IoT Security and Privacy

Attacks against IoT

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.
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. The doc must be submitted as ONE standalone file and cannot be tarred or zipped into a container.

Review questions:

1. Many IoT devices do not disable their debugging ports after the testing and validation stage, which give attackers full access to the internal firmware. (Yes/No)

2. A UART controller is a microchip and a key component of parallel communication of a SoC (System on a Chip). (Yes/No)

3. We may use JTAG of a SoC to access the SoC's memory. (Yes/No)

4. We may use SPI of a SoC to access the SoC's memory. (Yes/No)

5. An IoT system is a networked system and may suffer from issues including weak authentication protocols, unsanitized user input and various programming bugs. (Yes/No)

6. Stuxnet was a computer virus and targeted SCADA systems and caused serious damage to Iran's nuclear program. (Yes/No)

Essay questions

1. Please discuss why mutual authentication is necessary between IoT devices and the IoT server.

2. Why is Joint test action group (JTAG) important for IoT security?