Case of Study: Identity Theft in a University WLAN, Evil Twin and Cloned Authentication Web Interface

Jose Maria Briones, Mario Alejandro Coronel, Patricia Chavez-Burbano
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Guayaquil, Ecuador
jose080988@hotmail.com, macoronel@cti.espol.edu.ec, pchavez@fiec.espol.edu.ec

ABSTRACT: *This paper is about the insecurity of the Wireless LAN of a university that is supposed to be available only for students and teachers through a username and a password. This attack shows how to deceive a user making him think he is connecting to a real access point and entering his information in the real web interface that the university provides for user authentication. We create a fake access point using the same name of the university's WLAN to capture login credentials using a fake authentication web interface and then use this information for identity theft. After the demonstration we present possible solutions and recommendations to be aware and avoid this kind of attacks that are a high risk for the security of students and teachers.*

Keywords: Wireless, Identity Theft, Evil Tween

Received: 10 March 2013, Revised 19 April 2013, Accepted 24 April 2013

1. Introduction

Nowadays the wireless communications are implemented in most organizations around the world. It has become a need due to the lot of mobile users using laptops or smart phones and the ease of connection from every part of the covered area. The benefits increase when we talk about universities where large amount of students need to access to the internet and computer labs are not available in that moment. The disadvantage of wireless communication is the high risk of receiving attacks since the radio waves can be intercepted by someone who is not a legitimate user.

The "*victim university*" has a WLAN implementation for the purposes described above along with an authentication web interface which is working with a RADIUS server. We will create a fake access point with the same name as the ones used by this university and clone the authentication web interface to deceive the users and capture their credentials.

2. Materials and Methodology

The table 1 shows the materials we need to perform the attack. Take into account that the wireless network interface card must support the operation in monitor mode. Also, the operating system used for this practice is Backtrack 5 R3. In this release of Backtrack there are included tools that we use in this study such as Aircrack-ng Suite, Social Engineering Toolkit, DHCP and DNS server.

Device	Type
Laptop	Hardware
Wireless interface network card	Hardware
Backtrack 5 R3 OS	Software

Table 1. Materials

The methodology for this work is based on the wireless connection concepts of the standard IEEE 802.11 through a type of attack called Evil Twin, and a social engineering computer based technique called Phishing [6]. These both utilities together allow us to launch an attack to the WLAN in order to obtain valid credentials from a typical user.

3. Current Situation

When the user wants to connect to the wireless network of the university they have to look for the appropriated access. These access points use WPA-EAP security method to authenticate the user. So when the user connects to this wireless network and try to access to any website, he is redirected to an authentication web interface to log in with his username and password. Once done, the user has total access to the internet. This username and password are the same for university's email account access.

4. Evil Twin and Phishing Attack

To connect to the wireless LAN, the users have to authenticate in one of the access points located in the university. These APs are distributed around the campus of the university to cover most of the area. When a user wants to connect, his wireless network card automatically detects the most powerful signal in the air from all the APs with the same name, ignoring the rest. If we set up an AP with the same name, and a very strong signal that exceeds the other ones, this access point will be visible for the user, and when he tries to connect, he will do it to our AP. This fake AP is called rogue access point and is used for evil twin attacks. [1], [2]

Let's do the attack from the side of a malicious user that wants to collect some credentials. In Backtrack 5 R3 there are many tools that can scan the radio waves of access points in the air. One of these is called Aircrack-ng Suite. This tool is able to capture raw 802.11 frames around the place, inject traffic to the APs, deauthenticate associated users, crack WEP and WPAPSK passwords, create rogue access points, et al. [3]

Using this analyzer tool we can identify the name of the ESSID, the channel of operation, the power of the signal, the type of authentication and cipher it is using, the amount of data that is handling, the connected users, and so on. Aircrack-ng provides us a lot of information that we can use to perform an evil twin attack. This is a free tool that is available for both Linux and Windows. [3]

To use this tool, we needed a wireless network interface card that is able to operate on listening mode so it can capture all the packets in the air without the need of being associated to any access point.

According to the documents of the standard IEEE 802.11, a wireless network interface card can operate in four modes: (1) Master which acts as an access point and all the clients connect to it. (2) Managed which acts as a client. (3) Ad-hoc which is used for connections multipoint-to-multipoint and (4) Monitor which listens to all radio traffic on a specific channel. [4]

With Aircrack-ng Suite we created an interface operating in monitor mode from our wireless network interface card. This is the first step in order to create a fake access point to perform the attack. We did it using the command

$$airmon\text{-}ng\ start\ wlan0, \tag{1}$$

where wlan0 is the name of our current wireless network card. This command created a new interface in monitor mode called mon0 (See Figure 1).

We checked the new interface with the command *ifconfig* that shows general information of all interfaces in the system. We could see that the interface didn't have an IP address and network mask. (See figure 2)

```
TESIS tests # airmon-ng start wlan0

Found 5 processes that could cause trouble.
If airodump-ng, aireply-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
1156    avahi-daemon
1157    avahi-daemon
1191    NetworkManager
1209    wpa_suppicant
28994   dhclient
process with PID 28994 (dhclients) is running on interface wllan0

interface    Chipset       Driver

wlan0        Atheros       ath9k - [phy0]
                           (monitor mode enabled on mon0)
```

Figure 1. Creating interface in monitor mode

```
mon0  Link encap:UNSPEC HWaddr 00-25-D3-F4-3A-36-30-30-00-00-00-00-00-00
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:445 errors:0 dropped:0 overruns:0 frames:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:103336 (103.3 KB) TX bytes:0 (0.0.B)

waln0  Link encap:Ethernet HWaddr 00:25:d3:f4:3a:36
          inet addr:200:126:24.182  Bcast:200.126.27.255 Mask:255.255.252.0
          inet6 addr:fe80::225:d3ff:fef4:3a36/64 Scope:Link
        UP BROADCAST RUNNING MTU:1500 Metric:1
         RX packets:16527 errors:0 dropped:0 overruns:0 frames:0
         TX packets:15898 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0  txqueuelen:1000
         RX bytes:13398295 (13.3 MB) TX bytes:2318970 (2.3.B)
```

Figure 2. Information about interface mon0

Through the monitor mode interface, we scanned the access points available in the place. For this we executed the command

*airodump-ng mon*0. (2)

In few seconds the command showed all the actives access points around the place (See figure 3). We could see many access points with the ESSID name and information about authentication method, channel, MAC address and signal power.

We found that there were five access points with the appropriated ESSID. With wireless standard tools, in Windows for example, only appears once that network. With this program we can see all the access points with that name and identify if data is being sent to the clients. The closest AP has a power of -57 dBm in channel 1, and -91 dBm the farthest one in channel 11. We see that there are some APs which operate in channel 1 and others in channel 11 of the frequency spectrum. This difference channel is intended to avoid interference between access points. [5]

Once we identified the ESSID for the evil twin attack, we configured a DHCP server to provide IP addresses when the users connect to our access point. In this case we use the server called dhcp3. The configuration file is /etc/dhcp3/dhcpd.conf.

Then we configured a DNS server to redirect the user to our local server where we had the cloned web interface. For this purpose

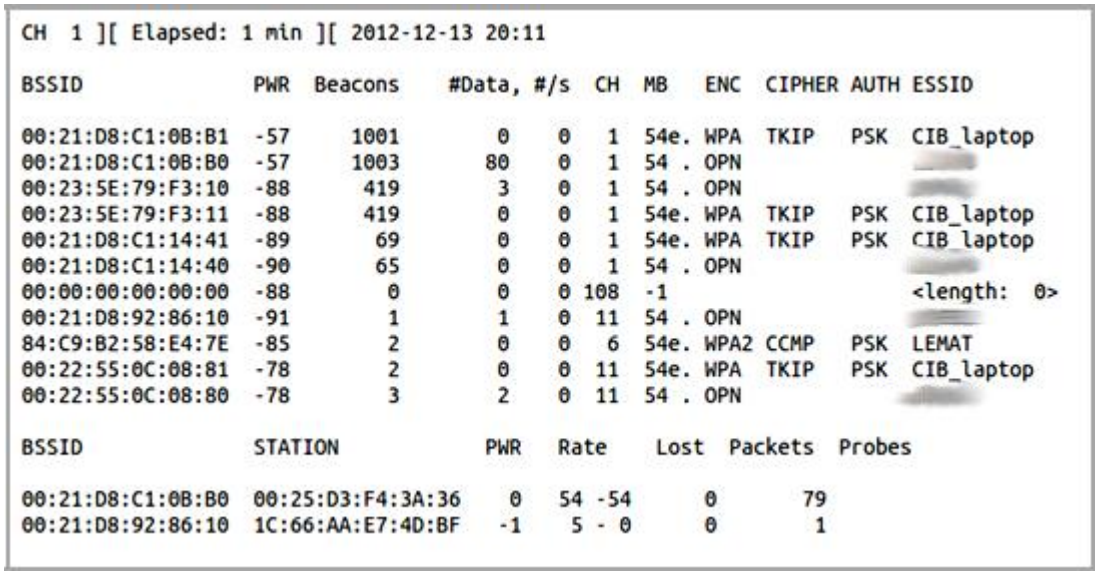

Figure 3. Scanning APs

we use the dnsmasq utility. In the configuration file/etc/dnsmasq.conf we entered the lines

$$interface = at0 \quad (3)$$

$$address=/\#/ 192.168.20.1 \quad (4)$$

In the first line, *at0* is the name of the fake access point. The second configuration line means that all HTTP requests whatever they are, go directly to the IP address 192.168.20.1 which is the IP of our fake access point and consequently the address of the cloned web interface.

After restarting the DNS server with */etc/init.d/dnsmasq restart*, we proceeded to create the evil twin access point using the same name of the "*victim*" and channel 11. We used channel 11 to avoid interference with the nearest AP that is operating in channel 1.

$$\text{airbase-ng -e victim -c 11 -v mon0 \&} \quad (5)$$

Then we enabled the network interface and we assigned it an IP address a network mask and a default gateway address.

$$ifconfig\ at0\ up \quad (6)$$

$$ifconfig\ at0\ 192.168.20.1\ netmask\ 255.255.255.0 \quad (7)$$

$$route\ add\text{-}net\ 192.168.20.0\ netmask\ 255.255.255.0\ gw\ 192.168.20.1 \quad (8)$$

If we want the victim to have internet access through our AP, we have to enable the packets forwarding between the interface of the AP and our internet connection and activate the NAT translation.

$$echo\ "1" > /proc/sys/net/ipv4/ip\_forward \quad (9)$$

$$iptables\text{-}t\ nat\text{-}A\ POSTROUTING\text{-}o\ wlan0\text{-}j\ MASQUERADE \quad (10)$$

Then we created a symbolic link to the DHCP service process to avoid errors when starting the service, and started the server on the access point interface.

$$ln\text{-}s/var/run/dhcp3\text{-}server/dhcpd.pid\ /var/run/dhcpd.pid \quad (11)$$

$$dhcpd3\text{-}d\text{-}f\text{-}cf\ /etc/dhcp3/dhcpd.conf\ at0\ \& \quad (12)$$

Once done, the fake access point was running and sending beacons to the users. This is the way how to create a rogue access point. Now we had to clone the web interface to deceive users when they connect to the access point. For this we used a tool called SET (Social Engineering Toolkit). This tool has many options and one of those is to clone websites.

We started the application and followed the steps shown by the same tool to clone a website, leading to an interface as shown in Figure 4.

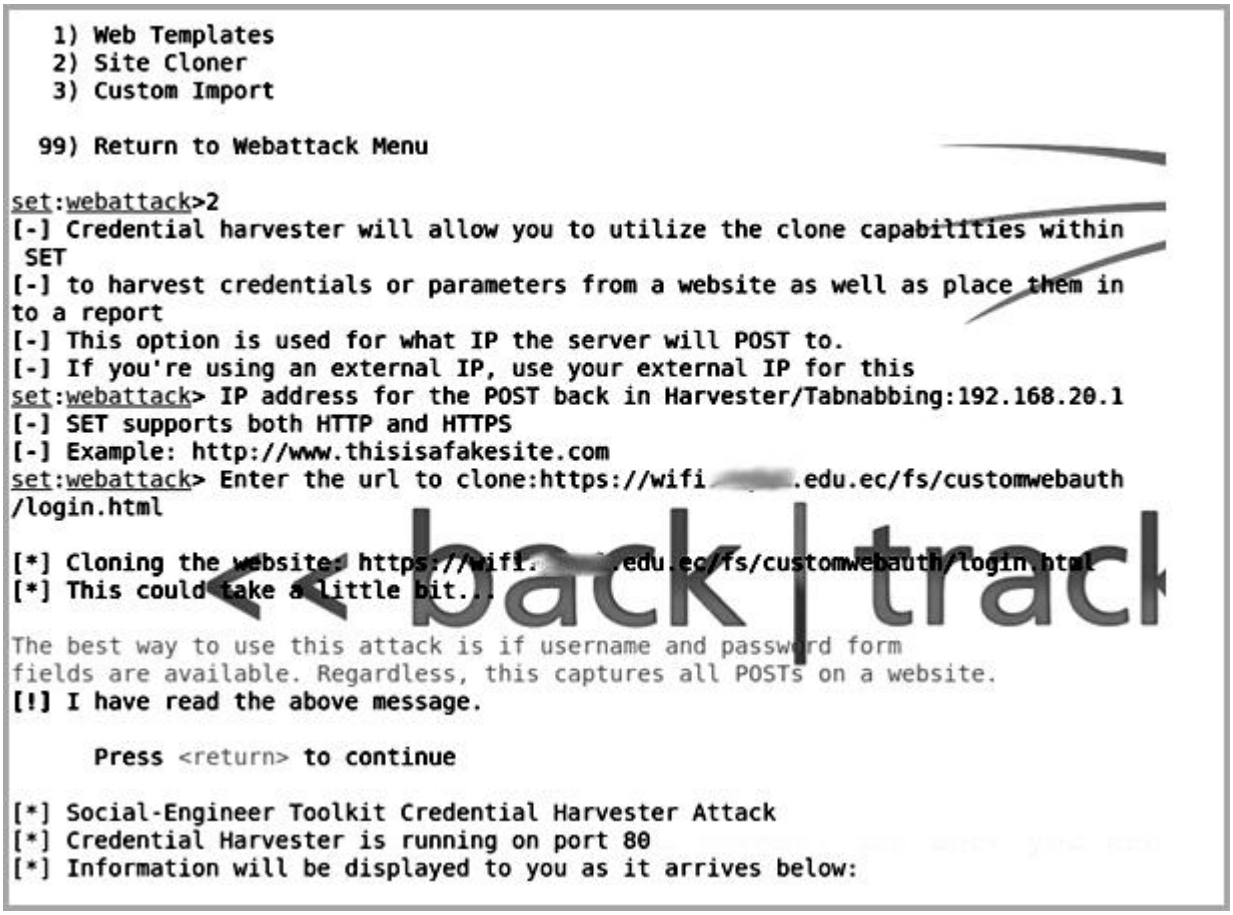

Figure 4. SET interface

We had to specify the IP address of the fake web server and the URL of the website we wanted to clone. After that, SET was waiting for a user to fill out the user and password information and click on Sign In button. The cloned page is shown in Figure 5.

It was only a matter of time for someone to connect to our fake AP and enter the credentials in the website. When this happened, SET captured the username and password and it was displayed in its interface. The Figure 6 shows one of the users that entered login information and clicked on Sign In button.

5. Analisys of the Attack

In the first part of the attack we used a fake access point to deceive the user. The user connected to our access point because the radio signal power was stronger than the others. This was possible because we were located in a crowded place where people probably would try to connect to the wireless network. This attack is based on the concept that the network cards that act as client (Managed mode) detect the best signal power of all access points with the same ESSID.

Through the social engineering computer based we could deceive the user making him think the authentication web interface to

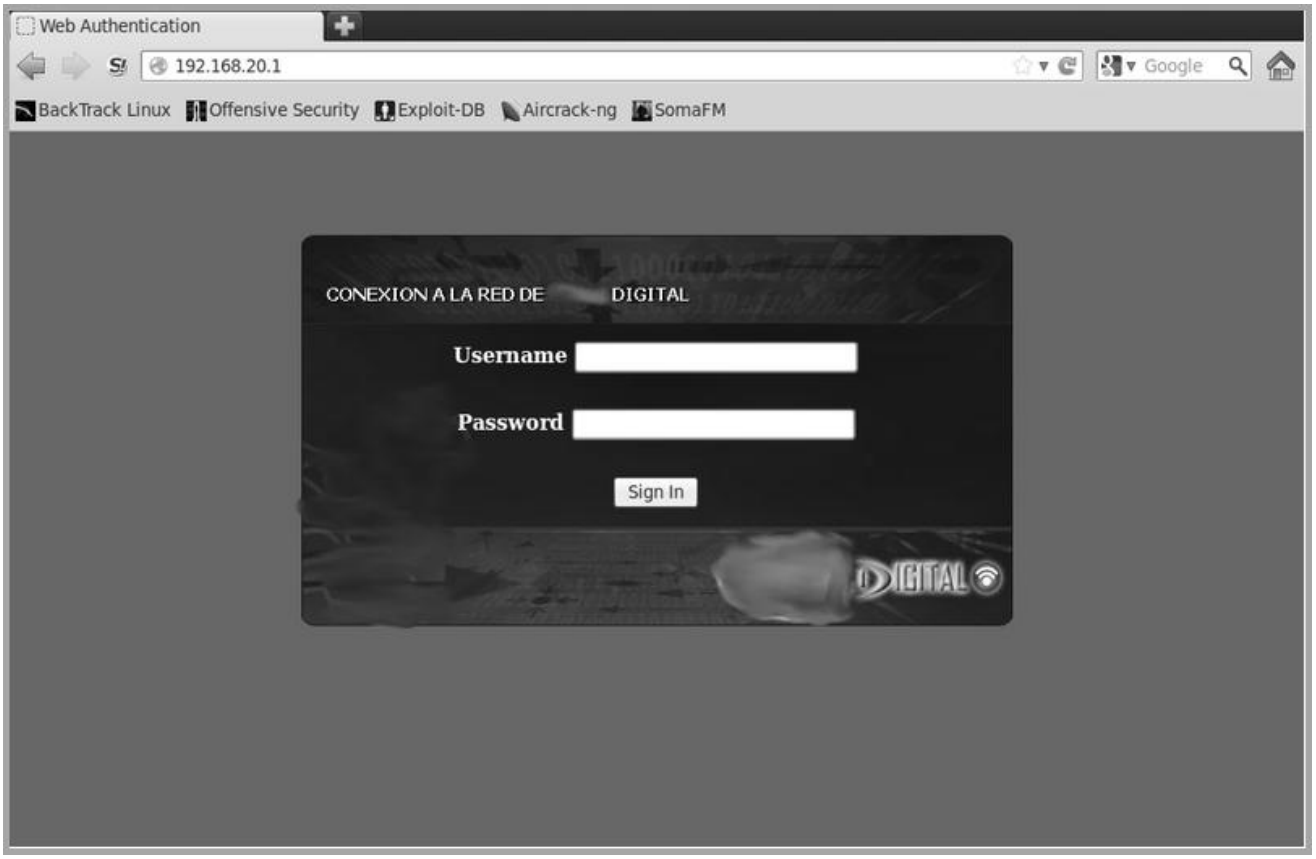

Figure 5. Cloned authentication web interface

the wireless network was legitimate. We didn't have to use emails, Trojan codes or other login forms to obtain the user credentials since the university has its own login form and it could be cloned.

```
192.168.20.18 - - [23/Nov/2012 12:15:36] "GET / HTTP/1.1" 200 -
192.168.20.19 - - [23/Nov/2012 12:16:10] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: buttonClicked=4
PARAM: redirect_url=
PARAM: err_flag=0
POSSIBLE USERNAME FIELD FOUND: username=c
POSSIBLE PASSWORD FIELD FOUND: password=1
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 6. Captured credentials

Easily the users connected to our access point and some users logged in the fake web interface. From here the users are susceptible to many attacks such as man in the middle, DNS spoofing, ARP spoofing, and so on. It's really hard for a regular user to be aware about this attack because everything seems to be normal. If something goes bad they immediately think that there is a problem with the network but never imagine that they are subject of attack.

The theft of this information is critical for the security of the users because the credentials we captured are the same for login to

computer services in the university such as email accounts, interactive system where students publish the homework and an academic system online that provide us full information of the user as full name, phone number, address, et al. Most of users use the same password for all kind of accounts they have on the Internet because it is easy for them to remember only one access key, so it is possible that the passwords we captured in our attack are the same for accounts like Facebook, Hotmail, Gmail, Twitter and many more. The user accounts can be obtained easily by Google searches taking into account that we have the user's full name.

6. Possible Solutions and Recomendations

a). It is hard for users to detect a fake access point and much more for those who don't know anything about networks. There are prevention systems of intruders such as AirDefense and Zone Alarm that have the capability to identify the fake access points. When an attacker uses these access points, he has to use other tools for capturing packets to a successful attack. These prevention systems alert the usage of capture packets tools.

b). To avoid becoming a victim of a cloned web interface, the user has to verify that the authentication web interface is shown in the browser through the *https* protocol. The organization in this case the university may warn the users through a pop up window when the authentication page appears, asking the user to check the website in search of this secure protocol before entering the credentials. With this message the users will be more conscious. Additional to this, a massive notification via email is needed to warn them about these frauds. The avoidance of this kind of attacks depends on the users because most of the time they don't care about the warnings. The figure 7 shows an example of this recommendation.

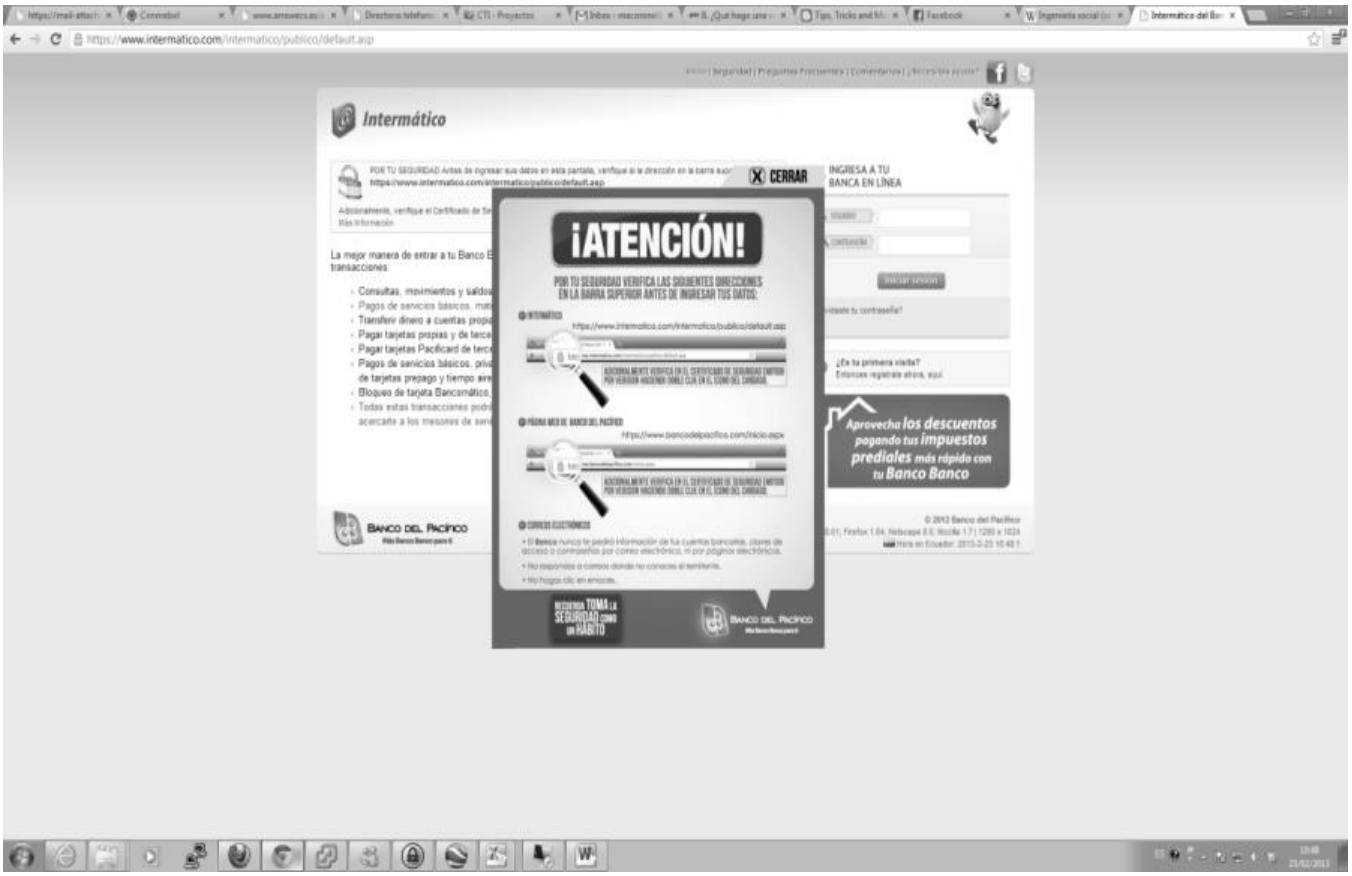

Figure 7. Intermatico [7]

c). The credentials of access are supposed to be unique for each user. However in the authentication system of this university it is possible to log in with the same username and password from two different terminals at the same time. Therefore it must be important to implement a security system that controls this event disallowing the access more than once. So when a legal user

tries to connect and someone is connected already with the same credentials, he will be notified that his account is being used by someone else, and also it will be reported automatically to the network administrator.

7. Conclusions

The evil twin attack is an easy way to obtain private information when we use social engineering techniques as we could see in this study. The success of this attack depends on the users and how informed they are about these kind of frauds. That's why it is important to educate all the users about the security of information and explain them the consequences that may result if they don't care about this. We can have the last technology in network security and the best policies to avoid attacks and frauds, but if the users are not committed or disregard these policies, we'll have an insecure network system undoubtedly.

References

[1] Wi-Fi Alliance. FAQ: What is an Evil Twin. Available in: http://www.wi-fi.org/knowledge-center/faq/what-%E2%80%9Ceviltwin%E2%80%9D.

[2] Hao Han, Bo Sheng, Chiu C. Tan, Qun Li,Sanglu Lu. (2011). A Timing-Based Scheme for Rogue AP Detection. 22 (11) Nobember. p. 1.

[3] Aircrack-ng Suite Documentation. (2007). Last Modify: July. Available in: http://www.aircrack-ng.org/doku.php#aircrack-ng_suite1.

[4] Wireless Networking in the Developing World, 2nd edition. December.

[5] Ermanno, Rob. (2010). Introducción a las Redes Wifi, *Materiales de Entrenamiento para Instructores de Redes Inalambricas.* June.

[6] Kimberly Graves. (2010). Certified Ethical Hacker STUDY GUIDE, Version 6. p. 50-53.

[7] Intermatico: Sistema de transacciones proporcionada por el Banco del Pacifico para uso de sus clientes. Available in: https://www.intermatico.com/intermatico/publico/index.asp.