CS 3IS3 Fall 2007

Midterm Test Answer Key

Instructor: William M. Farmer

You have 50 minutes to complete this test consisting of 6 pages and 27 questions. You may use your notes and textbooks, but you may not use any calculators or other electronic devices. Circle the *best* answer for the multiple choice questions, and write the answer in the space provided for the other questions. Good luck!

(1) [3 pts.] The Basic Security Theorem for the Bell-LaPadula Model is proved by induction on the number of state transitions. Is this statement true or false?

(a) [✓ True.]

(b) False.

(2) [3 pts.] A security mechanism that is *secure* but not *precise* could be completely useless. Is this statement true or false?

(a) [✓ True.]

(b) False.

(3) [3 pts.] In the Bell-LaPadula Model the set of security clearances is not the same as the set of security classifications.

(a) True.

(b) [✓ False.]

(4) [3 pts.] The Chinese Wall Model allows a subject to write documents in two different company datasets if the datasets are not in the same conflict of interest class. Is this statement true or false?

(a) True.

(b) [✓ False.]

(5) [3 pts.] Every organization has a security posture? Is this statement true or false?

(a) [✓ True.]

(b) False.

(6) [3 pts.] Determining whether a protection system based on the Access Control Matrix Model is safe with respect to a given right is a decidable problem. Is this statement true or false?

(a) True.

(b) [✓ False.]

(7) [3 pts.] Confidentiality is a much bigger concern than integrity in a hospital information system. Is this statement true or false?

(a) True.

(b) [✓ False.]

(8) [3 pts.] Copyright is an example of a mandatory access control. Is this statement true or false?

(a) True.

(b) [✓ False.]

(9) [3 pts.] The Chinese Wall Model cannot fully emulate the Bell-LaPadula Model. Is this statement true or false?

(a) [✓ True.]

(b) False.

(10) [3 pts.] A banker is concerned foremost with protecting the ________ of bank account information.

(a) Confidentiality.

(b) [✓ Integrity.]

(c) Availability.

(d) Size.

(11) [3 pts.] Which kind of cryptographic key would normally be known to the least number of people?

(a) Conventional encryption key.

(b) Conventional decryption key.

(c) Public key of a public-private key pair.

(d) [✓ Private key of a public-private key pair.]

(12) [3 pts.] An effective approach to modeling integrity in an information system is to

(a) View it as the dual of confidentiality.
(b) Control what objects are accessible in the information system.
(c) [✓ Control what actions can be performed in the information system.]
(d) All of the above.

(13) [3 pts.] Which security policy model includes a mechanism for handling changes to the system made by trusted subjects?

(a) Bell-LaPadula Model.
(b) Biba Model.
(c) [✓ Clark-Wilson Model.]
(d) None of the above.

(14) [3 pts.] A problem is mathematically infeasible if

(a) It is impossible to solve.
(b) It cannot be solved by a computer program.
(c) [✓ It can be solved but only with a huge number of computers running for a huge period of time.]
(d) It cannot be solved in linear time.

(15) [3 pts.] Which of the following models is more theoretical than practical.

(a) Bell LaPadula Model
(b) [✓ Biba Model.]
(c) Chinese Wall Model.
(d) Clark-Wilson Model.

(16) [3 pts.] A side-channel attack on a cryptosystem exploits flaws in the

(a) Design of the encryption algorithms used by the cryptosystem.
(b) Storage of the cryptographic keys of the cryptosystem.
(c) [✓ Implementation of the cryptosystem.]
(d) Procedures used by the human operators of the cryptosystem.

(17) [3 pts.] The Biba Model is a model for

(a) Confidentiality security policies.
(b) [✓ Integrity security policies.]
(c) Availability security policies
(d) Confidentiality and integrity combination security policies.

(18) [3 pts.] Which conventional encryption algorithm is now essentially obsolete?

(a) [✓ DES.]
(b) IDEA.
(c) Blowfish.
(d) RSA.

(19) [3 pts.] A security policy is to an information system as a(n) _________ is to a software system.

(a) [✓ Requirements specification.]
(b) Design architecture.
(c) Implementation.
(d) Product description.

(20) [3 pts.] Why is information security much more important today than it was 25 years ago?

(a) The amount of digital property in the world has mushroomed.
(b) Information is much more widely accessible today via the Internet.
(c) Information systems are much more highly interconnected today.
(d) [✓ All of the above.]

Answer each of the next six questions briefly with 1–3 sentences. (The marker will only read the first 3 sentences of an answer.)

(21) [5 pts.] Give an example in which the integrity of an object's metadata is crucial.

Answer: Part of the metadata of a submitted homework assignment is the time it was received. The integrity of the time-received metadata is crucial because a homework assignment is usually not accepted if it is received after the time it is due.

(22) [5 pts.] What is a denial of service attack?

Answer: A denial of service attack is an attempt to prevent users from having access to a service.

(23) [5 pts.] Why hasn't public key encryption made conventional encryption obsolete?

Answer: Conventional encryption is much more efficient for encrypting data than public key encryption. Public key encryption is only used to encrypt small amounts of data. Rather than confidentiality, its main applications are integrity and digital signatures.

(24) [5 pts.] What is the main difficulty in using conventional encryption over the Internet?

Answer: The distribution of session keys is the main difficulty in using conventional encryption over the Internet. A session key must be distributed as secret data to subjects who may not know each other.

(25) [5 pts.] Why will a brute force attack against a shuffle cipher usually not be successful?

Answer: A brute force attack against a shuffle cipher would have to potentially try

$$26! = 403291461126605635584000000$$

different keys.

(26) [5 pts.] What is the principle of least privilege?

Answer: The principle of least privilege is the idea that a subject should be given the minimum privileges needed to perform its prescribed task.

(27) [10 pts.] Present the information in the following Unix file table as an access control matrix. Assume that there are only four accounts (`dick, jane, sally, root`), four rights (`read (r), write (w), execute (x), own (o)`), and the group `admin` contains the accounts `root` and `jane`.

```
-rwxr-xr--  dick  admin   43520 18 Mar  2001 file1
-rw-rw----  root  admin  322362  4 Jun 09:32 file2
-rwxrwxr-x  jane  jane   478044  8 Jun 09:00 file3
```

Answer:

	file1	file2	file3
dick	{r,w,x,o}	{}	{r,x}
jane	{r,x}	{r,w}	{r,w,x,o}
sally	{r}	{}	{r,x}
root	{r,w,x}	{r,w,x,o}	{r,w,x}