Syllabus addendum for 491/591 Spring 09:

3 February 2009

The following are changes to the syllabus that was posted at the beginning of the semester:

Lab grading: Lab grading will be based on your progress assuming the following background at the beginning of the semester:

491: You took a class in C once, but are not 100% comfortable with it, especially pointers
591: You're comfortable with C and know basic linux commands

Each lab posting should be about one or two substantive paragraphs, and each week after the Wednesday midnight deadline I'll grade the posts you've done in the last week, i.e., you need to do at least one post a week.

Here is an example of a post that would get a 5:

"This week I worked on lab 1. I figured out how to get the values that are the inputs and outputs to the last round function, and I wrote code that tests various rounds keys in the third round against probabilistic linear functions for the S-boxes. I'm not able to get a definitive answer for the last round subkey, though. I suspect it has something to do with the permutation I'm applying to the right half of the ciphertext. I posted a question to secpriv-chat about if that permutation is the same as the one for the right half of the plaintext and got some interesting feedback so next week I plan to try some of the suggestions people gave me."

Here is an example of a post that would get a 2:

"This week I read the web page about linear cryptanalysis. I thought it was very interesting. I downloaded the example code as a place to start, but it didn't compile."

No post is a 0.

Attendance: As stated in the syllabus, all students registered for a grade are expected to attend regularly, and pass/fail students should adhere to whatever agreement they made with me. I'm adding one exception: if you are required to take the course for a grade for graduation requirements and I have a letter on file from a boss, commander, HR dept., etc. that says that you cannot possibly attend Friday lectures regularly, then students registered for a grade can make arrangements with me about Friday attendance.

Pop quizzes: I'm adding something to the homework policy: I reserve the right to hold pop quizzes in class and count them as homework points. Students with unexcused absences will receive a 0.