# ELEC-C7420 - Basic principles in networking

## Assignment III - Authentication

**End Point Authentication**

Endpoint authentication is a security mechanism designed to ensure that only authorized devices can connect to a given network, site or service. The approach is also known as device authentication. In this context, the endpoint most often considered is a mobile computing device, like a laptop, smart phone or tablet but it could be any connected hardware device on a TCP/IP network. The possibilities include desktop computers, printers, servers and specialized hardware such as POS terminals, smart meters and other smart devices. Endpoint Security Management is becoming increasingly important in the expanding areas of machine-to-machine (M2M) communications and Internet of Things (IoT) Endpoint fingerprint is one method of enabling authentication of non-traditional network endpoints such as smartcard readers, HVAC systems, medical equipment and IP-enabled door locks.

In human communications, endpoint authentication is often used in conjunction with user authentication for greater security. Authenticating both the user and the device can provide two-factor authentication (2FA). For a smartphone, there are apps that provide one time password tokens, allowing the phone itself to serve as the physical device to satisfy the possession factor. The password response sent from the registered device verifies that the user is connecting from an authorized endpoint.

**Sketch**

This sketch scans for 802.11b/g/n network with one of the boards that support this library. Your Arduino Software (IDE) serial monitor will print out information about the board and the networks it can see, with the encryption type. It will connect to a network via authentication.

**Steps**

- Create a sketch that prints the board's MAC address.
- It scans for the available encrypted WiFi networks every 10 seconds and prints the WiFi channel and BSSID on the serial monitor.
- After 3 cycles (10 seconds/cycle) it connects to a provided SSID.
- It connects to the network via authentication (Password)

You can use your cellphone personal hotspot to carry out the authentication.

- Bonus: Create a sketch which brute forces the password on your WiFi. Set a simple password, such as 4 letters. How long does a single guess take? How long does it take for it to guess the password? What about if the password was 5, 6, 8, 12 letters? How about when adding numbers and symbols? How to reduce the time to break the password? How to prevent this method/was it prevented by your router/phone?

**Questions**

- Which authentication methods did you find for 802.11?
- Please describe three authentication methods in detail.
- Describe briefly applications scenarios for these methods.

**Submission**

Please submit a written report with your sketch, explanation of it, and answers to the questions. Suggested template:

- Section 1: Goals of the experiment (What is the purpose and motivation behind the experiment).
- Section 2: Experimental Setup (Details of the experimental setup step by step)
- Section 3: Results & Conclusion (Please include snaps for each step containing proof of the successful implementation)
- Section 4: Answer to the given questions.
- Section 5: Annex (Please paste your sketches in this section)

**Grading**

There's 10 points + 1 bonus point in total, from the following areas:

- Successfully print MAC address - 1p
- Successfully scan and show wifi channel and BSSID - 2p
- Successfully implement reading the network to connect - 1p
- Successfully connects the protected network - 1p
- Successfully find authentication methods - 1p
- Good description of the methods - 3p
- Good description of application scenarios - 1p
- Brute force sketch, explanation and answer to questions – Bonus: 1p