CSCI 283 and CSCI 172- Graduate and Undergraduate Computer Security - Fall 2010
George Washington University

Homework 1

due 15 November, 6 pm.

50 points

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the test and final.

You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

You may not refer to solutions to previous years' problem sets, or ask for help students from previous years, except the TA.

Any violations will be treated as violations of the Code of Academic Integrity.

PLEASE submit all HW on Blackboard only. Name your files:
CS283_HW2_LASTNAME_FIRSTNAME.doc or .pdf or
CS172_HW2_LASTNAME_FIRSTNAME.doc or .pdf

Read the paper:

Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh Wenyuan Xu, Marco Gruteser, Wade Trappe, Ivan Seskar, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study", *USENIX Security*, 2010

Provide the following **on a single sheet of paper, with margins of at least one inch on all sides, and a font of size at least 11pt**. Optimal length is about 80% of a page.

1. **Contributions** 2-4 sentences: The main contribution(s) of the paper
2. **Summary: Analysis** One paragraph on the security analysis (attacks) described in the paper
3. **Summary: Design** One paragraph on the proposed solutions which are briefly described in the paper
4. **Comparison** One paragraph describing in what way the proposed solutions in the paper are different from the ones you submitted in HW 1. (Your solutions don't have the same as those proposed in the paper. The paper takes a broader view of the security problem, while you were told to focus on cryptographic solutions. Further, the paper has much more information on the tire pressure monitoring systems which you did not have for HW 1 so you could focus on what you were studying at that time, cryptographic approaches to solve these problems).