CS763 Secure Software Development

HW 3

**Name:**

**Instructions:**

1. Please name your file as CS763\_yourusername\_hw2.
2. All questions must be answered on an INDIVIDUAL basis. If your answer is inspired by the discussion with other students, you need mention their names in your acknowledgement section.
3. State clearly all your assumptions if anything is ambiguous. Always ask if you have any questions.
4. Please **correctly cite and list any (online) references. Please pay attention to the academic conduct code, particularly the definition of plagiarism**.
5. Please submit your homework through Blackboard on time.
6. Thank You!

**Questions (100%):**

1. Answer the questions based on the following program. (30%)
   1. What are variables in this program? Where is each variable stored? (10%)
   2. What are bugs/vulnerabilities in this program? Briefly describe each of them. (You can check the strncat manual page here: <https://linux.die.net/man/3/strncat>) (20%)



1. Suppose Alice wants to communicate with Bob, please describe all necessary crypto means to provide confidentiality and integrity for this communication channel. In particular, your solution should prevent MITM. Please also state your assumptions. (25%)
2. Please read the paper “Analysis of the HTTPS Certificate Ecosystem“ that is posted on Blackboard the Course Documents/Lecture notes folder and answer the following questions: (45%)
   1. What is PKI? (5%)
   2. What are the differences and relationships between digital signature and digital certificate? (10%)
   3. What is HTTPS? How is digital signature/digital certificate used? (10%)
   4. Write one/two paragraphs to state issues in the HTTPS ecosystem described in the paper. (15%)
   5. This paper was published in 2013. Do some research on the internet to find any solution that has been developed or used to address the issues and improve the situation in recent couple of years. (5%)

## **Feedback:**

1. How long do you take to complete this homework? Is it too hard, too easy or OK? Does this homework help learn the material?

2. Is the lecture clear? How well do you understand this topic?

3. Do you have any other feedback?