Chapter 2 - Authentication, Access Control & Cryptography

**1. Describe each of the following four kinds of access control mechanisms in terms of (a) ease of determining authorized access during execution, (b) ease of adding access for a new subject, (c) ease of deleting access by a subject, and (d) ease of creating a new object to which all subjects by default have access.**

**• per-subject access control list (that is, one list for each subject tells**

**all the objects to which that subject has access)**

**• per-object access control list (that is, one list for each object tells all**

**the subjects who have access to that object)**

**• access control matrix**

**• capability**

**2. Suppose a per-subject access control list is used. Deleting an object in such a**

**system is inconvenient because all changes must be made to the control lists of**

**all subjects who did have access to the object. Suggest an alternative, less costly**

**means of handling deletion.**

**3. File access control relates largely to the secrecy dimension of security. What**

**is the relationship between an access control matrix and the integrity of the**

**objects to which access is being controlled?**

**4. One feature of a capability-based protection system is the ability of one**

**process to transfer a copy of a capability to another process. Describe a situation**

**in which one process should be able to transfer a capability to another.**

**5. Suggest an efficient scheme for maintaining a per-user protection scheme.**

**That is, the system maintains one directory per user, and that directory lists all**

**the objects to which the user is allowed access. Your design should address the**

**needs of a system with 1000 users, of whom no more than 20 are active at any**

**time. Each user has an average of 200 permitted objects; there are 50,000 total**

**objects in the system.**

**6. Calculate the timing of password-guessing attacks:**

**(a) If passwords are three uppercase alphabetic characters long, how much**

**time would it take to determine a particular password, assuming that testing**

**an individual password requires 5 seconds? How much time if testing**

**requires 0.001 seconds?**

**(b) Argue for a particular amount of time as the starting point for “secure.”**

**That is, suppose an attacker plans to use a brute-force attack to determine a**

**password. For what value of *x* (the total amount of time to try as many**

**passwords as necessary) would the attacker find this attack prohibitively**

**long?**

**(c) If the cutoff between “insecure” and “secure” were *x* amount of time,**

**how long would a secure password have to be? State and justify your**

**assumptions regarding the character set from which the password is**

**selected and the amount of time required to test a single password.**

**7. Design a protocol by which two mutually suspicious parties can authenticate**

**each other. Your protocol should be usable the first time these parties try to**

**authenticate each other.**

**8. List three reasons people might be reluctant to use biometrics for**

**authentication. Can you think of ways to counter those objections?**

**9. False positive and false negative rates can be adjusted, and they are often**

**complementary: Lowering one raises the other. List two situations in which false**

**negatives are significantly more serious than false positives.**

**10. In a typical office, biometric authentication might be used to control access to**

**employees and registered visitors only. We know the system will have some false**

**negatives, some employees falsely denied access, so we need a human override,**

**someone who can examine the employee and allow access in spite of the failed**

**authentication. Thus, we need a human guard at the door to handle problems, as well**

**as the authentication device; without biometrics we would have had just the guard.**

**Consequently, we have the same number of personnel with or without biometrics,**

**plus we have the added cost to acquire and maintain the biometrics system. Explain**

**the security advantage in this situation that justifies the extra expense.**

**11. Outline the design of an authentication scheme that “learns.” The authentication**

**scheme would start with certain primitive information about a user, such as name and**

**password. As the use of the computing system continued, the authentication system**

**would gather such information as commonly used programming languages; dates,**

**times, and lengths of computing sessions; and use of distinctive resources. The**

**authentication challenges would become more individualized as the system learned**

**more information about the user.**

**• Your design should include a list of many pieces of information**

**about a user that the system could collect. It is permissible for the**

**system to ask an authenticated user for certain additional information,**

**such as a favorite book, to use in subsequent challenges.**

**• Your design should also consider the problem of presenting and**

**validating these challenges: Does the would-be user answer a truefalse**

**or a multiple-choice question? Does the system interpret natural**

**language prose?**

**12. How are passwords stored on your personal computer?**

**13. Describe a situation in which a weak but easy-to-use password may be adequate.**

**14. List three authentication questions (but not the answers) your credit card**

**company could ask to authenticate you over the phone. Your questions should be**

**ones to which an imposter could not readily obtain the answers. How difficult would**

**it be for you to provide the correct answer (for example, you would have to look**

**something up or you would have to do a quick arithmetical calculation)?**

**15. If you forget your password for a website and you click [Forgot my password],**

**sometimes the company sends you a new password by email but sometimes it sends**

**you your old password by email. Compare these two cases in terms of vulnerability**

**of the website owner.**

**16. Defeating authentication follows the method–opportunity–motive paradigm**

**described in Chapter 1. Discuss how these three factors apply to an attack on**

**authentication.**

**17. Suggest a source of some very long unpredictable numbers. Your source must be**

**something that both the sender and receiver can readily access but that is not obvious**

**to outsiders and not transmitted directly from sender to receiver.**

**18. What are the risks of having the United States government select a cryptosystem**

**for widespread commercial use (both inside and outside the United States). How**

**could users from outside the United States overcome some or all of these risks?**

**19. If the useful life of DES was about 20 years (1977–1999), how long do you**

**predict the useful life of AES will be? Justify your answer.**

**20. Humans are said to be the weakest link in any security system. Give an example**

**for each of the following:**

**(a) a situation in which human failure could lead to a compromise of**

**encrypted data**

**(b) a situation in which human failure could lead to a compromise of**

**identification and authentication**

**(c) a situation in which human failure could lead to a compromise of access**

**control**

**21. Why do cryptologists recommend changing the encryption key from time to**

**time? Is it the same reason security experts recommend changing a password from**

**time to time? How can one determine how frequently to change keys or passwords?**

**22. Explain why hash collisions occur. That is, why must there always be two**

**different plaintexts that have the same hash value?**

**23. What property of a hash function means that collisions are not a security**

**problem? That is, why can an attacker not capitalize on collisions and change the**

**underlying plaintext to another form whose value collides with the hash value of the**

**original plaintext?**

**24. Does a PKI perform encryption? Explain your answer.**

**25. Does a PKI use symmetric or asymmetric encryption? Explain your answer.**

**26. Should a PKI be supported on a firewall (meaning that the certificates would be**

**stored on the firewall and the firewall would distribute certificates on demand)?**

**Explain your answer.**

**27. Why does a PKI need a means to cancel or invalidate certificates? Why is it not**

**sufficient for the PKI to stop distributing a certificate after it becomes invalid?**

**28. Some people think the certificate authority for a PKI should be the government,**

**but others think certificate authorities should be private entities, such as banks,**

**corporations, or schools. What are the advantages and disadvantages of each**

**approach?**

**29. If you live in country A and receive a certificate signed by a government**

**certificate authority in country B, what conditions would cause you to trust that**

**signature as authentic?**

**30. A certificate contains an identity, a public key, and signatures attesting that the**

**public key belongs to the identity. Other fields that may be present include the**

**organization (for example, university, company, or government) to which that**

**identity belongs and perhaps suborganizations (college, department, program, branch,**

**office). What security purpose do these other fields serve, if any? Explain your**

**answer.**