CS 490 / ECE 492: Embedded Systems Security

Learning Linux Tools #01

Total Points: 100

Assigned Date : Wednesday, 20 January 2016
Due Date : Wednesday, January 27, 2016 @ 01:14:59 p.m.

1 Practice With Symmetric Key Encryption

Generate a text file with the networking stats of your PC (ie. IP address, DNS name, Gateway, etc.). Generate a key for the group to your left and encrypt your text file. Also, generate a different key for the group to your right and encrypt your text file. You should be able to exchange the encrypted file with either neighbor and both you and they should be able to decrypt it.

2 WiFi on BeagleBone

2.1 Install links2 on BB

From Lab 1, you should be able to connect your BeagleBone to the network through your desktop. Install links2 so that you can browse the web through a console.

2.2 Connect to SIUE-WIFI or Welcome to SIUE

You will be given a WiFi dongle to plug into the USB port of your BeagleBone. Figure out how to connect it to SIUE-WIFI (or Welcome to SIUE).

2.3 *tcpdump* Your Authentication to SIUE-WIFI

SIUE-WIFI (Welcome to SIUE) is not encrypted, but still requires username/password authentication. You should *tcpdump* your authentication connection to see if you can detect username/passwords being sent. Can you or can't you? Why?

2.4 Connect to SIUE-WPA

Figure out how to connect to the encrypted SIUE network, SIUE-WPA or eduroam on your BeagleBone.

3 Analyze Stock WiFi Router Firmware

You will also be given a WiFi access point/router. You should attempt to figure out how to connect your BeagleBone to it. Once connected, you should attempt to port scan it. You should also attempt to tcpdump the default authentication to the admin console on your AP. Save this dump. Next, at the very least, change the admin password to something other than the default. As more APs come online during class, try to sniff out your neighbors admin account credentials. Use nmap or another analyzer to try to do some more in depth fingerprinting on the router (ie. see if you can figure out which webserver is running and the version, see if you can find the OS version, etc.). Research if there are any vulnerabilities/exploits for the stock TP-Link firmware. (Note, next lab we will flash the firmware with OpenWRT.) If you find one, try to see if there is code for an exploit or if you can use Metasploit.