IoT Security and Privacy

HTTP, HTTPS, WebSocket

Instructions:

1. Note: Blue text points to a web link. Ctrl + Click to follow link.
2. Answers to all questions must be put into **ONE** document. That is, every time, each student can only submit one report document, answering all questions of this assignment, if not explicitly stated otherwise.
3. Students must put answers following each question in this assignment. The instructor will not grade a report with only answers in it and the student gets zero for such an assignment. An assignment report must include original questions.
4. Students MUST submit the finished assignment in either Microsoft Word or pdf format to Blackboard. The doc must be submitted as ONE standalone file and cannot be tarred or zipped into a container.
5. All required files or docs must be submitted in one submission (last submission). Note: Blackboard allows unlimited number of submission of one assignment by students.

Review questions

1. HTTP is a communication protocol between a client (browser) and a web server. (Yes/No)

2. HTTP is similar to HTML. (Yes/No)

3. https is http over SSL/TLS. (Yes/No)

4. SSL client performs the certification path validation algorithm. (Yes/No)

5. The certification path validation algorithm checks only if the certificate is valid. (Yes/No)

6. HTTP is full-duplex. That is, the client and server can communicate with each other simultaneously. (Yes/No)

7. WebSocket is full-duplex. (Yes/No)

Essay questions

1. Please discuss the path validation algorithm used by a web client authenticating a web server.

2. Assume that a server wants to authenticate a client with SSL/TLS/HTTPS. What information about the client should the server hold for the authentication? Why?