Principles of Web Development

Mini Assignment 1
Due: September 17, 2018

Download Wireshark from wireshark.org. Get familiar with their website and watch their instructional video. Then install Wireshark on your PC.

Conduct two experiments: (a) save a 30 second (or more) Wi-Fi packet recording session of your PC's interaction with your home network. Then (b) save a 30 second (or more) Wi-Fi packet recording session at an open hot spot, like an outside city free hot spot, or McDonald's, or Tim Hortons (the less secure the better). You will need to set Wireshark in promiscuous mode. This will allow you to see other people's packets.

Note: depending on how your operating system is configured it may restrict your access to other people's packets. The wireshark.org website will have some suggestions for you or you can google your situation for help. But, in the end, this assignment is about understanding how much information can be extracted from packets, so seeing other people's packets is only the fun part not the important grading part of this assignment. Don't be stressed if you can't get to see other people's packets.

Write a report answering the following questions:

1. Identify the exact location you were when recording your two Wi-Fi packet recording sessions.
2. Experiment 1 (at home):
    1. Seclect, from the recording, a packet. By default, the GUI has three sections. The top section shows all the packets in summary. The middle section shows the packet you selected from the first section. The last section shows the raw data of the selected packet. Notice that the selected packet, in the middle section, has many rows, for example: Frame, Ethernet, Internet, Transmission, etc. If you have taken a network course then all these rows make sense to you, but for this course the Internet row and all the rows below that are important. Select one packet. Include a screen shot of it in your report.
    2. Identify the fields contained within the Internet packet. Compare that with the lecture slide that showed the structure of a sample complex Internet packet.
    3. What information does this packet contain? (where did it come from, where is it going, what protocol is it using, what security is it using, what message does it contain). This is the fun part, how much information can you extract from the packet you selected? Write down what you have discovered. Some packets are more interesting than others. Some packets are easier to read then others. Be wise in what you select.
3. Experiment 2 (at public hot spot):
    1. Select and sort by a sender IP address and try to deduce what they were trying to do.
    2. Include a screen shot of the sorted top summary panel for the above sender IP.
    3. Include a screen shot of one detailed packet from the sender IP that most helped you identify what that person was doing.
    4. NOTE: If you were not able to do that for someone else, then do that to your own packets.
4. Now, comparing your two data sets. Which location was more secure? Justify your position by providing screen shots and estimate, very roughly, the percentage of packets having strong and weak security.

WHAT TO HAND IN

Submit a PDF report to myCourses Mini Assignment #1 electronic drop box.

GRADING

This is graded proportionally as to how closely you were able to follow the instructions.

This mini assignment has two late days with -5% penalty per late day.

Total 20 points

- Question 1: 2 points
- Question 2: 9 points (3 for each sub-question)
- Question 3: 7 points (proportionally across all 4 sub-questions)
- Question 4: 2 points (with justification or 0 points)