

Homework 2

Due Date: Thursday, October 20, 2005

Points: 100

1. (25 points) Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.
 - a. John copies Mary's homework.
 - b. Paul crashes Linda's system.
 - c. Carol changes the amount of Angelo's check from \$100 to \$1,000.
 - d. Gina forges Roger's signature on a deed.
 - e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.
 - f. 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.
2. (25 points) A respected computer scientist has said that no computer can ever be made perfectly secure. Why might she have said this?
3. (25 points) A bank has thousands of ATMs that it must control. It does so by building into each ATM a small server that accepts commands from the bank's master computer. The ATM software consists of a general purpose operating system (such as Windows or Linux) with some specific software designed to allow the bank to check the amount of money in the ATM, download a record of transactions conducted on the ATM, and perform specific supervisor functions such as shut down or disable the ATM.
 - a. The Principle of Least Privilege says that a system should not run unnecessary software. Do you believe the bank's ATM system obeys this principle? Why or why not?
 - b. Why do you think the bank did not write its own operating system?
4. (25 points) In Festa's article (handed out in class), Gary McGraw points out that extensibility allows a system to run software that the developers had not anticipated. He gives as an example a mobile telephone. The telephone does not contain all the programs the user might want or need, so the telephone has the ability to download and run software to update itself as required.
 - a. Why does McGraw consider this a major factor influencing the computer security problem?
 - b. McGraw says that incoming code may "change the environment." Assuming the telephone's software environment is known at the time of sale, and the software with which the telephone is sold relies on features of that environment, why is changing the environment bad?

Extra Credit

5. (10 points) In Miller *et al*'s article (handed out in class), they say "On machines like the VAXTM, the reference through the null pointer is valid and reads data at address zero." (The null pointer is defined as the zero pointer, hence the reference to address zero.) References through a null pointer should cause an error. Why do you think that, on the VAXTM system, the reference is valid? What might the designers have had in mind when they made this decision?