Lab 5 Wireless Security

April 14, 2011

Contents

1 Introduction

1.1 Description of the test bed

Shown in fig.1 and fig.2, one wireless testbed is divided into two sections, wired and wireless. The wired network consists of two hubs, four computers and two access points. The PC router is named STREETCAR in testbed A or CABARET in testbed B. On either side of the router, there is one VLAN, totally 2 VLANs. The computer router acts as a connector as well as a gateway for the computers on either side of each VLAN. In each VLAN, one of the computers is playing the role of gateway or router to forward the packets between wired and wireless networks. WESTSIDE and DREAMCOAT in testbed A, SAIGON and RENT in testbed B are all connected to a wireless access point, which then acts as a connector to the wireless devices, iPAQs. The infrastructures of testbed A and B are illustrated in figure 1 and figure 2.

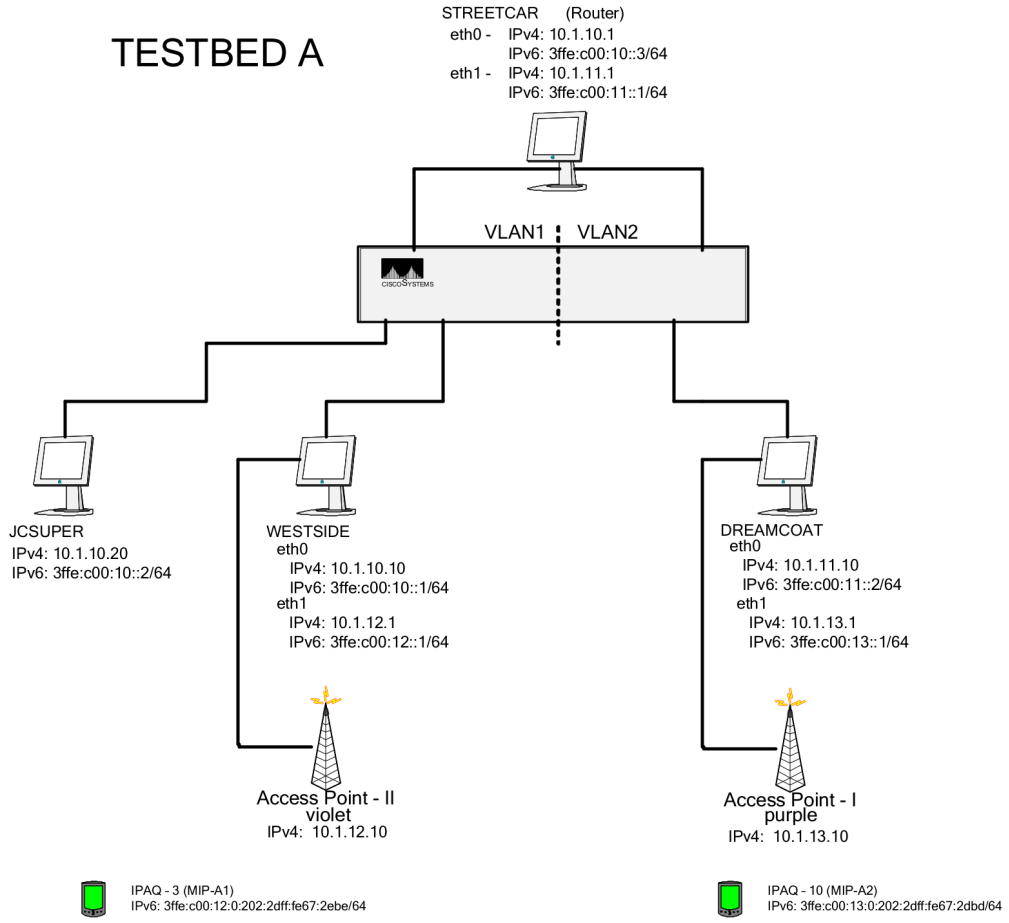

Figure 1: Infrastructure of Wireless Testbed A

1.2 Wireless Security: WEP Protocol

Wired Equivalent Privacy(WEP) is an IEEE standard security protocol for wireless 802.11 networks. Introduced in 1997, WEP was found to be very inadequate and was

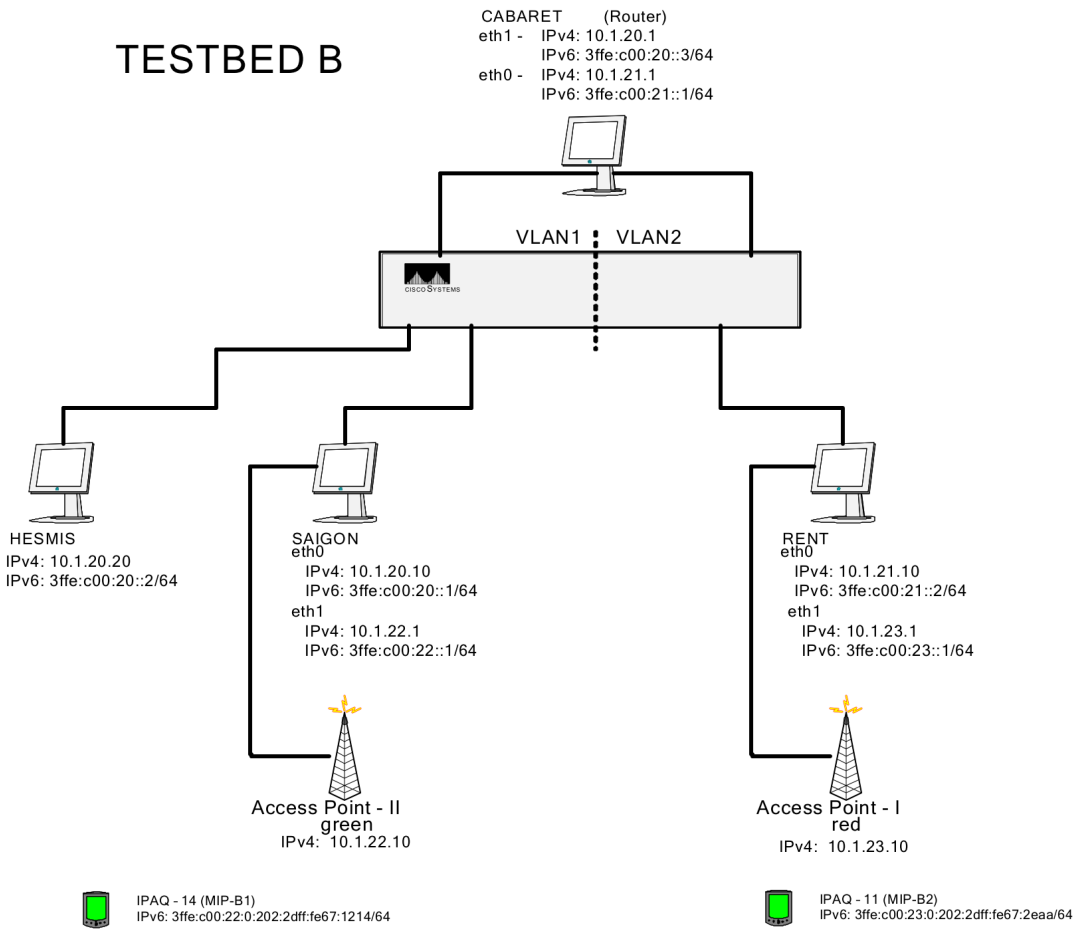

Figure 2: Infrastructure of Wireless Testbed B

superseded by WPA, WPA2 and 802.11i. Its authentication method was extremely weak and even helped an attacker decipher the secret encryption key. As a result, WEP authentication was dropped from the Wi-Fi specification.

WEP uses passwords that are entered manually at both ends. Using the RC4 encryption algorithm, WEP originally specified a 40-bit key, but was later boosted to 104 bits. Combined with a 24-bit initialization vector, WEP is often touted as having a 128-bit key. See WPA, 802.11i and initialization vector.

Purpose: The aim of this exercise is to provide practical experience on Wired Equivalent Privacy (WEP) protocol and its configurations. We will also analyze the impact of the protocol on response time, when the mobile node is in its home and foreign network.

1.3 Simplification for lab5

The above testbeds require a total number of 16 desktops for this single lab. However, this number of desktops are not available. We could simplify lab5 to get the same purpose using less desktops.

We could simplly use the testbed for lab4 and using WEP to secure it.

The addresses we are using in our test-bed are global. Our test-bed consist of four nodes, see figure 3.

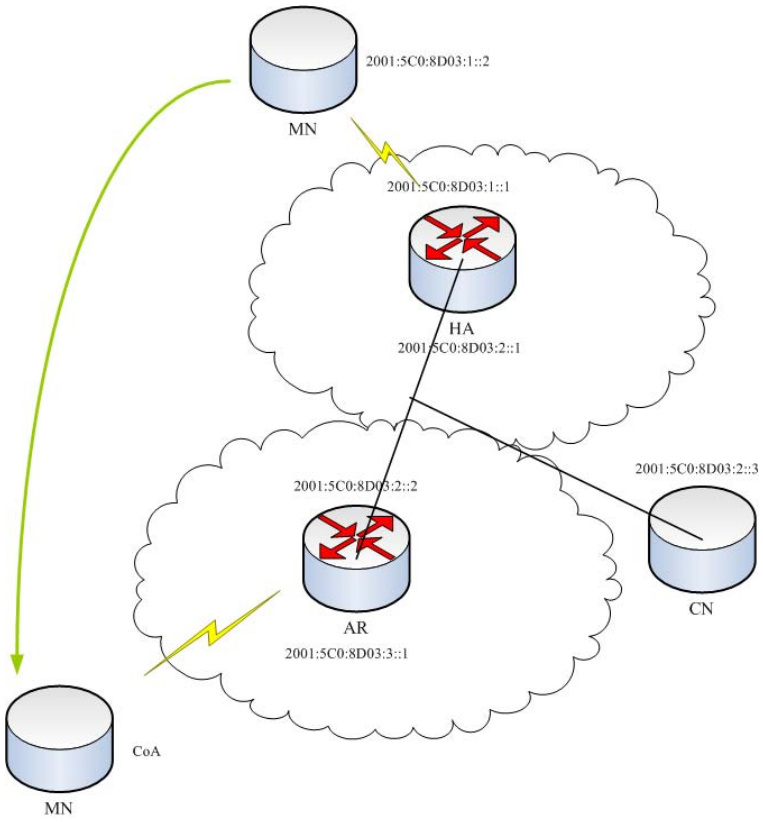

Figure 3: Mobile IPv6 testbed

2 Get prepared

First, we set up our testbed as lab4 indicates. We also use mobile ipv6 protocol to set up MN, HA, CN, AR nodes.

- The Mobile Node(MN) travels to a foreign network and gets a new care-of-address.
- The MN performs a binding update to its Home Agent (HA) (the new care-of-address gets registered at HA). HA sends a binding acknowledgement to MN.
- A Corresponding Node(CN) wants to contact the MN. The HA intercepts packets destined to the MN.
- The HA then tunnels all packets to the MN from the CN using MN's care-of-address.
- When the MN answers the CN, it may use its current care-of-address(and perform a binding to the CN) and communicate with the CN directly (route optimization) or it can tunnel all its packets through the HA.

Configure those nodes and start radvd and mip6d on specific nodes. Make sure they could reach the other nodes.

```
$ ping6 <the ipv6 address>
```

3 The Exercise

After the testbed has been set up, you could make some changes to get lab5 done.

Step 1: Start "pinging" on MN to home agent(HA) of your testbed. On the HA desktop, start wireshark to capture ping packets as follows:

```
$ sudo wireshark
```

The wireshark window would be as figure 4. Observe ping packets in wireshark window.

Step 2: Then, we configure WEP on our homenet. On HA desktop, type the following command:

```
$ iwconfig wlan0 key 1234567890
```

Observe ping packets in wireshark window.

Step 3: Type following command on MN to set encryption key for WEP.

```
$ iwconfig wlan0 enc 1234567890
```

Observe ping response.

Step 4: Stop all ping action. Type the command on MN

```
$ iwconfig wlan0 essid visitnet_groupX channel 3
```

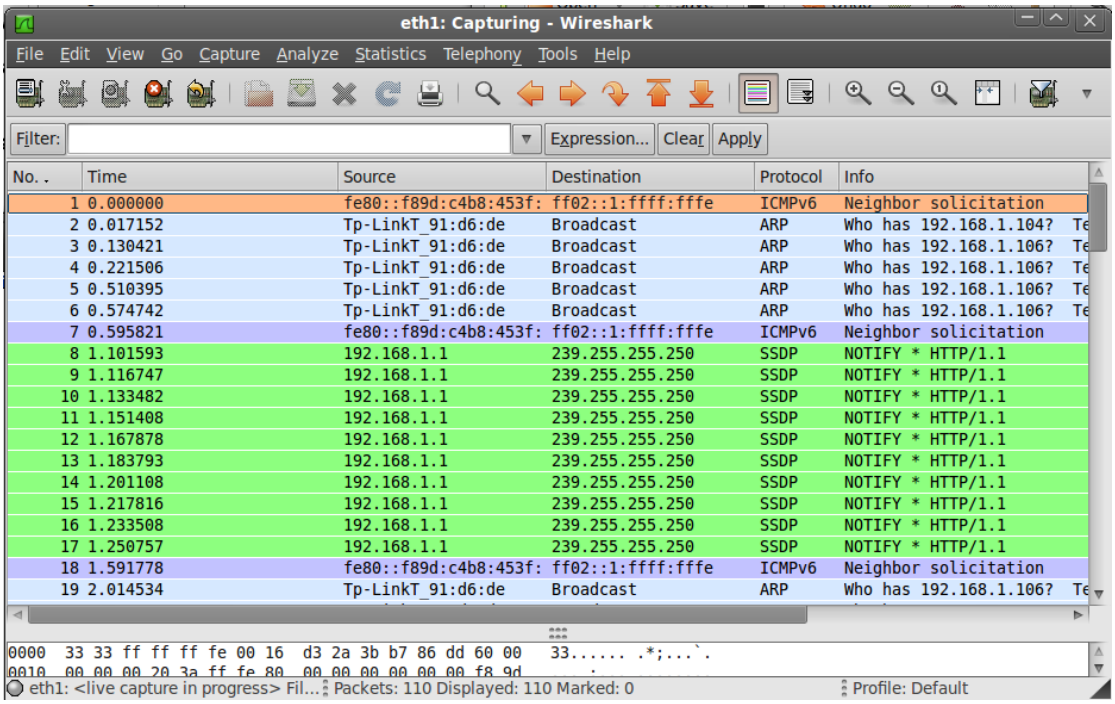

Figure 4: Wireshark Window

Now the MN has roamed to the foreign network visitnet.

Step 5: Start Ping again on MN to correspondent node. Observe ping response.

Step 6: Type following command on MN to turn off encryption key for WEP:

```
$ iwconfig wlan0 enc off
```

Then do step(4) again. Observe ping response.

4 Questions

1. Based on the knowledge gained during configuration of Access point (step 2), list down different authentication mechanisms supported by WEP. (Hint: use man command could help.)

2. After execution of step 2, does MN receive PING response from home agent? If yes, why? If not, why not?

3. After execution of step 3, does MN receive PING response from home agent? If yes, why? If not, why not?

4. Explain encryption mechanism used in WEP and also list down different key sizes supported by WEP.

5. Analyze the packets captured in ethereal and explain with reasoning the difference in response time when WEP is enabled.

6. When mobile node roams in step 4, does MN receive ping response after step 5? If yes, why? If not, why not?

7. After execution of step 6, does MN receive PING response? If yes, why? If not, why not?

8. During communication between MN and home agent, is complete path from MN to home agent encrypted? If yes, provide reasoning. If not, explain which part of the path is not encrypted and why?

A Wireshark installation

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues.

For lots of softwares in Linux, you could use apt-get to auto install in your desktop. Wireshark is one of them.

```
$ sudo apt-get install wireshark
```

You could go to its official website to get details information:
`http://www.wireshark.org/`