Computer Science 530 - Assignment #2 -- Fall 2022

Due: Wednesday November 9th, 2022, 11:59 p.m.

This question is taken from the Fall 2017 Final exam:

Explain how the use of IPSec to protect the confidentiality and Integrity of communications between a web browser and a web server differ from the use of SSL (or TLS). In answering this question, assume you are using only one method - even though one could employ both. In you answer, be sure to discuss how all of the keys used are negotiated (chosen and communicated), and also identify the end-points that are authenticated (is it the Web Server, the Web Browser, the User, the company running the web server, or the host running the web server).

INSTRUCTION:

The report must be submitted by 11:59 p.m. on Wednesday November 9th. The report should be approximately 3 pages, or roughly 1200 to 1500 words. To submit your report you will use the USC DEN D2L Assignment Dropbox. Please be sure to include your name in the body of the assignment (i.e. within the Word, PDF, or Text File).

It is the individual student's responsibility to follow the submission instruction. Submissions that do not follow this instructions, e.g., submitted late, or only "Saved" and not submitted. may be penalized or may not be graded at all.

For the three reading reports in this course (of which this is one), students may receive an automatic extension of 48 hours total that may be applied across the three homework assignments. If you turn in one of your assignments 8 hours late, then you will only have 40 hours remaining in extensions to use on subsequent assignments. I suggest not using the whole 48 hours on the first assignment, because if you have an unforseen scheduling issue arises later in the semester, it will be your problem. Late assignments (beyond any extension) will be assesed 1 full letter penalty per day they are late, and if the topic of an assignment is covered in the lecture following the due date, then the assignment will not be accepted beyond that lecture.

GUIDELINE:

This is a lot to cover in so few words - so our advice is to write a first pass at your answer that is longer, and then edit out material that is redundant or not to the point. The use of tables can be very effective in conveying your ideas in a small area, but the tables must be integrated with your textual discussion, and not the only item in your submission.