

Homework 1

Due: April 12, 2013

Points: 100

Questions

- (14 points) Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination of each. Remember to justify your answers.
 - John copies Mary's homework.
 - Paul crashes Linda's system.
 - Carol changes the amount of Angelo's check from \$100 to \$1,000.
 - Gina forges Roger's signature on a deed.
 - Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.
 - Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.
 - Henry spoofs Julie's IP address to gain access to her computer.(text §1.12, exercise 1).
- (20 points) Consider a very high-assurance system developed for the military. The system has a set of specifications, and both the design and implementation have been proven to satisfy the specifications. What questions should school administrators ask when deciding whether to purchase such a system for their school's use? (text §1.12, exercise 10).
- (36 points) The obvious way to test for overflow is to multiply the absolute value of *size* and `sizeof(int)` and see if the result is smaller than the absolute value of *size* (because if $|ab| < |a|$ when $|a| > 1$ and $|b| > 1$, then overflow has occurred). Does this always work—if so, say why, and if not, give a counterexample? Assuming it works, what problems would it introduce? (Hint: think about architectures allowing arithmetic overflow to cause a trap.) Suggest an alternate method without these problems. ("Robust Programming" handout, exercise 2).
- (10 points) On a Linux or UNIX-like system, how does `ftell(3S)` use `errno` to distinguish failure from success? ("Robust Programming" handout, exercise 15, modified).
- (20 points) A program called `lsu` gives access to role accounts. The user's access rights are checked, and the user is required to enter her password. If access rules allow the change and the user's password is correct, `lsu` allows the change. Given that Mary uses `lsu` from her account, why does `lsu` require her to enter her password? Name the principles involved, and why they require this. (text §13.6, exercise 8).

Extra Credit

- (14 points) The program `su` enables a UNIX user to access another user's account. Unless the first user is the superuser, `su` requires that the password of the second user be given. A (possibly apocryphal) version of `su` would ask for the user's password and, if it could not determine if the password was correct because the password file could not be opened, *immediately* grant superuser access so that the user could fix the problem. Discuss which of the design principles this approach meets, and which ones it violates. (text §13.6, exercise 10).