CS 490 / ECE 492: Embedded Systems Security
Man-In-The-Middle and PKI #05
Total Points: 100

Assigned Date : Wednesday, February 17, 2016
Due Date : Monday, February 29, 2016 @ 11:59:59 a.m. [**Group assignment**]

1 Man-In-The-Middle Web Control System

By now, you and your neighbor should have a working web interface to control your stepper motor and read your temperature sensor. This lab, we are going to have you act nefariously by having you intercept and change the traffic in transit, what is known as a Man-In-The-Middle attack.

1.1 Tasks

1. Write a program to have your BeagleBoneBlack query your neighbor's temperature and/or set their motor speed through this interface and output the temperature and current motor speed, if changed, to the console. Ostensibly, to make this more realistic, you nominally are not allowed to ask your neighbor the format of their web API. You would have to port scan/monitor/netcat/telnet them to figure it out. However, many real systems do post API documentation, so we will allow it in this case, even though such API documentation in this lab is word of mouth.
2. MAKE SURE THE PATH YOUR DATA TAKES HAS GOES THROUGH YOUR KALI DESKTOP! Don't use Wi-FI/LAN connections on your router to route the traffic, unless you want to attempt the MITM attack using OpenWRT (it may be possible, depending on if you have enough space left in the 32MB of flash). This might entail some port-forwarding in Kali/OpenWRT to get outside traffic to your BeagleBone, which will be plugged in through USB to the desktop. Once you have ensured all traffic is routed through Kali, have your BBB script request the temperature from your neighbor. Kali should be able to intercept the response from your neighbor and alter the value to read -273.15C or -459.67F before forwarding it to your BBB, so your BBB reads erroneous data without being any wiser! Secondly, when your BBB tells your neighbor to spin the motor, you should intercept and change this request to be the maximal rate in the opposite direction of that requested (if they request some speed with a clockwise direction, you should alter it to be the max speed in the CCW direction and vice versa). Their poorly secured web interface should do exactly as you command, and, if this were a real industrial system, you'd have broken the $100,000 machine!

2 PKI and TLS Authentication

How do you stop these attacks? One way is through a public-key infrastructure and authenticated, secure transport layer communication. You will have to implement this for the lab.

2.1 Tasks

1. You are to generate a SSL/TLS certificate for your BeagleBone. As port forwarding should be setup for the web interface, you should act like it's a real cert for a real web server, and so you can use your exp.ee.siue.edu domain name for the cert. Once you have generated your public/private key pair and cert, you are to submit a certificate signing request to Dr. Gamage or Dr. York to have the root certificate for the lab sign and verify your newly minted certificate. For this to work, everyone in lab will have to add this root certificate to your system's list of trusted certificate authorities, so do so. Normally, you wouldn't touch custom certs with a 10 foot pole, but we are your instructors, you can trust us ;)!

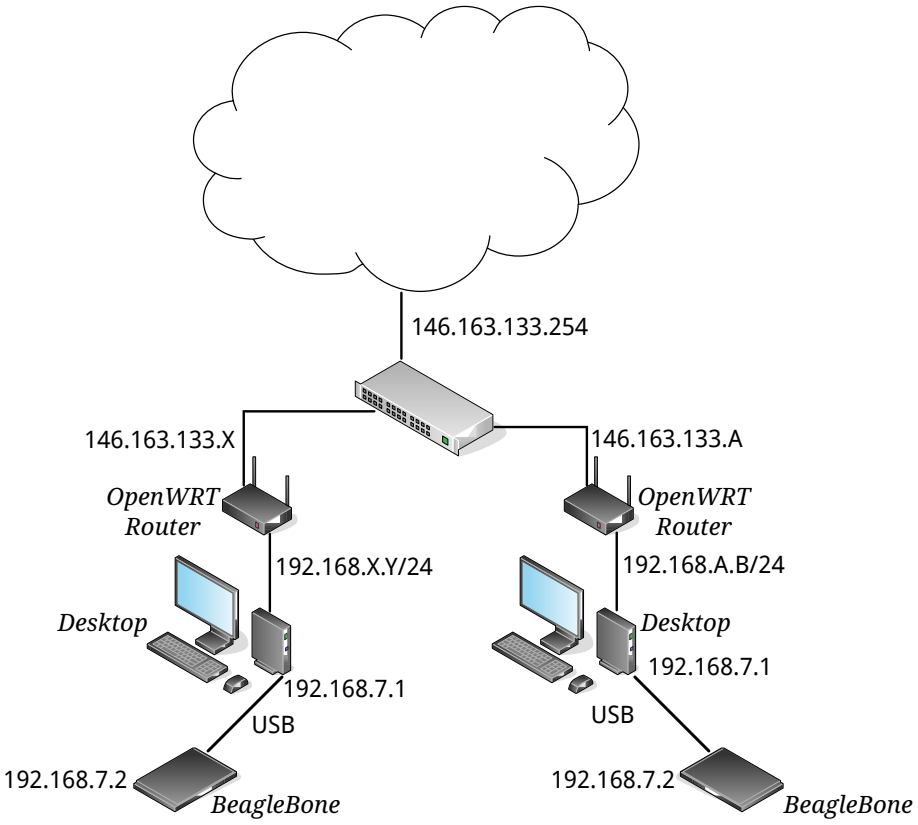

Figure 1: Network Topology

2. You should now run your temperature/motor web server on both an open, unencrypted port, as in Lab 4, and a separate, encrypted port (443 is typical, but you will be allowed any port for this lab). Encryption stops MITM attacks, but for the real-deal in web security, authentication is where it's at. Configure your encrypted web server to require a valid username/password before any response to temperature queries or motor commands.

Deliverables

The due date of this assignment is **Monday, February 29, 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 demo of your work. We will again ask you questions on what you've done and how you've done it.
- [**45 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.

- [**5 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.