CS 4235 / CS 8803IIS Homework 6

Assigned: 30 March 2011
Due: 8 April 2011, 5:00pm Atlanta time. Students submitting solutions after that time but by 5:00pm Atlanta time on 11 April will have their scores scaled by 0.8. No solutions will be accepted after 5:00pm on 11 April.
Teaming: Work individually.

Solutions should be typewritten and submitted as a PDF file on T-Square. Be sure to include your name and GTID number on your submission. Scores will be posted on T-Square.

Although you may use outside sources for information, you:

- **must not** copy-and-paste text or figures from those sources, and
- **must** cite the sources. A citation should provide sufficient information for myself or anyone else to find the source that you used.

You do not need to cite the textbook or any course materials. If you are unsure whether or not you are using outside material appropriately, please ask me rather than guessing.

This homework has one written part worth 205 points. Please solve the following problems.

Written exercises

1. From Chapter 10:
   (a) (20 points) #1.
   (b) (15 points) #3.
2. From Chapter 4:
   (a) (10 points) #4.
   (b) (15 points) #11.
   (c) (20 points) #14.
   (d) (15 points) #19.
   (e) (15 points) #20.
   (f) (10 points) #25.
   (g) (10 points) #26.
   (h) (15 points) #27.
3. (10 points) Most access control in commercial operating systems is implemented using per-object access control lists, but other designs still have their uses. Give a real-world example of a capability-based access control system.

4. (20 points) A common OS-level security protection makes application program code execute-only and program data read/write-only.

   (a) Why are these access control protections useful? Explain the types of attacks that these protections defend against.

   (b) Is this protection always suitable? Can we impose these access control restrictions on every application? Explain your answer.

   (c) Operating systems provide system calls, like `mprotect`, that allow applications to change the permissions on their memory pages. Explain why this does or does not defeat the security of the memory page access control restrictions.

5. (30 points) Suppose testing an individual password for correctness requires 3 seconds.

   (a) If passwords are three uppercase alphabetic characters long and an attacker can try one password at a time, how much time on average would an attacker require to determine a particular password?

   (b) If passwords are six symbols long and each symbol is any of uppercase characters, lowercase characters, and numerals, then how much time on average would an attacker require to determine a particular password?

   (c) Suppose an English dictionary contains 50,000 words. If an attacker knows that a user's password is an English word followed by two digits, how much time on average is needed to determine the password?

   (d) If an attacker knows that a user's password is a phrase made of two words from the dictionary, how much time on average is needed to determine the password?

   (e) Desktop processors are now multicore. Explain how multicore processors improve an attacker's ability to determine a user's password.

   (f) How could an attacker utilize a botnet to efficiently determine a user's password?

   (g) How could an operating system detect an attacker attempting to find a password via brute force search?