**IoT Security and Privacy**

**Term Project – MITM attacks against HTTP and HTTPS with mitmproxy**

**(10 points)**

### Instructions

**Please read the instructions carefully. Those students who fail to follow the instructions may get a zero score for this assignment.**

1. This is a group assignment while it can be done by one student. The instructor highly recommends students form groups given the complexity of this project. Each group can have at most two students. Each student MUST submit the group report even if it is the same for the group members. Those who do not submit the report will get ZERO for this assignment.
2. Answer each question following the original question. Do NOT delete the original question.
3. Answers to all questions must be put into **ONE** document.
4. 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.
5. 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.
6. All required files or docs must be submitted in one submission. Note: Blackboard allows unlimited number of submissions of an assignment and the instructor counts the last one.
7. Refer to [Print screen](http://en.wikipedia.org/wiki/Print_screen) on how to take a screenshot.
8. Underlined blue text points to a web link. Ctrl + Click to follow link.

**Lab**

In this term project, students will repeat the work in the tutorial on [MITM attacks against HTTP and HTTPS with mitmproxy](https://github.com/xinwenfu/mitmproxy-get/tree/main).

Read the entire tutorial first before starting to work on the project.

**Questions**

1. For [*Software setup*](https://github.com/xinwenfu/mitmproxy-get/tree/main#2-software-setup), please design approaches to show that the web server on Ubuntu VM works.
   1. Include a screenshot below to show *http* works. (1 point)
   2. Use a screenshot below to show *https* works. (1 point)
2. For [*Set up iptables to intercept HTTP traffic*](https://github.com/xinwenfu/mitmproxy-get/tree/main#3-set-up-iptables-to-intercept-http-traffic), include a screenshot to show iptables rules are added into the system. (1 point)
3. For [*MITM against HTTP*](https://github.com/xinwenfu/mitmproxy-get/blob/main/README.md#4-mitm-against-http)
   1. Include a screenshot to show mitmproxy can monitor HTTP flows. (1 point)
   2. Include a screenshot to show mitmproxy can intercept and modify HTTP traffic. (2 points)
4. For [*MITM against HTTPS*](https://github.com/xinwenfu/mitmproxy-get/blob/main/README.md#5-mitm-against-https)*,* include a screenshot to show mitmproxy can monitor HTTPS flows. (2 points)
5. For [*Decrypt TLS traffic*](https://github.com/xinwenfu/mitmproxy-get/blob/main/README.md#6-decrypt-tls-traffic)
   1. Include a screenshot to show if TLS traffic can be decrypted before sslkeylogfile.txt is imported into Wireshark and give the answer yes/no below. (1 point)
   2. Include a screenshot to show if TLS traffic can be decrypted after sslkeylogfile.txt is imported into Wireshark and give the answer yes/no below. (1 point)