Mosul University WLAN Security: Evaluation, Analysis and Improvement

Omar Ahmed Hachum

Faculty Computer Eng. Dept., Engineering College
Mosul University, Iraq
Email: omar_hachum@uomcoe.org

Abstract **In this paper, Mosul University Wireless Local Area Networ (MUWLAN) security will be evaluated. The evaluation was made to test the confidentiality, integrity and availability of the MUWLAN. Addressing these issues will help in ensuring tighter security. After the evaluation, serious security pitfalls were found that can allow any attac er to have access to the MUWLAN and uses their internet service. Based on the obtained results, suggestions for improvement were made to tighten the security of Mosul University wireless local area networ .**

Keyword: *- WLAN security, WEP encryption, PTW attack, Wireshark, MITM attack, SSLStrip attack.*

I. INTRODUCTION

Wireless access is quickly broadening network reach by providing convenient, and inexpensive access in hard-to-wire locations. Users are clamoring for WLAN access, because it allows them to access their network and the Internet from anywhere in the workplace, without having the wire environment. Administrators are attracted to WLAN because they are easier to install, flexible, and less expensive to maintain over the long term. WLAN has already made significant penetration into the education, hospitality, healthcare and financial industries, and continually decreasing equipment prices should help drive adoption in other industries. As with any technology shift, migrating users to WLAN has its chief drawbacks concern. The chief concern is security problems [1].

The term *information security* covers a wide array of activities in an organization. The design goals of a security topology must deal with issues of ***confidentiality***, ***integrity***, ***availability***, and ***accountability***. Addressing these four issues as an initial part of the network design will help to ensure tighter security. It is often to see confidentiality, integrity, and availability referred to as the *CIA* of network security, but the accountability component is equally important, design goals must identify who is responsible for the various aspects of computer security [2].

In this paper, Mosul University Wireless Local Area Network (MUWLAN) will be evaluated to address the CIA network security principles [3][4][5]. Results was deleted or replaced with the symbol $ for security purposes.

II. HARDWARE/SOFTWARE USED IN THE EVALUATION

The equipments used in this evaluation are

1. Omni-directional antenna:
   - Gain: 15dBi.
   - Operating frequency: 2.4GHz.
2. Coaxial cable:
   - Type: LMR 400.
   - Length: 15m.
3. Wireless LAN card:
   - D-Link DWL-G520 High Speed PCI Adapter (rev B).
   - 802.11b/g compatible.
4. Workstation with a linux-backtrack3 operating system (Linux version 2.6.21.5, gcc version 4.1.2) installed in it.

Softwares that will be mentioned later in this paper can be found pre installed in the operating system except for *SSLStrip* software.

III. EVALUATION PROCEDURE

This section will explain the main steps that have been used to evaluate MUWLAN security.

A. Identifying Network SSID

The Service Set Identifier (SSID), also known as the wireless network name, identifies the wireless network. The SSID is a name configured on the wireless Access Point (AP) (for infrastructure mode) or an initial wireless client (for ad hoc mode) that identifies the wireless network. The SSID is periodically advertised by the wireless AP or the initial wireless client using a special 802.11 MAC management frame known as a *beacon* frame. One way to limit the visibility of a wireless network is to hide the SSID. Without knowing the SSID, client cannot send the association request frame to gain access to the WLAN [2].

The first main step was to capture and reveal all the network's SSID transmitted through the air. Since the management frames used in the 802.11 has no means of security, the attacker can easily gain useful information about the WLAN. The SSID will be unhided simply by analyzing 5 subtype frames of the main management frame as shown in Table 1.

TABLE 1
The Frame Body contents of a management frame depends on the frame subtype. [6].

Frame Body Contents	Association Request	Association Response	Reassociation Request	Reassociation Response	Probe Response	Probe Request	Beacon	Disassociation	Authentication	Deauthentication
Authentication Algorithm Number									X	
Authentication Transaction Sequence Number									X	
Beacon Interval					X		X			
Current IP Address			X							
Listen Interval	X		X							
Reason Code								X		X
Association ID (AID)		X		X						
Status Code		X		X					X	
Timestamp					X		X			
Service Set Identity (SSID)	X		X		X	X	X			
Supported Rates	X	X	X	X	X	X	X			
FH Parameter Set					X		X			
DS Parameter Set					X		X			
CF Parameter Set					X		X			
Capability Information	X	X	X	X	X		X			
Traffic Indication Map (TIM)							X			
IBSS Parameter Set					X		X			
Challenge Text									X	

The WLAN card will capture all the frames in the air when it is operating in the monitor mode. The captured frames will be huge due to the fact the there are many wireless network broadcasting in Mosul City. Wireshark software [7], which will be pre installed under the operating system, will be used to capture and filter the wireless traffic. The following filter will be used to instruct the wireshark to filter (i.e keep) frames contains subtypes number 0,2,4,5 and 8 (see Table 1).

wlan.fc.type_subtype == 0_00
wlan.fc.type_subtype == 0_02
wlan.fc.type_subtype == 0_04
wlan.fc.type_subtype == 0_05
wlan.fc.type_subtype == 0_08 **(1)**

The wireshark will be used to capture all the frames in the airwave channels ranging from (1~13). After a while, all the SSIDs in the range of the omni-directional antenna were revealed. After reviewing all the SSID names. Table 2 summarizes all the APs with the SSID's including the phrase Mosul University.

Upon identifying more than one AP that belongs to the MUWLAN, one AP will be selected to penetrate MUWLAN. The AP with the following SSID *M0SuLUniversiTy$$$$$* will be selected. To find if this AP uses any mean of data encryption. The data frames sent and received by this AP will be captured by applying the following filter to the captured data.

wlan.bssid == 00:60:b3: : : **(2)**

TABLE 2
SSID's containing the phrase Mosul University was captured in the range of the testing omni-directional antenna.

SSID	MAC address
M0SUIUniVersiTy$$$$$	00:60:B3:$$:$$:$$
M0SUI0FUNlVeri$$$$$	00:60:B3:$$:$$:$$
M0SUIUNlVerSlT$$$$$	00:60:B3:$$:$$:$$
M0SuLUniversiT$$$$$	00:60:B3:$$:$$:$$
M0SUIUNlVersiT$$$$$	00:60:B3:$$:$$:$$

In the captured data, the protected flag data was set to 1 so the data was WEP encrypted. The index key that was used to encrypt the data was key number 2 (starting from 0) as shown in Figure 1.

Figure 1 : Management frame captured using wireshark software showing wireless data is protect and the key number used to encrypt data.

B. Cracking WEP

The IEEE 802.11 standard defines the Wired Equivalent Privacy (WEP), encapsulation of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network.

Encryption in WEP uses a secret key, k, shared between an access point and a mobile node. To compute a WEP frame, the plaintext frame data, M, is first concatenated with its checksum *c(M)*, to produce $M \bullet c(M)$ (where • denotes concatenation). Then, a per packet initialization vector (IV) is prepended to the secret key, k, to create the packet key, $IV \bullet k$. The RC4 stream cipher is then initialized using this packet key, and the output bytes of the cipher are exclusive-ored (denoted $\oplus$) with the checksummed plaintext to generate the ciphertext [8]:

$$\mathbf{C = (M \bullet c(M)) \oplus RC4(IV \bullet \ )}$$

The extension of Klein's attack which is optimized for usage against WEP [9], also known as *PTW* attack (*PTW* stands for the initial letters from the names of this attack creators, Andrei **P**yshkin Erik **T**ews , Ralf-Philipp **W**einmann ,) was used on MUWLAN and that attack can be easily done by using aircrack-ng software on enough

captured encrypted data packets. After capturing enough data and applying *PTW* attack, WEP key for the SSID *M0SuLUniversiTy$$$$$* used by the MUWLAN AP is found and as shown in Figure 2.

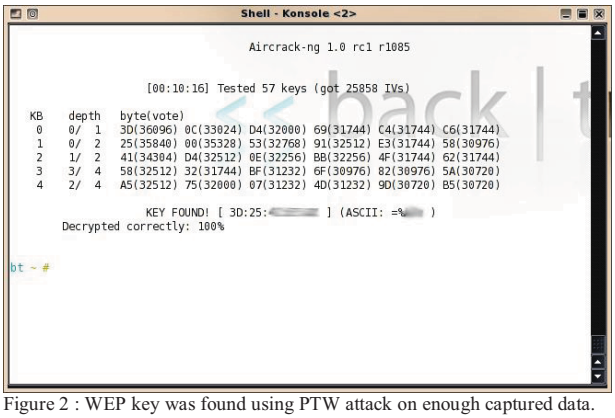

Figure 2 : WEP key was found using PTW attack on enough captured data.

Now all the capture data traffic from *M0SuLUniversiTy$$$$$* can be decrypted using the WEP key. The idea now is to consume the identity of a MUWLAN client and enters the MUWLAN when the client is offline.

IV. WLAN PACKETS ANALYSIS

After the WEP key was found, the attacker can now analyze all the traffic (data) between the wireless clients and the AP. To have the right to use the services provided by the MUWLAN, such as the internet service, the configuration of the MUWLAN wireless client must be known and they are:

- IP and MAC address.
- Subnet mask.
- IP address of the gateway.
- IP address of the DNS server.

The easiest way to find these parameters is to search for DHCP packets replies or offers in the captured data. So the following filter will be applied to the captured data:

wlan.bssid == 00:60:b3: : : && bootp.type == 2 (3)

Unfortunately for the attacker, no DHCP replies or offers packed was captured.

A. IP and MAC address.

The IP address of the wireless client can be easily found by applying the following filter on the wireless traffic (data) of the MUWLAN.

wlan.bssid == 00:60:b3: : : && ip (4)

The majority of IPs found in the captured data was class B privet IP address. So, it's a matter of time, when these clients are offline, the attacker can consume any IP address and access the network. Also from the same packet, the wireless client MAC address can be found as shown in Figure 3.

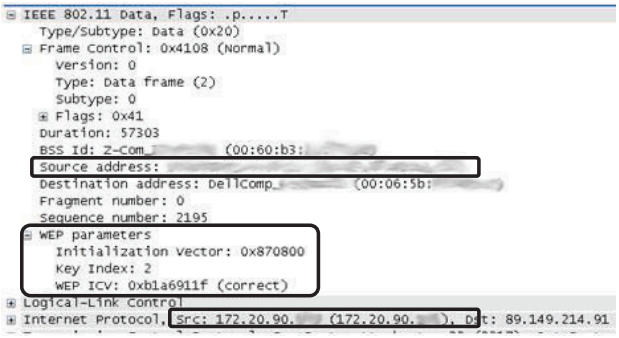

Figure 3 : The WLAN IP address and MAC address of one MUWLAN client.

B. Network subnet mask

Since there is no DHCP server, finding subnet mask will be tricky. The following filter will be applied to the wireless traffic to capture only the broadcast traffic (destination MAC address equals all 1's) on the network.

wlan.bssid == 00:60:b3: : : &&
wlan.da == ff:ff:ff:ff:ff:ff &&
ip.dst = 172.20.0.1 &&
ip.dst = 172.20.255.255 (5)

This can be accomplished by checking the destination IP address of that broadcast packets as shown in Figure 4.

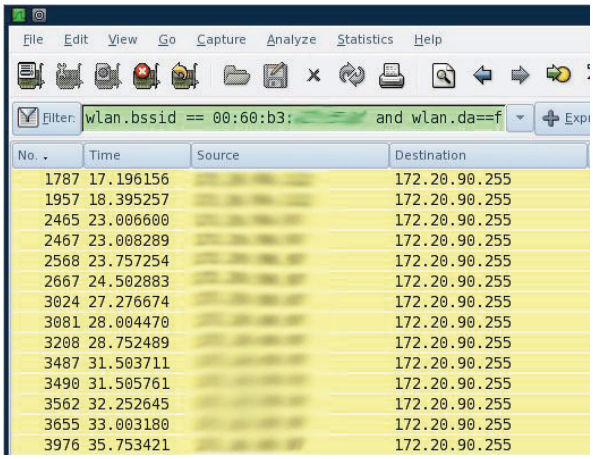

Figure 4 : The broadcast IP address obtained after filtering the captured data.

The majority destination IPs was 172.20.90.255, thus it is obvious that the subnet mask must be 255.255.255.0

C. IP address of the gateway

By checking the MAC addresses (Destination and Source) of the wireless traffic, it is easy to find the gateway MAC address, because that MAC address will be the dominating one. Since all the traffic must be sent to the gateway to access the internet, clients want to access the

Internet will have to pass through the gateway. Therefore the same MAC address will be fixed in all the packets while a verity of destination IP or source IP addresses that will not falls into the 172.20.90.0 will belong to the same MAC address. To find the IP address that belong to that MAC address, all the packets that have the gateway MAC address as a destination and its IP address will fall into class B network address also a destination will be filtered using the following filter.

wlan.bssid == 00:60:b3: : : &&
wlan.da == 00:06:5b: : : &&
ip.dst =172.20.90.1 &&
ip.dst =172.20.90.254 **(6)**

After filtering the captured data as shown in Figure 5, the IP gateway is identified as 172.20.90.2.

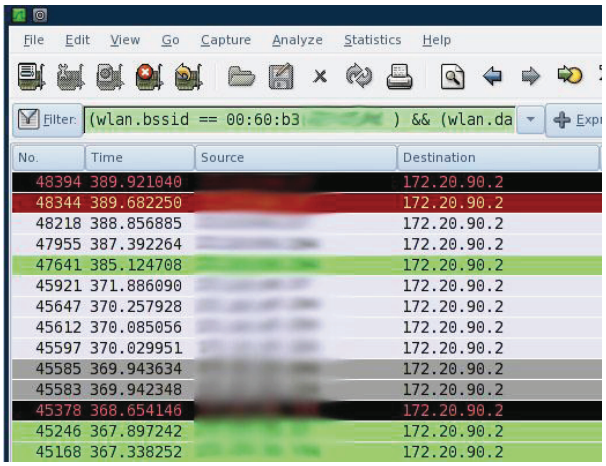

Figure 5 : The IP address of the gateway obtained after filtering the captured data.

D. IP address of the DNS server

Finding the IP address of the DNS server will not be a hard task, because when a client want to visit any website using webpage Uniform Resource Location (URL), internet browser must know the IP address that belongs to the given URL. This can be done by using DNS server. Capturing any response from a DNS server to a client can recover the DNS server IP address. The following filter was used to capture such a response.

wlan.bssid == 00:60:b3: : : &&
ip.dst =172.20.90.1 &&
ip.dst 172.20.90.254 &&
dns.response to **(7)**

For MUWLAN, The IP address of the DNS server is the same IP address of the gateway which is 172.20.90.2 as shown in Figure 6.

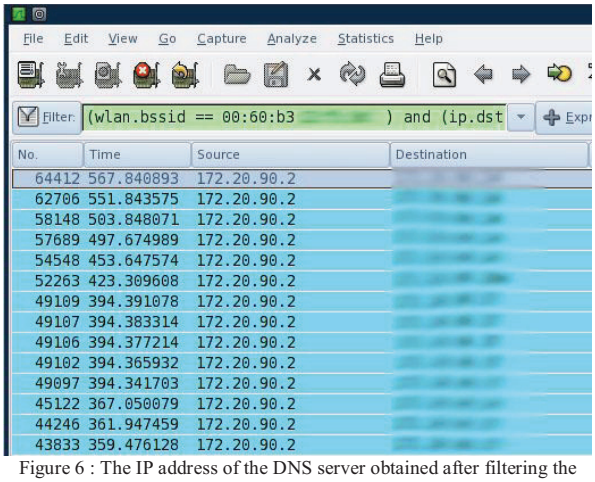

Figure 6 : The IP address of the DNS server obtained after filtering the captured data.

V. BYPASSING THE 24 ONLINE SOFTWARE.

Mosul University uses 24 online software from Elitecore Technologies Limited for billing and bandwidth management. For authenticating, the user to access the internet, it uses web-based logging on technique that asks the client to enter user name and password in order to access the internet. Any request to access the internet using MUWLAN will show up a web page asking the user to enter his/her user name only once to authenticate.

By viewing the source code of the client logging webpage, no means of security was found. Therefore, the user name and the password will be sent as a plain text. It is easy to catch the user name and password if the attacker lies between the wireless the client and the wireless AP of MUWLAN. Since the gateway is also the 24 online server, the following filter will capture all the user names and passwords that will be sent to the gateway using http protocol only as shown in Figure 7.

wlan.bssid == 00:60:b3: : : &&
ip.dst==172.20.90.2 &&
http contains Pass **(8)**

Now it's easy for the attacker to access MUWLAN and uses the internet service. Also it is easy for the attacker to change the password of the client perverting the real client from accessing the internet.

Also, by viewing the administration logging web page, it shows no means of security. Therefore, if the attacker lies between the administration's PC and AP of the Mosul University, it will be a matter of time till the administration access the 24 online server wirelessly and then the attacker can have both the user name and the password of the 24 online server.

```
Hypertext Transfer Protocol
  GET /24online/webpages/liverequest.jsp?isfirsttime=false
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjp
    Accept-Language: en-us\r\n
    UA-CPU: x86\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
    Host: 172.20.90.2\r\n
    Connection: Keep-Alive\r\n
    Cookie: _Pass=[illegible]; _UserName=[illegible]; _SaveInfo=saveinfo
    \r\n
```

Figure 7 : Captured user name and password sent from client to the MUWLAN AP.

VI. APPLYING MAN IN THE MIDDLE ATTACK (MIMT)

The attacker now is a ligament user. The following attacks can be used not for a wireless networks only but also can be implemented against wired networks. All the above evaluation measurements used passive attacks only, but the attacker can use an active attack such as MITM attack that will be started using the famous ARP poisoning attack.

ARP allows the network to translate IP addresses into MAC addresses. When one host using TCP/IP on a LAN tries to contact another, it needs the MAC address or hardware address of the host it's trying to reach. It first looks in its ARP cache to see if it already has the MAC address; if it doesn't, it broadcasts an ARP request asking, "Who has the IP address I'm looking for?" If the host that has that IP address hears the ARP query, it responds with its own MAC address, and a conversation can begin using TCP/IP. ARP poisoning is a technique that's used to attack an Ethernet network and that may let an attacker sniff data frames on a switched LAN or stop the traffic altogether.

ARP poisoning utilizes ARP spoofing where the purpose is to send fake, or spoofed, ARP messages to an Ethernet LAN. These frames contain false MAC addresses that confuse network devices such as network switches. As a result, frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or to an unreachable host (a Denial of Service [DoS] attack). ARP spoofing can also be used in a man-in-the-middle attack in which all traffic is forwarded through a host by means of ARP spoofing and analyzed for passwords and other information[10].

Poisoning ARP cache table can be done using *Ettercap* software that is preinstalled in the backtack3 operating system. *Ettercap* can ARP poising the victim's PC only or both the victim's PC and the gateway so that all the traffic between the victim's PC and the gateway will be passed through the attacker's PC.

A. SSLStrip attack.

The main trick of this attack is that people access HTTPs web site through HTTP and HTTP is not secure. Most of the people access Yahoo!, gmail and hotmail by click on hyperlink embedded in html web pages or by typing for example http://www.gmail.com and less of them is using the https://www.gmail.com to access the emails server. In this attack both the gateway and the victim's PC must be ARP cache poisoned and that can be done using *Ettercap* software.

After implementing ARP cache poisoning, all the traffic between the gateway and the victim's PC is now passing through the attacker's PC. The attacker can use *SSLStrip* -0.4 tool[11] which is not installed under the backtrack operating system but can be found free in the internet.

The main job of this tool is to strip every HTTPS link contained in a web page requested by the victim into an HTTP link, When the victim tries to access a web site using HTTPS by typing for example http://www.gmail.com or by click on a hyperlink, the attacker will catch that request and start new HTTPS session between him (the attacker) and gmail as shown in Figure 8.

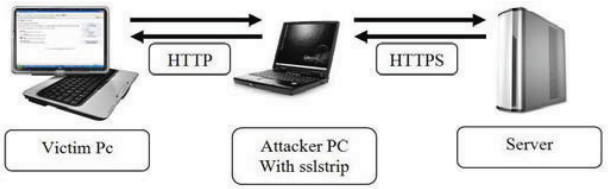

Figure 8 : Attacker will uses stripssl tool between the server and the victim's PC .

Now gmail will send its login web using HTTPS protocol to the attacker. The attacker will send the same web page to victim using HTTP. The difference between the HTTPS gmail login web page and the HTTP gmail login web page is shown in Figures 9 and 10 respectively. The victim will enter his/her user name and password and press the login button and that page will be sent to the attacker in plain text using HTTP. The attacker now can use the received user name and password and login to the HTTPS gmail account. After that, gmail will send the inbox web page to the attacker and in return the attacker will decrypt the inbox web page using the shared key received during the ssl handshaking protocol and redirect that page using HTTP to the victim's PC. Now the victim can browse his/her email without knowing that his/her user name and password is caught by an attacker.

SSLStrip attack was implemented on the MUWLAN against Yahoo! , gmail, and hotmail email accounts and Figure 11 shows the obtained result.

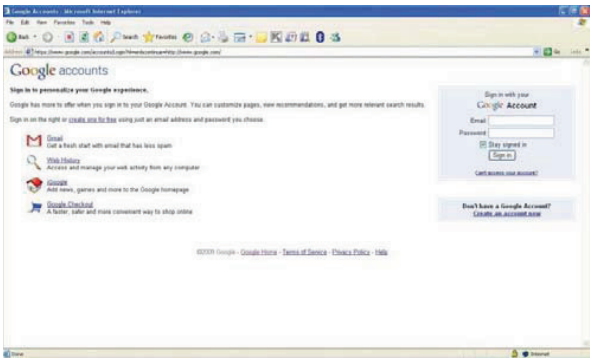

Figure 9: gmail login web page using HTTPS.

Figure 10: gmail login web page using HTTP.

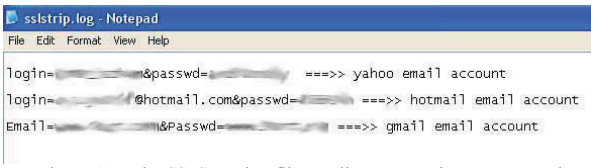

Figure 11 : The *SSLStrip* log file reveling captured user name and password for Yahoo!, gmail and hotmail accounts.

VII. IMPROVING MUWLAN SECURITY

The big question is how to improve the security of the Mosul University wireless network. Let's review the steps led to crack the wireless network and try to solve them one by one.

First: it is good that MUWLAN hides the SSID of their APs but it's a matter of time till a client send some type of frame that leads to unhide them. But the attacker can't tell if those APs are belong to the Mosul university or not if the SSID have a name that not related to Mosul University such as Network1 or any other name without containing the phrase Mosul University or University name in the SSID filed. Because these names will be a hint to the attacker to attack these APs.

Second: changing static WEP is important to the latest wireless encryption suit such as enterprise WPA2.

Third: Secure the login access by using MD5 based login software since the user name and the password of the 24online can be cached with or without using SSL login access.

Four: To stop ARP poising attack, it is good idea that both gateway and client involved in the protection process since attacker can attack only the client, even when there is an ARP poisoning watcher installed at the gateway. At the server side, ArpON software can be installed and it can detect and prevent an ARP poisoning attack. At the client side, static ARP cache table can be implemented easily since the only important IP in the network will be the gateway IP, clients can add static entry to the ARP cache table using the following windows command

arp -s IP address MAC address

Alliteratively, clients can install ArpON software or any other operating system compatible ARP cache protection software.

VIII. CONCLUSIONS

This paper revealed that any attacker can have all the information to access the MUWLAN and to uses their services such as the internet and can change the password of the real clients. The confidentiality issue is also broken since anyone has the WEP key can monitor the wireless client's traffic. Integrity issue is broken too, since that attacker can manipulate the data sent through MUWLAN using *SSLStrip* attack. Availability issue is also broken, since the attacker can change the password of the logging web page making the attacker is the legitimate user and the client is the rogue user so the internet service will be unavailable to the client at the time when the real client wants to access the internet. Based on the obtained results, suggestions for improvement were made to tighten the security of Mosul university wireless local area network.

REFERENCES

[1] Wang Shunman, TaoRan, WangYue, ZhangJi, "***WLAN and its Security Problems*** ", IEEE , Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 241- 244 ,2003.

[2] Emmett Dulaney, "***CompTIA Security+ Study Guide: Exam SY0-201***", Sybex publisher, 4th edition, 2008, ISBN-13: 978-0470372975.

[3] James M. Stewart, Ed Tittel, Mike Chapple, "***CISSP: Certified Information Systems Security Professional Study Guide***", Sybex, 4th edition, 2008, ISBN-13: 978-0470276884.

[4] Susan Snedaker, "***Syngress IT Security Project Management Handbook***", Syngress publisher, 1st edition, 2006, ISBN-13: 978-1597490764.

[5] Mizhael Horton, Clinton Mugge, "***HackNotes(tm) Network Security Portable Reference***", McGraw-Hill Osborne publisher, 1st edition, 2003, ISBN-13: 978-0072227833.

[6] Neeli Prasad, Anand Prasad, "***WLAN Systems & Wireless IP for Next Generation Communications*** ", Artech House publishers, 2002, ISBN-13: 978-1580532907

[7] Angela Orebaugh, Gilbert Ramirez, Jay Beale, Joshua Wright, "***Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide***", Syngress publisher, 2007, ISBN-13: 978-1597490733.

[8] Adam Stubblefield, John Ioannidis, Aviel D. Rubin, "***Using the Fluhrer, Mantin, and Shamir Attack to Break WEP***", AT&T Labs Technical Report TD-4ZCPZZ , 2001.

[9] Erik Tews , Ralf-Philipp Weinmann , Andrei Pyshkin, "***Breaking 104 Bit WEP in Less Than 60 Seconds***", Springer, Vol. 4867/20082,2008.

[10]Kimberly Graves, "***CEH Official Certified Ethical Hacker Review Guide***", Wiley publishing, Inc, 2007, ISBN-13: 978-0782144376.

[11]Moxie Marlinspike, "***New Tricks For Defeating SSL In Practice***", Black Hat conference,USA-DC,2009.