# CS 3IS3 Fall 2007

## Final Examination Answer Key

Instructor: William M. Farmer

Revised: 11 December 2007

(1) [2 pts.] A biometric authentication mechanism measures physiological or behavior characteristics of a person. Is this statement true or false?

A.) [True.]

B.) False.

(2) [2 pts.] It is crucial to protect the confidentiality of public keys. Is this statement true or false?

A.) True.

B.) [False.]

(3) [2 pts.] The Unix and Windows operating systems both use ring-based access control. Is this statement true or false?

A.) True.

B.) [False.]

(4) [2 pts.] The information security of direct-recording electronic (DRE) voting systems is clearly greater than that of optical scan voting systems. Is this statement true or false?

A.) True.

B.) [False.]

(5) [2 pts.] An X Windows client authenticates itself to an X Windows server by proving that it knows the *magic cookie*. Is this statement true or false?

A.) [True.]

B.) False.

(6) [2 pts.] Denial of service attacks are attacks against the confidentiality and integrity of information. Is this statement true or false?

A.) True.

B.) [False.]

(7) [2 pts.] The path name of a file in a URL is usually absolute. Is this statement true or false?

A.) True.

B.) [False.]

(8) [2 pts.] Security mechanisms should be as user-friendly as possible so that users do not try to go around them. Is this statement true or false?

A.) True.

B.) [False.]

(9) [2 pts.] Many operating systems implement the access control matrix model as a single matrix stored in a single file. Is this statement true or false?

A.) True.

B.) [False.]

(10) [2 pts.] Mobile code is usually malicious. Is this statement true or false?

A.) True.

B.) [False.]

(11) [2 pts.] The purpose of the Needham-Schroeder protocol is to distribute a session key to two parties without allowing a replay attack. Is this statement true or false?

A.) [True.]

B.) False.

(12) [2 pts.] In the Clark-Wilson Integrity Model *enforcement rules* are used to guarantee that transactions do not violate the integrity constraints of the system. Is this statement true or false?

A.) True.

B.) [False.]

(13) [2 pts.] Without a security policy it is not possible to decide whether

A.) A program is malicious.

B.) An access control mechanism is working correctly.

C.) An information system is secure.

D.) [All of the above.]

(14) [2 pts.] A common form of phishing combines _____ with web site forgery.

A.) [Spamming.]

B.) Password cracking.

C.) Session hijacking.

D.) Cryptanalysis.

(15) [2 pts.] What is the best way for $A$ to send $B$ an e-mail message and then for $B$ to send $A$ an e-mail message back without $B$ knowing who $A$ is?

A.) $A$ spoofs the source address in the e-mail message sent to $B$.

B.) [$A$ sends the e-mail message to $B$ via a pseudo-anonymous remailer.]

C.) $A$ sends the e-mail message to $B$ via a Cyberpunk remailer.

D.) $A$ encrypts the header information of the e-mail message to $B$.

(16) [2 pts.] Which of the following is the least important application of public key encryption?

A.) Confidentiality.

B.) Integrity

C.) Digital signature.

D.) Secret key exchange.

(17) [2 pts.] Why is the Mozilla Firefox web browser more secure with respect to the *autocomplete* feature than other popular web browsers?

A.) Mozilla Firefox does not support the autocomplete feature.

B.) Mozilla Firefox does not support the autocomplete feature with passwords.

C.) Mozilla Firefox does not allow passwords to be saved.

D.) Mozilla Firefox offers the option of using a master password to protect saved passwords.

(18) [2 pts.] Which kind of intrusion detection looks for abnormal events?

A.) Anomaly detection.

B.) Misuse detection.

C.) Specification-based detection.

D.) Login detection.

(19) [2 pts.] A Unix setuid program executes with the privileges of the

A.) Root account.

B.) Program's caller.

C.) Program's owner.

D.) Program's group.

(20) [2 pts.] A reference validation mechanism is a means to satisfy which security design principle?

A.) Principle of least common mechanism.

B.) Principle of separation of privilege.

C.) Principle of complete mediation.

D.) Principle of least privilege.

(21) [2 pts.] Which of the following statements about the security of McMaster University's WebCT is true?

A.) Authentication is based on cookies instead of passwords.

B.) Passwords are sent across the network as plain text.

C.) Only the login portion of a WebCT session is encrypted.

D.) The entire portion of a WebCT session is encrypted.

(22) [2 pts.] Which kind of access control mechanism does Unix use?

A.) Access control lists.

B.) Capability lists.

C.) Propagated access control lists.

D.) All of the above.

(23) [2 pts.] Which kind of access control mechanism divides access privileges between objects and subjects?

A.) Access control lists.

B.) Capability lists.

C.) Locks and keys.

D.) All of the above.

(24) [2 pts.] Which kind of malicious software usually provides a useful function?

A.) Trojan horse.

B.) Computer virus

C.) Computer worm.

D.) Computer bacterium.

(25) [2 pts.] According to the principle of fail-safe faults,

A.) A system should be fail-safe in its initial state.

B.) A system should not give subjects access to objects by default.

C.) If a subject fails to complete a task, the access rights given to it for the task should be revoked.

D.) All of the above.

(26) [2 pts.] A computer virus that inserts code into a shell script is called a

A.) Stealth virus.

B.) Macro virus.

C.) Polymorphic virus.

D.) Metamorphic virus.

(27) [2 pts.] SMTP is

A.) The most popular anti-spam software that runs on mail servers.

B.) The protocol for sending e-mail across the Internet.

C.) A group of principles for countering social engineering tricks.

D.) A security policy for payment account systems.

(28) [2 pts.] Which access control model is concerned with confidentiality but not integrity?

A.) Bell-LaPadula model.

B.) Biba model.

C.) Clark-Wilson model.

D.) Clinical Information Systems Security Policy.

(29) [2 pts.] Fill in the blank. Definite description is related to the word **the** as indefinite description is related to the word *a*.

(30) [2 pts.] Fill in the blank. A DNS domain name is related to a Unix login name as a(n) **IP address** is related to a Unix UID.

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

(31) [5 pts.] What is proof-carrying code?

**Answer**: Proof-carrying code is a program that carries with its code a proof that the program satisfies its requirements.

(32) [5 pts.] $\{e_{\mathsf{Alice}} \parallel \mathsf{Alice} \parallel T\}d_{\mathsf{Cathy}}$ represents a certificate. What does $d_{\mathsf{Cathy}}$ mean in this representation?

**Answer**: $d_{\mathsf{Cathy}}$ is the private key belonging to Cathy that is used to encrypt the certificate.

(33) [5 pts.] Give an example of a mandatory access control (MAC) rule.

**Answer**: The no-read-up and no-write-down rules of the Bell-LaPadula model are MAC rules.

(34) [5 pts.] What is the purpose of *integrity invariants* in a transaction-based information system?

**Answer**: The system is designed so that, as long as the transactions preserve the integrity invariants, the system will not violate the integrity of the information it holds.

(35) [5 pts.] In the Bell-LaPadula model, what does *no read up* mean?

**Answer**: The no-read-up rule means that a subject may not read an object that has a security classification strictly higher than its security clearance.

(36) [5 pts.] In the use of cryptographic locks and keys, what is the difference between or-access and and-access?

**Answer**: Or-access and and-access is access to an object given to a group of subjects. With or-access, access is allowed if it is requested by *any* member of the group, while with and-access, it is allowed if it is requested by *every* member of the group.

(37) [5 pts.] Why are type 1 dictionary attacks of Linux and Unix systems more difficult to perform today than they were several years ago?

**Answer**: The list of encrypted passwords was previously contained in the file `/etc/passwd` which is readable by every user account. The list of encrypted passwords is now contained in a highly protected file. As a result, it was much easier several years ago to obtain the list of encrypted passwords than it is now.

(38) [5 pts.] The Unix password system can be viewed as an authentication system $(A, C, F, L, S)$. What is $F$ for the Unix password system?

**Answer**: $F$ is the set $\{f\}$ where $f : A \rightarrow C$ is the one-way encryption algorithm that is used to encrypt user passwords.

The End