CSE544/Fall 2015 - Takehome Midterm Exam

Due: M, November 13, 2015, 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?

```
type_transition foo_t user_home_t:dir user_foo_t;
allow foo_t user_home_t:dir { create read getattr search };
allow user_t foo_t:process transition;
allow user_t foo_exec_t:{ file } { read execute };
type_transition user_t foo_exec_t:process foo_t;
```

2. (*10pts*) Detail how the Linux Security Modules framework satisfies the reference monitor concept (aims to anyway). How does X. Zhang *et al.* verify complete mediation? How would you use Muthukumaran *et al.* to verify complete mediation? Devise a case that would *not* be verified correctly be each of Zhang and Muthukumaran.

3. (*10pts*) What is *address space layout randomization* (ASLR)? Describe one concrete *indirect disclosure* attack that would enable compromise of ASLR. How does Readactor *Crane et al.* enable a function to obtain a code pointer and use that pointer without revealing the code address (specify the process precisely - psuedocode)?

4. (*10pts*) Define each of the categories of driver operations that must be mediated from Herder *et al.* Prove *complete mediation* for the memory access and device I/O solutions.

5. (*10pts*) How does *control-flow integrity* prevent *return-oriented attacks*? Design a *dispatcher* function (Carlini et al.) and describe a CFI-based policy to prevent an adversary from compromising control flow with your function.

6. (*10pts*) How do capability systems enable blocking of confused deputy attacks? How could you enforce Jigsaw (Vijayakumar *et al.*) name flow graphs using a capability system (broad idea is sufficient)? Specifically, how would you configure Hydra to control a call from function A, which builds a file name using adversary input, to the callee, the `open` library function?

7. (*10pts*) Consider the access matrix below. Does it enforce *protection* of $O2$ data's integrity, where the only authorized writer is $S2$? Does it enforce *integrity security* over $O2$, where the only authorized writer is $S2$? Explain. If a MAC enforcement mechanism with protected path (see Loscocco *et al.*) is used to enforce this access matrix policy, how does this impact our ability to enforce security? Change the policy as necessary to enforce integrity security.

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

8. (*10pts*) Either prove that Biba integrity is sufficient to express Clark-Wilson for rules C1, C2, C5, E1, and E2 or provide a counterexample for each (for each rule, prove that Biba fails to satisfy Clark-Wilson by counterexample). I am expecting a proof or counterexample per rule. Be sufficiently detailed in your counterexamples.

9. (*10pts*) The MaLT system of F. Zhang *et al.* uses various software and hardware-based methods to trigger monitoring. Please describe each method precisely and assess whether the method is transparent to a determined and power adversary who knows MaLT may be running.

10. (*10pts*) Detail the methods for securely initiating a Private VM in Proxos and a cloaked process in Overshadow. The papers describe the basics, but there are several details that are implicit and must be ensured to bootstrap such processes securely. Use Biba integrity as a guide for whether you have bootstrapped securely.