Exercise Questions

1. Distinguish between vulnerability, threat, and control.
   Ans: A threat is a potential to do harm. A vulnerability is a means by which a threat agent can cause harm. A control is a protective measure that prevents a threat agent from exercising a vulnerability.

   2. Describe two examples of vulnerabilities of automobiles for which auto manufacturers have instituted controls. Tell whether you think these controls are effective, somewhat effective, or ineffective. Example answers: 5

   (1) Vulnerability: Someone drives your car away without your permission. Control: Ignition switch lock. Effectiveness: Somewhat effective because it deters casual theft, but the knowledgeable thief can "hot wire" the engine, bypassing the ignition switch. (2) Vulnerability: Someone who does not realize your car has stopped crashes into the back of your car. Control: Brake lights. Effectiveness: Reasonably good. Note the redundancy of the system: with two brake lights, even if one fails, the second one warns other drivers.

2. Preserving confidentiality, integrity, and availability of data is a restatement of the concern over interruption, interception, modification, and fabrication. How do the first three concepts relate to the last four? That is, is any of the four equivalent to one or more of the three? Is one of the three encompassed by one or more of the four? 6
   Ans: There is not a good one---to---one correspondence. Modification is primarily a failure of integrity, although there are aspects of availability (denial of service). Fabrication is probably the closest to being exclusively an integrity violation, although fabrication of covert outputs could be used to leak otherwise confidential data. Interruption is an availability concern, although one can argue that it is also a failure of the integrity of a communication or information flow. Interception primarily results in a breach of confidentiality, although it could also be seen as an attack on availability. The distinctions drawn here are primarily semantic. There are also possible arguments over whether an incident is a lack of confidentiality or integrity, too. The point is not to split hairs of categorization among the three or four terms but rather to use the terms to envision a broad range of vulnerabilities and threats.

3. 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 Per---subject access control: (a) A simple lookup from the list, which can be an O(1) operation in the average case if implemented as a hash table. (b) An addition to that subject's list, which can effectively be an O(1) operation. (c) A removal from that subject's list, which can effectively be an O(1) operation. (d) An entry needs to be added to all subjects' lists, which is an O(n) operation where n is the number of subjects. Per---object access control: (a) A simple lookup from the list, which

can effectively be an O(1) operation. (b) An addition to the list, which can effectively be an O(1) operation. (c) A removal from the list, which can effectively be an O(1) operation. (d) In this model, default access rights for an object can be set, so this, too, can be an O(1) operation. Access control matrix: (a) This is essentially a lookup by subject and object, and the speed depends on implementation, but is likely O(n). (b) Assuming the subject is being newly created, a new row must be added to the matrix, which can be quite costly depending on implementation (potentially requiring the whole table to be copied). (c) This is essentially a lookup by subject and object, and the speed depends on implementation, but is likely O(n). (d) Depending on implementation, creating a new object may require making a copy of the whole table, which would be O(n^2), or may just require adding a new entry to an existing table, which can be made to have a default entry for a performance of O(1). Capability: The capability model needs to be backed by one of the other models, so, depending on implementation, it can effectively have the same performance as any of the other models. The only potential difference is in revocation, where the need to track capability "tickets" for revocation becomes an issue.

4. 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?

   The matrix can control mode of access (e.g., read, write, delete), of which write and delete have integrity dimensions. However, the control is very coarse: the ability to write is controlled, but what is written is not controlled.

5. Defeating authentication follows the method–opportunity–motive paradigm. Discuss how these three factors apply to an attack on authentication.

   Method: There are many potential methods to defeating authentication: password guessing, brute---force attacks, biometric forgery, identity theft, guessing answers to password reset questions, etc. Opportunity: Opportunity changes depending on a variety of factors, such as how accessible the system is, how it behaves when a user fails to authenticate a number of times, what types of passwords it allows, and how the system resets lost passwords. Motive: This is typically something of value the attacker might gain from defeating the authentication. Without a motive, an attacker would have no reason to execute the attack and certainly not to pour expensive resources into it.

6. 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?

   A key may be guessed or learned, which renders all ciphertext from that point forward vulnerable. This is similar to why experts recommend changing passwords periodically. The period of key or password change should match the sensitivity of the data being encrypted: more sensitive data entails more frequent key changes.

7. Explain why hash collisions occur. That is, why must there always be two different plaintexts that have the same hash value?

   For any given hash length (e.g., 128 bits), there will always be more possible strings in the universe than there are possible hashes. Therefore, some pair of plaintexts must always hash to the same value.

8. Does a PKI perform encryption? Explain your answer.
   While a PKI takes advantage of asymmetric encryption algorithms to sign information, it does not actually encode the information to hide its meaning, so it does not perform encryption.

9. Does a PKI use symmetric or asymmetric encryption? Explain your answer.
   PKIs use asymmetric encryption algorithms to digitally sign certificates

10. 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.
    This depends on a number of factors, but primarily performance requirements and the security requirements of the certificates. For normal use cases, certificates should be created only when the creator knows the identity of the recipient with high assurance, and a fully automated distribution mechanism is therefore inappropriate.

11. The SilentBanker man-in-the-browser attack depends on malicious code that is integrated into the browser. These browser helpers are essentially unlimited in what they can do. Suggest a design by which such helpers are more rigorously controlled. Does your approach limit the usefulness of such helpers?
    Two possible answers: (a) Limit the API calls the helpers can make. (b) Allow only helpers from a curated app store, similar to Apple's App Store for iOS devices.

12. A CAPTCHA puzzle is one way to enforce that certain actions need to be carried out by a real person. However, CAPTCHAs are visual, depending not just on a person's seeing the image but also on a person's being able to recognize distorted letters and numbers. Suggest another method usable by those with limited vision.
    One very common method sites use to address this problem is playing a spoken word. If something more complicated is needed, the system can play audio of a simple math problem that any real user could solve.

13. Are computer-to-computer authentications subject to the weakness of replay? Why or why not?
    Computer---to---computer authentications are subject to the weakness of replay in the exact same ways as user---to---computer authentications, and the weakness can be mitigated in the same ways.
14. Why does a web server need to know the address, browser type, and cookies for a requesting client?
    Address: To send back requested pages/files. Type: Different browsers render differently and support different functions, so they may require different versions of files. Cookies: Web servers use cookies to track session and user information; without a cookie, the server can't know the context of the request.

15. Suggest a technique by which a browser could detect and block clickjacking attacks.
    One possible answer is for the browser to look for and block the telltale signs of clickjacking: transparent frames, for instance.

16. Is the cost, processing time, or complexity of cryptography a good justification for not using it? Why or why not?
This decision depends on a variety of contextual issues: what the system owner can afford, system performance requirements, security needs, and so on.

17. What attack is a financial institution seeking to counter by asking its customers to confirm that they see their expected security picture (a hot red sports car or a plate of cookies) before entering sensitive data?
A spoofed web page made to look like the legitimate one.

18. Give an example of the use of physical separation for security in a computing environment.
Confidential work is run on machines that are not shared. For example, confidential sales projects are run on a stand---alone microcomputer not connected to any other corporate resources.

19. Give an example of the use of temporal separation for security in a computing environment. In some secure systems, only processes of one sensitivity level are run at one time. When a batch of tasks requiring higher or lower security are to be run, all tasks are removed from the system, storage media containing sensitive data and programs are removed and new ones installed, and the operating system is rebooted.

20. Give an example of an object whose sensitivity may change during execution. One example is a printer that is used to print both confidential and nonconfidential data. Another example is a portion of unused disk space that would initially have a low sensitivity. However, once the space is assigned to an active file, it would acquire a different sensitivity value, depending on the sensitivity of the data in the file.

21. Explain how a fence register is used for relocation of a user's program.

The address in the fence register is the starting address of the user space. Thus, the user program can be written relative to address 0. Adding the fence register's contents will properly relocate the user's address references.

22. The discussion of base/bounds registers implies that program code is execute-only, and data areas are read-write-only. Is this ever not the case? Explain your answer.
Occasionally, program code must be treated as data, for example, to dump the binary value of executed machine code for very low---level debugging or to patch (update) a piece of code during its execution to make a fast repair. Some programmers design "self---modifying" code, code that overwrites a portion of itself, to optimize efficiency during execution. This type of code is extremely hard to maintain or modify, and so it is not a recommended design practice. Sometimes the instruction set of a computer will condone code modification during execution. For example, the IBM S/390 machines use an Execute instruction to modify the length field of character move and compare instructions.

23. A problem with either segmented or paged address translation is timing. Suppose a user wants to read some data from an input device into memory. For efficiency during data transfer, often the actual memory address where the data are to be placed is provided to an I/O device. The real address is passed so that time-consuming address translation does not have to be performed during a very fast data transfer. What security problems does this approach bring?
Address bounding, possibility of a process's moving while the I/O transfer is going on, possibility of forging an address or modifying it after translation but before its receipt by the I/O device, possibility of translation or transmission failure so that the I/O device receives an incorrect address. With paging, there is also the problem of the amount of data crossing a page boundary.
24. A directory is also an object to which access should be controlled. Why is it not appropriate to allow users to modify their own directories?
The user might assign himself or herself unauthorized rights to objects to which he or she has limited legitimate access. There is also an integrity problem.

25. 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?
The matrix can control mode of access (e.g., read, write, delete), of which write and delete have integrity dimensions. However, the control is very coarse: the ability to write is controlled, but what is written is not controlled.

26. List two disadvantages of using physical separation in a computing system. List two disadvantages of using temporal separation in a computing system.
Example disadvantages (of both forms of separation): inability to share, inconvenience to users, record---keeping burden, inefficient resource utilization.

27. Some operating systems perform buffered I/O. In this scheme, an output request is accepted from a user, and the user is informed of the normal I/O completion. However, the actual physical write operation is performed later, at a time convenient to the operating system. Discuss the effect of buffered I/O on integrity in a DBMS.
Because of buffered I/O, the DBMS will think a write has been completed when in fact it may not have been.

28. Explain the differences between public, private, and community clouds. What are some of the factors to consider when choosing which of the three to use?
Public clouds are available to the general public; private clouds are operated for the use of one organization; and community clouds are shared by several organizations with common needs. Some factors to consider: Which models can you afford? Are there other organizations with whom you might be able to share cloud costs? Can you afford the risks of shared infrastructure?

29. How do cloud threats differ from traditional threats? Against what threats are cloud services typically more effective than local ones?
Public and community clouds are vulnerable to the threats posed by shared infrastructure. Cloud services are often more robust to single points of failure and DoS attacks. Cloud services may also provide better security than smaller organizations that can't afford adequate security staff.

30. You run a website in an IaaS environment. You wake up to discover that your website has been defaced. Assume you are running a web server and an FTP server in this environment and that both an application proxy and a firewall sit between those servers and the Internet. All of your VMs are running SSH servers. What logs might help you determine how the website was defaced? What kind of information would you look for?
    Some possible logs to look at and the SSH connection logs, FTP logs, application proxy logs, firewall logs, and server security event logs. Look for logins, connections from unknown IP addresses, file uploads, and changes to files.

31. Name three security benefits of FIdM over requiring users to use a new set of credentials. Some possible answers:
    When a user leaves an organization and his/her primary account is deleted, he/she loses access to other services as well; the primary organization can set the authentication requirements (e.g., minimum password length) according to their standards; the primary organization can control user access to outside services in an automated way.

32. Name four services that might allow you to control a VM in an IaaS environment. What entity controls each service?
    Some possible answers that would be controlled by the customer are SSH; Remote Desktop Protocol (RDP); Virtual Network Computing (VNC); Telnet. Some possible answers that would be controlled by the service provider are Application Programming Interface (API); web console.

33. Suppose, you are designing a filter that would distinguish queries revealing sensitive data about the inquirer from those that do not reveal anything. What qualities might indicate that a query was sensitive?
    A typical answer will look for key terms that are related to sensitive attributes: social security numbers, medical records, and so on.

34. The open systems interconnection (OSI) model is inefficient; each layer must take the work of higher layers, add some result, and pass the work to lower layers. This process ends with the equivalent of a gift inside seven nested boxes, each one wrapped and sealed. Surely this wrapping (and unwrapping) is inefficient. Cite a security advantage of the layered approach.
    Example answers:
    Modularity and encapsulation, least privilege, least common mechanism.

35. TCP is a robust protocol: sequencing and error correction are assured, but there is a penalty in overhead (e.g., if no resequencing or error correction is needed). UDP does not provide these services but is correspondingly simpler. Cite specific situations in which the lightweight UDP protocol could be acceptable, that is, when error correction or sequencing is not needed.

Large quantities of somewhat redundant data. Examples are music, video, and photo imagery, in which the loss of a small proportion of packets is not perceived by the receiver but for which the volume and speed of data transfer would be affected by a protocol with high overhead.

36. Assume no FTP protocol exists. You are asked to define a function analogous to the FTP PUT for exchange of files. List three security features or mechanisms you would include in your protocol.
    (a) End---to---end error detection and perhaps correction. (b) On the receiving end control of where file is placed. (c) On the receiving end control of acknowledgment for receipt of packets. (d) Ability to resume transfer of a failed transmission "in the middle." (e) Optional end---to---end encryption for very sensitive files.

37. Explain why the onion router prevents any intermediate node from knowing the true source and destination of communication.
    Intermediate nodes do not know the source/destination of the communication to preserve anonymity. If traffic from an intermediate node is read, no information about who is communicating with whom is obtained.

38. Onion routing depends on intermediate nodes. Is it adequate for there to be only one intermediate node? Justify your answer.
    One intermediate node is insufficient—the intermediate node knows both the communication's original source and final destination, which implies fully trusting the single intermediate node. This trust is counter to the purpose of onion routing.

39. Why is segmentation recommended for network design? That is, what makes it better to have a separate network segment for web servers, one for the back-end office processing, one for testing new code, and one for system management?
    Least privilege, least common mechanism.

40. Does a VPN use link encryption or end-to-end encryption? Justify your answer.
    A VPN is point---to---point encryption. It may be on a single link, or it may tunnel through a more complex network; in the latter case it resembles end---to---end encryption.

41. Why is a firewall a good place to implement a VPN? Why not implement it at the actual server(s) being accessed?
    Typically, the firewall is positioned at the perimeter of the protected zone of an organization, such as a company's office or a particular network segment. Therefore, the firewall is an entry gate into a domain that is protected (usually both physically and logically). Encryption protection is not as necessary within the domain. The firewall represents a single entry point, and so it is efficient to install a cryptographic process (or processor) at that one point instead of having to install one at each internal server.

42. Does a VPN use symmetric or asymmetric encryption? Explain your answer.
    Typically, a VPN uses asymmetric encryption to establish a symmetric key between the two VPN end points; then the communication proceeds under symmetric encryption.

43. Do firewall rules have to be symmetric? That is, does a firewall have to block a particular traffic type both inbound (to the protected site) and outbound (from the site)? Why or why not?
    No. A firewall could, for example, allow its users to access any site but restrict incoming traffic to a single web server.

44. Firewalls are targets for penetrators. Why are there few compromises of firewalls?
Reference monitor concept: tamper resistance and correctness achieved through simple design and careful analysis.

45. Should a network administrator put a firewall in front of a honeypot? Why or why not?
Perhaps. The firewall can direct certain kinds of traffic to the honeypot (and other traffic to regular users). But the purpose of the honeypot is to be exposed, to draw attention. The firewall can make it seem to most senders (ideally including attackers) as if the honeypot is the only resource on the system.

46. Can a firewall block attacks using server scripts, such as the attack in which the user could change a price on an item offered by an e-commerce site? Why or why not?
Although the firewall could do this kind of filtering, in theory, supporting that amount of detail would add significant complexity to the firewall.