COMP 4900D: Operating System and Web Security

Fall 2012 Midterm Exam

October 18, 2012
Instructor: Anil Somayaji
2 hours, Open Book

Answer 3 out of the following 5 questions (you should omit 2). If you answer more than 3 questions, clearly indicate which ones should be graded (or ideally, don't include the extra answers). Please write your answers in a text or PDF file and upload to cuLearn by 9 PM today (October 18th).

The exam is open book, open note, open Internet. The only thing you may not do is discuss questions with other individuals. In other words, no emailing/IM/texting/whatever with other people during the exam!

If you have questions, email me at `soma@ccsl.carleton.ca`, and if you wish give me a phone number at which to call you. I will only guarantee to answer questions today between 10-12:30, however. If you feel a question is ambiguous, explain how you are resolving the ambiguity and answer the question.

Plan to do this midterm in one setting in two hours. Please indicate on your exam document how long you took to write the exam. Do not spend more than three hours on the exam. Make sure your answers are submitted by 9 PM.

How to Answer the Questions: Please do not simly answer the sub-questions individually and sequentially! Instead, please write a small essay that addresses all of these questions. Be specific where possible but make appropriate generalizations. Be concise—the essays will be long enough if you really answer the questions and time is short.

While you may structure your essays around the given questions, you are not obligated to do so; instead, what is important is for you to construct a coherent argument on the topic that roughly addresses the specific sub-questions. I will be grading each question holistically. A coherent essay that leaves out a few minor points will get a better grade than one that completely answers each sub-question but doesn't connect those answers together to form a larger argument. Above all, show me what you understand, not what you remember.

Good luck!

1. How is a cross-site scripting attack like a buffer overflow attack? Is there a mapping of the classic structure of no-op sled, shellcode, and return addresses to XSS attacks; if not, how are the two connected?

2. Compare and contrast the security protection provided by the randomization mechanisms in ASLR on Android, Noncespaces, and Instruction Set Randomization.

3. What security benefits to microkernels potentially provide? How are these benefits limited in practice?

4. To what extent does the L4 microkernel satisfy the highest Orange Book assurance level (A1)? What conditions does it satisfy, and what does it not (on its own)?

5. How is the protection provided by the MashupOS's sandbox tag like that provided by process isolation in a standard operating system? How is it different?