COMP 5370/6370 Test #2 – This is the take-home part
Instructor: A. Skjellum; TA. A. Ravipati
November 4, 2015

YOUR NAME: ____

CLASS (5370 or 6370) ____________________ TIME SPENT ON EXAM? ____________

YOUR ID: ____________________

MAXIMUM TIME: 5 hours. Expected time: 2-3 hours.

Test conditions: It has to be done on your own, on your honor. No sharing materials, talking, or use of electronic devices other than to look up data of your own, without sharing it with others, during the exam. Academic Honestly rules of Auburn University apply as does the class syllabus. COMP5370 students: complete problems A and B. COMP6370 students: complete problem C as well. Undergrads, you can do problem "C" for extra credit, but still within the total time available.

This is due by class time on Monday, November 9, 2015. You will submit that by bringing hardcopy to class on Monday. It will be an additional 50 points for both sections.

Turn in this cover sheet, with your answers (written or printed, or both) attached with a staple, and please make sure the entire package has your name on every page.

High quality responses include: Concepts enumerated; comparisons and contrasts, cited sources, explanations; diagrams if appropriate.

PROBLEM A. (25 points for COM5350, 20 for COMP6350). You are on a desert island with "Computer Security: Art and Science," by Matt Bishop. You're well fed and warm and safe, and have time to read and write about computer security. You also have a working tablet that can surf the web (but only purposive sites about computers, security, and assurance).

Learn about ways to attack the integrity of virtual machines – in the cloud, and stand alone. Write about what you learn. Describe known attacks, how they work, what they do. Cite your sources.

Please note that attacks that steal secret keys are of interest here.

PROBLEM B. (25 points for COM5350, 20 for COMP6350). Explain “HIDS” and “NIDS” and how they work and what they do. Compare and contrast. Use your book and web resources. Differentiate anomaly from intrusion. Explain false positives and false negatives. Which is worse in either case?

PROBLEM C (10pts for COMP 6350 only). Explain how to perform denial of service attacks against TCP/IP using one of several approaches. Look them up, cite them, explain how they work. How do you mitigate them?