Midterm Exam
CS 136
Spring, 2009

Answer all questions. There are 100 points total.

Multiple Choice questions. Each multiple choice question is worth 4 points. There is one best answer for each multiple choice question.

1. In asymmetric cryptography, which of the following MUST be true:
    a. Different keys are used for encryption and decryption
    b. Different algorithms are used for encryption and decryption
    c. Cryptographic operations are one-way, and not reversible
    d. Encryption takes much longer than decryption
2. Which of the following is NOT a common use of public key cryptography?
    a. Digital signatures
    b. Key distribution
    c. Protection of real time streaming data
    d. Certificates
3. Crossover error rate refers to:
    a. The point at which cryptography cannot keep up with speed of data creation
    b. The intersection between false positive and false negative curves for a biometric authentication measurement
    c. The measurement used in differential cryptanalysis to determine the next plaintext to offer to a cipher
    d. The data rate achievable by a covert channel
4. Full disk encryption protects against which of the following threats:
    a. Buffer overflows
    b. Covert channels
    c. Compromises of the operating system
    d. Loss of data when computers are stolen

5. Social engineering refers to:
    a. Attackers fooling human users into revealing information
    b. Proper design of security solutions for usability
    c. Improvements in user training and education to reduce security risks
    d. Methods of designing web-of-trust applications to match real world social structures
6. The *-property of the Bell-La Padula security policy prevents the following from happening improperly:
    a. Unprivileged subjects from reading sensitive objects
    b. Transfer of privileges from one subject to another
    c. Alteration of a critical object by an unprivileged subject
    d. Write-down by a privileged subject

7. The Microsoft Vista operating system contains a mandatory access policy. Which of these is its purpose?
    a. Maintaining integrity of files when a user runs untrusted executables
    b. Maintaining secrecy of files between users on a server system
    c. Implementing the Chinese Wall policy
    d. Allowing access only to authenticated users
8. Encapsulation mechanisms allow a system to achieve which of these security goals?
    a. Allowing access only to authenticated users
    b. Maintaining integrity of critical data
    c. Implementing the principle of least privilege for executables
    d. Improving protection of cryptographic keys
9. Why do conflicts in access control lists occur?
    a. Because users disagree on when access should be granted
    b. Because a principal matches multiple entries in the access control list
    c. Because users are not properly authenticated
    d. Because a principal's access privileges change over time
10. Which of the following is true of man-in-the-middle attacks?
    a. They cannot be performed if one uses public key cryptography
    b. They require the attacker to have pre-recorded some legitimate messages for use in the attack
    c. They require the ability to intercept communications between legitimate parties
    d. They can only be performed with the active involvement of a human attacker
11. Which of the following pairs of desirable properties in a cipher will be hard to achieve simultaneously?
    a. Freedom from complexity and low error propagation
    b. Good diffusion and good confusion
    c. Good diffusion and low error propagation

    d. Good confusion and freedom from complexity
12. If one uses a cipherblock chaining (CBC) cryptographic mode, which of the following is true?
    a. A single bit flip error in the first block will corrupt decryption of that block only
    b. A single bit flip error in the first block will corrupt decryption of the first and second block
    c. A single bit flip error in the first block will corrupt decryption of the first, second, and third blocks
    d. A single bit flip error in the first block will corrupt decryption of all blocks of the transmission
13. Which of the following statements is true about using symmetric cryptography to provide authentication of the creator of a piece of information?
    a. It cannot be done
    b. It cannot be used for authentication of information stored for a long period of time
    c. Untrusted third parties can directly check the authentication
    d. It requires use of a trusted third party
14. If a particular cipher used by party A to encrypt a packet sent to party B has been cracked by brute force, which of the following is true?
    a. The cracker can now easily read all messages encrypted with that cipher by all parties using it
    b. The attacker has only gained access to the information encrypted in the particular packet he cracked
    c. Communications between party C and party D using the same cipher are likely to be just as secure as before the crack
    d. The particular key used by A and B must never again be chosen by anyone using that cipher
15. Which of the following issues is NOT critical to the secure use of public key cryptography?
    a. Key length
    b. Authentication of the owner of a particular public key
    c. Inability of anyone to derive a private key given a matching public key
    d. Ensuring that only desired communication partners learn one's public key
16. Alice and Bob each have their own public/private asymmetric cryptographic key pair. Alice knows Bob's public key and Bob knows Alice's public key. Neither knows each other's private key. Alice encrypts a message to Bob with her private key and transmits it to him. What does Bob know, based on this cryptography, when he receives and decrypts this message?
    a. The message could only have been created by Alice
    b. The message has been kept secret from everyone except himself and Alice
    c. Alice meant this message only for Bob
    d. None of the above

17. In a cryptographic protocol, what is the purpose of a nonce?
    a. To ensure that each run of the protocol is new and fresh
    b. To handle situations where clock synchronization is hard to obtain
    c. To verify that a trusted arbitrator has responded with a key for the desired communication partner
    d. To defeat brute force attacks on the session key

18. Choosing good passwords depends on a number of factors, including the set of characters one chooses from and the number of characters in the password. Assuming 8 character passwords, if you go from passwords chosen randomly using only the English lower case letters a-z, to passwords that include both the lower and upper case English letters, how many more passwords are possible?
    a. Twice as many
    b. 256 times as many
    c. 128 times as many
    d. 26 times as many
19. Which statement best describes the standard operating system approach to protecting data in RAM?
    a. Use hardware protection to limit what pages can be named
    b. Use standard access control mechanisms to handle access requests
    c. Encrypt data on data pages
    d. Detect illegal accesses and log them
20. Which of these describes a fundamental difference between the Unix/Linux setuid/setgid mechanism and role-based access control?
    a. One of them allows controlled expansion of a human user's privileges, while the other doesn't
    b. One of them requires careful setting of access permissions if it is to be used safely, while the other doesn't
    c. One of them allows specification of only a limited number of identities, while the other allows specification of an arbitrary number
    d. One of them is explicitly tied to use of particular executables, while the other isn't

Short Answer questions. Answer each of these in 1-3 sentences. Each question is worth 4 points.

1. Originator controlled access control policies (also known as ORCON or ORGCON) are usually technically difficult to implement in computer systems. Why?

2. How could you use the Chinese Wall model to achieve the desirable goal of separation of duties for a critical task requiring multiple steps?

3. Which would be easier to implement in hardware, DES or RSA? Why?

4. One method of revoking a capability is to require a generation number to be provided with the capability when presented for use. To revoke the capability, one increments the required generation number at the capability checking mechanism, providing the new number to those who should still have access, and not providing it to those who should have access revoked. What is problematic about this approach in a distributed capability system where multiple authorities run the different machines?

5. One approach to automatically generating passwords for people to use is to create random, but pronounceable, passwords by combining phonemes. What are the advantages and disadvantages of this approach?