COMP 4108: Computer Systems Security

Winter 2016 Mid-term Exam

February 25, 2016

Instructor: Anil Somayaji

80 minutes, closed book

Answer all of the following three questions. Please write your answers in a separate exam booklet, or, alternately, type them on a computer and email them to `anil.somayaji@carleton.ca` or submit them on a provided USB key.

The exam is closed book. No notes, references, web sites, or collaboration.

How to Answer the Questions: Answer each question with a small essay. When the question has multiple parts, please do not answer them separately; instead, use them to help structure your small essay answer. Be specific and refer to specific readings covered in class; however, you should also make appropriate generalizations. Each essay should have multiple paragraphs including a (potentially brief) introductory paragraph (which states the thesis you are arguing) and concluding paragraph.

Above all, show me what you understand, not what you remember.

Good luck!

1. (6) Give a review of a security tool that you have used (for attack or defense). What is the tool? What is its purpose? To what extent does it achieve that purpose? What is its quality, in terms of functionality, reliability, and usability? Support your answer with specifics from your experiences with the tool.

2. (6) For an operating system of your choosing, to what extent is it a secure operating system? Specifically, does it implement a reference monitor, and is that reference monitor offer complete mediation, is tamperproof, and is verifiable? Be specific. You may refer to hardware features where applicable (but it is not required).

3. (8) For **two** systems where authorized users, and only authorized users, should have access to information (read, write, or both) stored on a system, describe the following:

   - What is the system?
   - What is a specific security threat the system faces? Remember this threat may involve matters of confidentiality, integrity, and availability. The threat may be hypothetical; it just needs to be plausible given the environment the system is designed or deployed for.
   - For this threat, what is one security mechanism that provides at least a partial defense against this threat?
   - To what extent is your chosen mechanism's effectiveness potentially compromised due to user and system administrator choices?
   - To what extent do you think there are vulnerabilities in the mechanism that could cause it to fail catastrophically?

   Rather than discuss two separate systems and two separate threats, you may discuss one system; however, you must discuss two distinct threats and two distinct mechanisms (one for each).