CIS 551 HW2 Phase II

Aditya Deshpande

Aryaa Gautam

Aniruddha Rajashekhar

Di Wu

1. Steps to Execute

-make server generates the executable for server called “badbuf”, make client generates the executable for client called “client”.

-The server executable(“badbuf”) is deployed on the drone using gcc cross compiler. We also need to transfer the script restore.sh to the drone.

-The client is invoked by typing two parameters in the command line: ./client <host> ,i.e., ./client 192.168.1.1

- Both the server and the client commmunicate on the port number 10551, which is hard-coded in both server and client modules.

- After valid authentication, we can perform the following operations:

1)"add user" allows us to add a <username,password> pair to the system

2)"update password" allows to change the password for the current logged in user

3)"add mac address" allows to couple a MAC address and a port with the drone by prompting the user to “Enter Mac Address:” and “Enter Port:”

4)”delete mac address” allows the user to decouple an existing MAC address and port by prompting the user to “Enter Mac Address:” and “Enter Port:”

5)”quit” closes the connection

6) other shell commands like ls,cat and pwd

2. Implementation Details:

The file “names.txt” contains a table with existing <username,password> pairs.

The client enters a name and password after connecting to the server. The server checks the table contained in “names.txt” to verify whether authentication is successful or not.

If Authentication is successful, the server will simulate a shell, and the user can type the following options:

1 - add user

2 - update password

3 - add mac address

4 - delete mac address

5 - quit

6- Any other shell commans like cat,ls,pwd

The drone server or the authentication server drops/rejects all the connections except the ones trying on the port no. 10551. As a result, any traffic cannot reach the drone unless being authenticated by the authenticating server. Once the authentication is successful, the user can perform the following operations.

1 – “add user” As the name suggests, add user allows the client to add a new user and this leads to a new <username,password> entry in the table contained in names.txt

2 - “update password” is used to update the password of the user who is currently logged in.

3 – “add mac address” allows user to add devices that can connect to the server on a given port. For Example: A device can telnet to the drone by adding the Mac address of the device and adding port no 23 and if the MAC address coupling is successful. By default, the server doesn't allow any telnet connections to the drone.

4 – Delete mac address is used to block an already coupled device. Hence if we decouple an already paired device by entering the port no 23 and MAC address, the device will not be able to telnet to the drone.

5 - Quit closes the connection.

If authentication is not successful, The user is allowed to enter the login details for a maximum of 5 times. If the <name,password> pair turns out to be invalid after these attempts, a message “Invalid Identity” is displayed on the screen and the current connection closes.

The <name,password> pair addition and updation of password is done by performing update a linked list and by adding a node in a linked list, respectively.

The shellcode if filtered with the iptablels. The packets that contains the string “/bin/sh” or its hex string will be dropped. Also, the program checks for presence of shellcode in the username or the password entered for authentication.

The file “restore.sh” is used to restore the iptables’ state every five minutes.