CS 490 / ECE 492: Embedded Systems Security

Firmware Analysis and Wi-Fi Security #03

Total Points: 100

Assigned Date : Wednesday, January 27, 2016
Due Date : Wednesday, February 03, 2016 @ 11:59:59 a.m. [**Group assignment.**]

1 Reverse Engineering Router Firmware

Obtain a copy of your router's stock firmware. I got mine from here: (http://www.tp-link.com/en/download/TL-WR1043ND.html#Firmware). Analyze the router firmware. Use commands like strings, hexdump, binwalk, etc. to examine the contents of the firmware.

(http://www.devttys0.com/2011/05/reverse-engineering-firmware-linksys-wag120n/ gives a good tutorial on the techniques). Attempt to dissassemble the code. IDA Pro is a great tool for this, however it is proprietary. There are some GNU utilities you can try to see if you can do it (ie. objdump). However, you need to know the instruction set of your router's CPU in order to do so. Find this out (it's not that hard). I'm not guaranteeing there will be anything interesting in the firmware, but many embedded devices are "hacked" using firmware analysis tools. You might be surprised at what you find in there. I think it runs Linux, so you might want to see if you can get access to the /etc/password, /etc/shadow, /etc/group files.

2 OpenWRT

The stock firmware for the TP-LINK is great, but can be somewhat limited in what it allows you to do. Fortunately, there is alternative, open-source firmware available through OpenWRT (Page for our router here: https://wiki.openwrt.org/toh/tp-link/tl-wr1043nd). Download this firmware file (https://downloads.openwrt.org/snapshots/trunk/ar71xx/generic/openwrt-ar71xx-generic-tl-wr1043nd-v3-squashfs-factory.bin). DO NOT USE ANY OTHER FIRMWARE FILE!!! YOU MAY BRICK YOUR ROUTER!!! Flash your router to use OpenWRT. Your router is now a full fledged Linux box (albeit somewhat limited). You should read up and install the web interface for OpenWRT. We will begin setting up a network in lab. To avoid conflicting networks, your internal network address should be 192.168.Y.0/24, where Y is the last number of your desktop's IP address (ie. 146.163.133.1 would be 192.168.1.0/24). Your desktop and BeagleBone will be on this internal network. To be able to access these stations remotely, you should set up a VPN to your internal network on your OpenWRT box.

3 WEP Cracking

As we know by now, unencrypted login pages and WiFi are bad news. So, why not encrypt your wireless connection using WEP? We know that WEP is a terrible scheme, but it still comes with router firmware. Encrypt your wireless connection with WEP with a pre-shared key. Research how to break WEP. Once you see other routers in class come online as WEP encrypted points you should be able to figure out their WEP keys (You might have to move your Wi-Fi adapter to your desktop, I've had mixed results with the Edimax adapters on the BeagleBone).

Deliverables

The due date of this assignment is **Wednesday, February 03, 2016 @ 11:59:59 a.m.** A dropbox will be opened for submission on Moodle before the due date. You are required to detail your findings in a report. All reports must be in **PDF** format. No exceptions.

- [**50 points**] A group report with the followings:
  - Motivation and objective of the experiment.
  - A detailed methodology of your experiment. You must be able explain the commands, tools, procedures you've used. Don't simply list the commands. We want you to explain what you've done and why you did it. Screenshots highly recommended.
  - A detailed testing plan and test results.
  - Justification of your observations. You must be able to justify and/or argue why (or why not) your method worked.
  - Final conclusions.
- [**20 points**] An individual report. Use this report to explain your individual contributions towards the experiment. This is a separate writing on your own. In essence, both members of the group will write their own individual report and make their own submission; you are only required to submit one group report. You can use the individual report to explain/mention/complain about your teammate's contributions to the project as well.
- [**30 points**] A group demo of your work. We will again ask you questions on what you've done and how you've done it.