CSE544/Spring 2018 - Takehome Midterm Exam

Due: Th, March 22, 2018, 11:59pm — Professor Trent Jaeger

Please read the instructions and questions carefully. You will be graded for clarity and correctness. All work must be your own or you will receive a failing grade.

Questions

1. (*10pts*) Define a *mandatory protection system* and its concepts. What is the purpose of each concept? Identify the mapping between MPS concepts and the following SELinux rules. What do these rules mean?

   ```
   allow httpd_t user_home_t:dir { read getattr search };
   allow httpd_t user_home_t:{ file lnk_file } { read getattr };
   type_transition httpd_t httpd_tmp_t:file httpd_tmp_t;
   allow httpd_t sysadm_t:process transition;
   type_transition sysadm_t httpd_exec_t:process httpd_t;
   ```

2. (*10pts*) Detail how the Scomp reference validation mechanisms (in multiple rings) satisfy the reference monitor concept (or fail to satisfy). Assume that all objects mediated outside the kernel are files (some reading between the lines is necesary here).

3. (*10pts*) What is a disclosure vulnerability? How is this exploited by JIT-ROP? How does Readactor prevent such a vulnerability from being exploited? Why does replacing readable code pointers with trampolines prevent indirect JIT-ROP attacks?

4. (*10pts*) Restate in your own words what you learned about driver isolation techniques from the Related Work of Herder *et al.* paper. Define each of the categories of driver operations that must be mediated and identify at least one technical challenge in mediating that type of operation. What problem is being solved by *memory grants*? How does this approach differ from the use of paging?

5. (*10pts*) What are CDIs and UDIs in the Clark-Wilson integrity model? What does Clark-Wilson integrity require of programs that process UDIs to maintain their integrity? What do programmers need to do to meet this requirement such that their programs satisfy Clark-Wilson integrity? How does CW-Lite approximate this requirement? What do programer need to do to their programs to satisfy the CW-Lite requirement (and enable their program to function)?

6. (*10pts*) Define *confinement*. Specify three ways to ensure that capability systems enforce confinement of their processes. Which approach has better performance and why? Does CHERI achieve confinement if a process has secret and public components and wishes to enforce MLS among them?

7. (*10pts*) Consider the access matrix below. Does it enforce *protection* of $O1$ data's integrity for subject $S2$? Does it enforce *integrity security* over $O1$ for subject $S2$? Explain. If a traditional capability system (e.g., Hydra) is used to enforce this access matrix policy, how does this impact our ability to enforce security? Explain.

	O1	O2	O3
S1		read getattr	read
S2	read write	read ioctl	
S3	read	append	read

8. (*10pts*) What is information flow control? How does Flume enable a secret process to reply to a message from a public process? How does Flume prevent the self-revocation problem in LOMAC from occuring? Can you express SELinux policies in the Flume model? Explain.

9. (*10pts*) Under what conditions can an adversary launch exploits against name resolution in file access operations? Under what conditions can an adversary successfully exploit a program to cause it to use an adversary-chosen filepath in an open system call? How does Jigsaw use a name flow graph to prevent these two attacks? What should Jigsaw do if a system call is performed that is outside the name flow graph that Jigsaw has available so far?

10. (*10pts*) What is control-flow integrity for kernel software (i.e., what are all the indirect control transfer events?)? Describe why it is difficult to enforce CFI for a preemptive kernel? Why is it difficult for the kernel to ensure control-flow integrity on kernel exits to user-space code?