacks

IV. PRESENT WORK

4.1 Working Methodology

There area unit totally different forms of security attacks in local area network network which may hurt the network and may exploit it. This report explains the various general attacks with their mitigation techniques and a few special attack son security solutions. in the main there area unit 2 general forms of attacks, physical and logical attacks. Here area unit few attacks in local area network and additionally there solutions the way to secure from those attacks.
• Logical Attacks with their mitigation techniques (Spoofing of raincoat address, Denial of Service Attack, Man within the Middle Attack., Default Access purpose Configuration, intelligence operation Attacks, spoken language Sniffing, and Dynamic Host Configuration Protocol Attack).
• Physical Attacks with their mitigation techniques (Rogue Access Points, Physical placement of Access Points, Access Points Coverage, and Spam Attack).
So first build straightforward Wireless native space Network (WLAN) in AN infrastructure mode by exploitation obtainable equipments. at first no security to network suggests that network is totally liable to attacks suggests that network is open for the unwelcome person to access the knowledge terribly simply. sensible work is split into 3 experimental labs.
(1) For the first research laboratory, designed a local area network in infrastructure mode by exploitation all the obtainable equipments. to supply initial security to the local area network assemble the WEP security answer from each AP and shopper perspective within the research laboratory surroundings though this WEP is relatively sensible instead of local area network having while not security. once implementing WEP security, use the cracking tool backtrack5 so as to interrupt the WEP (64 and 128 bit) long security key and conclude that however WEP secret's straightforward to interrupt forWLAN and analyze that however WEP security is unreliable for secured network.
(2) For the 2d research laboratory use identical local area network infrastructure network and assemble the WPA and check out to interrupt the WPA coding key by wordbook attacks exploitation identical cracking computer code backtrack5 and analyze what proportion reliable this security answer with relevancy WEP and conclude that one is a lot of higher.
(3) For the third research laboratory additionally we tend to use identical local area network infrastructure network, however now we tend to assemble the WPA2 and check out to interrupt the WPA coding key by wordbook attacks exploitation identical cracking computer code backtrack5 and analyze what proportion reliable this security answer with relevancy WEP &amp; WPA and at last conclude that one is that the best among all the 3 protocols.

4.2 *Required Tools*

In WLAN configuration many different types of tools are uses according to the requirements, in this project following tools are used to fulfill the task.

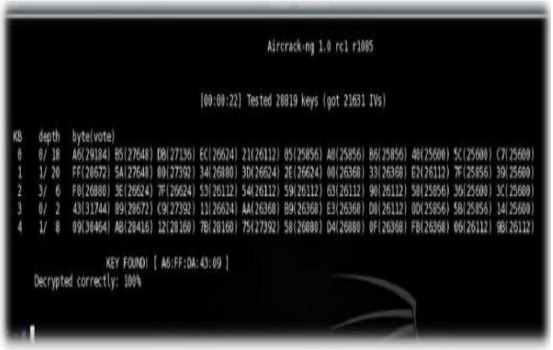
- A Wireless Router
- Minimum two Laptops with Compatible WLAN cards
- The BACKTRACK-5 Operating System
- A Flash Drive (pen drive) for booting the OS directly.

Word List – Searched via torrents.

V. RESULT AND DISCUSSION

5.1 WEP

From the top of research laboratory experiments, it's clear that WEP key's abundant easier to crack victimization some commands of the double back OS, and also the whole method takes a couple of minutes solely. thus WEP is very unsafe for WLAN security. the full procedure is shown within the previous chapter.
It is clearly visible that the WEP key has been cracked with success. The retrieved key's within the hex and may be accustomed hook up with the network.

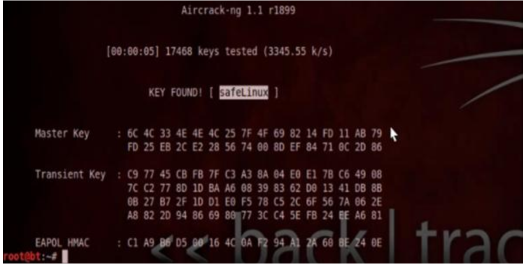


```
                              Aircrack-ng 1.0 rc1 r1085


                    [00:00:22] Tested 28819 keys (got 21631 IVs)

KB   depth  byte(vote)
 0   0/ 18  A6(29184) B5(27648) DB(27136) EC(26624) 21(26112) 05(25856) A0(25856) B6(25856) 40(25600) 5C(25600) C7(25600)
 1   1/ 20  FF(28672) 5A(27648) 80(27392) 34(26880) 3D(26624) 2E(26624) 00(26368) 33(26368) E2(26112) 7F(25856) 39(25600)
 2   3/  6  F0(26880) 3E(26624) 7F(26624) 53(26112) 54(26112) 59(26112) 63(26112) 90(26112) 58(25856) 36(25600) 3C(25600)
 3   0/  2  43(31744) 89(28672) C9(27392) 11(26624) AA(26368) B9(26368) E3(26368) D8(26112) 0D(25856) 5B(25856) 14(25600)
 4   1/  8  09(30464) AB(28416) 12(28160) 7B(28160) 75(27392) 58(26880) D4(26880) 0F(26368) FB(26368) 06(26112) 9B(26112)

                    KEY FOUND! [ A6:FF:DA:43:09 ]
      Decrypted correctly: 100%
```

- As demonstrated above, WEP cracking has become more and more easier over the years, in past it's going to needed tons of, thousands packets or days of capturing knowledge to crack the WEP however currently a days it is accomplished inside couple of minutes about 20k knowledge packets. WEP attack is minimize or tougher by victimisation longer IVs size like forty eight bit long IVs instead of 24-bit long IVs.
- WEP's major weakness is its use of static coding keys. once you came upon a router with a WEP coding key, that one secret's employed by each device on your network to cypher each packet that is transmitted. however the actual fact that packets are encrypted does not stop them from being intercepted, ANd owing to some deep technical flaws it's entirely attainable for an snooper to intercept enough WEP-encrypted packets to eventually deduce what the secret's.
- This drawback accustomed be one thing you'll mitigate by sporadically ever-changing the WEP key (which is why routers usually enable you to store up to four keys). however few trouble to try and do this as a result of ever-changing WEP keys is inconvenient and long.
- It wasn't long before a replacement technology referred to as WPA, or Wi-Fi Protected Access debuted to deal with several of WEP's shortcomings.

5.2 WPA

Now we have a tendency to come back to WPA. within the similar fashion WPA may also be cracked as shown within the last chapter. In my experiment I even have used the wordbook attack, within which we have a tendency to use an outsized variety of words (keys) hold on in numerous wordlists. The time taken to crack the key depends on the dimensions of the wordlist. Larger the dimensions, easier the cracking.



```
                    Aircrack-ng 1.1 r1899

          [00:00:05] 17468 keys tested (3345.55 k/s)

                 KEY FOUND! [ safeLinux ]

Master Key     : 6C 4C 33 4E 4E 4C 25 7F 4F 69 82 14 FD 11 AB 79
                 FD 25 EB 2C E2 28 56 74 00 8D EF 84 71 0C 2D 86

Transient Key  : C9 77 45 CB FB 7F C3 A3 8A 04 E0 E1 7B C6 49 08
                 7C C2 77 8D 1D BA A6 08 39 83 62 D0 13 41 DB 8B
                 0B 27 B7 2F 1D D1 E0 F5 78 C5 2C 6F 56 7A 06 2E
                 A8 82 2D 94 86 69 80 77 3C C4 5E FB 24 EE A6 81

EAPOL HMAC     : C1 A9 B6 D5 00 16 4C 0A F2 94 A1 2A 60 8E 24 0E
root@bt:~# 
```

The figure shows that finally the key has been cracked which is “safeLinux” in this case.

Improvements over WEP:

Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA was created to replace WEP in securing wireless networks when it was found out that serious flaws made it very easy to gain access. Despite being much harder to crack, it was still possible with the use of more advanced tools like the one used above (Backtrack5).

5.3 WPA2

To overcome the shortcomings of WPA, WPA2 came into picture that addresses this downside with the introduction of the AES algorithmic program. in theory, passphrases created with the AES algorithmic program are just about uncrackable. however it may be cracked with a lot of and a lot of word lists, though it takes plenty of your time to crack WPA2 key, that’s why we are saying it in theory uncrackable. the sole disadvantage of WPA2 is within the quantity of process power that it desires so as to shield your network. This interprets to an immediate want for a lot of powerful hardware or suffer a discount in network performance for heavily used networks. this is often a problem with older access points that were designed and engineered before WPA2 and solely enforced WPA2 via a computer code upgrade. Most of the newer access points are equipped with a lot of capable hardware to reduce the speed degradation. So on the idea of all the study and experiments, we have a tendency to came to understand that WEP, WPA each the protocols are unsafe for WLAN, even WPA2 with PSK is additionally crackable. However it's terribly troublesome or virtually not possible to crack WPA2 with AES.

VI. CONCLUSION AND FUTURE WORK

6.1 Conclusion

The main goal of this thesis was to show the attacks on WLAN and test the few of attack in lab environment and finally decide which one is the best solution in lab environment. This thesis implemented the three major security techniques WEP, WPA and WPA2.

- First lab implemented the WEP security technique and this lab clearly showed that how much network is vulnerable if it uses the WEP static key regardless of the size of IVs, by using the cracking tool aircrack under Backtrack5 environment.
- Second lab implemented the WPA and WPA2 pre-shared key; this lab showed that the dictionary attack and showed that how network is unsecure if it uses the common phrase key. This lab successfully cracked the 8-63 character long key.
- From all the experiments, we came to conclude that WEP and WPA are unsecure for WLAN. Even WPA2 with PSK is also crackable using dictionary attacks with a large number of wordlists. But if WPA2 is implemented with AES algorithm then it is very difficult to crack the key or we can say it is almost impossible to crack the key. So from all the available protocols WPA2 with AES is proved to be the best for WLAN security.

6.2 Scope of future work

- We can make our WLAN security much stronger by using larger passphrases and key words.
- We can implement the WPA2 using AES, which is much secured than using with TKIP
- We can implement WPA2 using the 802.1x authentication technique and due to port based security it is impossible to crack the key. Although, it is quite tough to secure wireless network due to RF signals on the air but by using the proper security technique these attacks can be minimized.

REFERENCES

[1] White paper, “Deploying WPA and WPA2 in the Enterprise”, Wi-Fi Alliance, March 2005.

[2] White paper,“WLAN Security Today: Wirelessmore secure than wired”, Siemens Enterprise Communications, July 2008.

[3] Ahmed M.Al Naamany et al,“IEEE 802.11 WirelessLAN Security Overview”, Department of Electrical and Computer Engineering, Sultan Qaboos University, Oman, 2006.

[4] Anand R.Prasad et al, “802.11 WLANs and IPnetworking: security, QoS andmobility”, Artech House, 2005.

[5] Andrea Goldsmith. “Wireless Communication” Cambridge University Press, New York, 2005.

[6] Martin Beck et al, “Practical attacks against WEP and WPA”,(pp 9), November 8, 2008.

[7] Benny Bing , “The worldwide wifi technological tre nds and business strategies”,John Wiley & Sons, Hoboken, New Jersey,2003.

[8] Arash Habibi Lashkarietal, “Wired Equivalent Priva cy (WEP) versus Wi-Fi Protected Access (WPA)”, International conference on Signal Processing Systems, Singapur, 2009.

[9] Fluhrer, S., Martin, I., and Shamir, A., “Weaknesses in the key scheduling algorithm of RC4”, Eighth Annual Workshop on Selected Areas in Cryptography.(pp 9), August 2001.

[10] Robert Moskowitz,“Weakness in Passphrase Choice in WPA Interface”, ICSALabs, a division of TruSecure Corp, November 4 2003.

[11] Tim Newsham, “Cracking WEP Keys Applying kno wn techniques to WEP Keys”, http://www.lava.net/ ~newsham/wlan/WEP password cracker.pdf, 2001.

[12] S.Fluhreretal, “Weaknesses inthe Key Scheduling A lgorithm of RC4”, Lecture Notes in Computer Science, 2259:1 –24, 2001.

[13] D. Wagner, “Weak Keys in RC4”, http //www.cs.b erkeley.edu/~daw/my-posts/my-rc4-weak-keys, 1995.

[14] Anand R.Prasad &etal, “802.11 WLANs and IP Networking Security, QoS andMobolity”, Artech house Universal personal communication Series, 2005.

[15] Arinze Nwabude, “Wireless local areanetwork (WL AN): security risk and countermeasures”, Blekinge Institute of Technology, 2008.