Homework 1

Due: January 25, 2016 **Points:** 100

1. (*20 points*) Companies usually restrict the use of electronic mail to company business but do allow minimal use for personal reasons.

   (a) How might a company detect excessive personal use of electronic mail, other than by reading it? (*Hint:* Think about the personal use of a company telephone.)

   (b) Intuitively, it seems reasonable to ban *all* personal use of electronic mail on company computers. Explain why most companies do not do this.

2. (*20 points*) Peter Denning [1] formulated the principle of attenuation of privilege as "a procedure cannot access an object passed as a parameter in ways that the caller cannot." Contrast this formulation to that of the principle of attenuation of privilege in Section 2.4.3, which states "a subject may not increase its rights, nor grant rights it does not possess to another subject". In particular, which is the "subject" and which is the "other subject" in the Denning's statement?

3. (*20 points*) StackGuard is a tool for detecting buffer overflows. It modifies the compiler to place a known (pseudo)random number (a *canary*) on the stack just before the return address when a function is called. Additional code is added so that, just before the function returns, it pops the canary and compares it to the value that was placed upon the stack. If the two differ, StackGuard asserts a buffer overflow has occurred, and invokes an error handler to terminate the program. How effective is this approach at stopping stack-based buffer overflows? Under what conditions might it fail?

4. (*20 points*) As encryption conceals the contents of network messages, the ability of intrusion detection systems to read those packets decreases. Some have speculated that *all* intrusion detection will become host-based once all network packets have been encrypted. Do you agree? Justify your answer. In particular, if you agree, explain why no information of value can be gleaned from the network; if you disagree, describe the information of interest.

5. (*20 points*) Write a Ponder instance authorization to allow a professor to read an assignment submitted to a drop box between 7:00am and noon.

Extra credit

6. (*20 points*) Is it possible to design and implement a system in which no assumptions about trust are made? Why or why not?

References

1. P. Denning, "Fault Tolerant Operating Systems," *ACM Computing Surveys* **8**(4) pp. 359–389 (Dec. 1976). DOI: 10.1145/356678.356680