Sample Midterm Answers

1. Please define the following terms in one or two sentences.

   (a) assurance

   Answer: Assurance is a measure of evidence showing that a system meets specific requirements.

   (b) firewall

   Answer: A firewall is a system that sits between two networks and filters messages between the two, blocking those which violate the rules set in the firewall.

   (c) availability

   Answer: Availability means that one can interact with the system to the desired level of service ("quality of service").

   (d) cypherpunk remailer

   Answer: A cypherpunk remailer is used to send anonymous email; it keeps a table of the sender and a randomly chosen alias so that it can return replies to the sender. If this table is revealed, anonymity disappears.

2. Please circle the best answer, and *justify it*.

   (a) Which of the following is a good password?

   i. Mary
   ii. bananna
   iii. Clas$-1s+Boring
   iv. kglem23+fy

   Answer: iii; the first two are easy to guess ("bananna" is a misspelling, but a very common one), and the last is very difficult to remember. The third is a slightly mangled version of "Class is boring".

   (b) Which of the following is not an access control model?

   i. DAC
   ii. ORCON
   iii. RBAC
   iv. FTP

   Answer: iv; FTP is a protocol used to transfer files from one machine to another. DAC is discretionary access control, ORCON is originator-controlled access control, and RBAC is role-based access control, all of which are access control models.

   (c) Which of the following best describes a computer worm?

   i. A program that copies itself into other programs
   ii. A program that copies itself to other computer systems
   iii. A program that copies keystrokes and sends them to another system over the network
   iv. A program that accepts commands from a remote server and sends spam to a list of emails

   Answer: ii; the first is a computer virus, the third is a keystroke logger, and the last does not move from system to system, as a worm does.

   (d) Which of the following is *not* a principle of secure programs?

   i. Paranoia: assume the user will try to attack the system using the program

ii. Stupidity: assume the user will not know anything about the program

iii. Impossibility: assume anything that can't happen, will happen

iv. Clarity: assume the user needs to know, and rely on, the way the internals of the program works

Answer: iv; the others are basic principles of secure programming, and the last is exactly the opposite of the fourth principle, which says to hide that which the user need not know, so it can be changed without affecting his or her use of the program.

3. What is non-repudiation? Please give an example of a situation requiring non-repudiation.

   Answer: Non-repudiation is the inability to deny having done something like send a message or sign a contract. A situation that requires non-repudiation is the signing of a contract. When people sign a contract, they assume none will be able to deny having signed it, or else the repudiators could get out of complying with the contract.

4. Why is a precise statement of security requirements critical to the determination of whether a given system is secure?

   Answer: Security requirements define the security policy, which in turn states what the system must do to be considered secure. If the requirements are not precisely stated, it may be impossible to determine whether the system meets the requirements, and hence whether the system is secure.

5. Please label the following as a "policy" or a "mechanism". Justify your answers.

   (a) Only students may use the system.

   Answer: Policy; it does not identify anything to enforce that only students may use the system. It simply states that must happen.

   (b) A program that checks that the user enters the correct password.

   Answer: Mechanism; this describes something that enforces the user entering the correct password.

   (c) Systems can be connected to the Internet on alternate Thursdays only.

   Answer: Policy; it does not identify anything that connects the systems on alternate Thursdays, and disconnects them on other days. It simply states that must happen.

   (d) A firewall that prevents access to the system from non-University systems.

   Answer: Mechanism; this identifies something that will block access as stated above.