Chapter 6 - Networks

**1. In this chapter we have described sequence numbers between a sender and**

**receiver as a way to protect a communication stream against substitution and**

**replay attacks. Describe a situation in which an attacker can substitute or replay**

**in spite of sequence numbers. For which type of sequence numbering—one**

**general stream of sequence numbers or a separate stream for each pair of**

**communicators—is this attack effective?**

**2. Does a gasoline engine have a single point of failure? Does a motorized fire**

**engine? Does a fire department? How does each of the last two compensate for**

**single points of failure in the previous one(s)? Explain your answers.**

**3. Telecommunications network providers and users are concerned about the**

**single point of failure in “the last mile,” which is the single cable from the**

**network provider’s last switching station to the customer’s premises. How can a**

**customer protect against that single point of failure? Comment on whether your**

**approach presents a good cost-benefit trade-off.**

**4. You are designing a business in which you will host companies’ websites.**

**What issues can you see as single points of failure? List the resources that could**

**be involved. State ways to overcome each resource’s being a single point of**

**failure.**

**5. The human body exhibits remarkable resilience. State three examples in**

**which the body compensates for failure of single body parts.**

**6. How can hardware be designed for fault tolerance? Are these methods**

**applicable to software? Why or why not?**

**7. The old human telephone “switches” were quaint but very slow. You would**

**signal the operator and say you wanted to speak to Jill, but the operator,**

**knowing Jill was visiting Sally, would connect you there. Other than slowness or**

**inefficiency, what are two other disadvantages of this scheme?**

**8. An (analog) telephone call is “circuit based,” meaning that the system**

**chooses a wire path from sender to receiver and that path or circuit is dedicated**

**to the call until it is complete. What are two disadvantages of circuit switching?**

**9. The 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. (Proof of this slowness is**

**that the protocols that implement the Internet—TCP, UDP, and IP—are**

**represented by a four-layer architecture.) From reading earlier chapters of this**

**book, cite a security advantage of the layered approach.**

**10. Obviously, the physical layer has to be at the bottom of the OSI stack, with**

**applications at the top. Justify the order of the other five layers as moving from low**

**to high abstraction.**

**11. List the major security issues dealt with at each level of the OSI protocol stack.**

**12. What security advantage occurs from a packet’s containing the source NIC**

**address and not just the destination NIC address?**

**13. TCP is a robust protocol: Sequencing and error correction are ensured, but there**

**is a penalty in overhead (for example, 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.**

**14. 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.**

**15. A 32-bit IP addressing scheme affords approximately 4 billion addresses.**

**Compare this number to the world’s population. Every additional bit doubles the**

**number of potential addresses. Although 32 bits is becoming too small, 128 bits**

**seems excessive, even allowing for significant growth. But not all bits have to be**

**dedicated to specifying an address. Cite a security use for a few bits in an address.**

**16. When a new domain is created, for example, yourdomain.com, a table in the .com**

**domain has to receive an entry for yourdomain. What security attack might someone**

**try against the registrar of .com (the administrator of the .com table) during the**

**creation of yourdomain.com?**

**17. A port scanner is a tool useful to an attacker to identify possible vulnerabilities in**

**a potential victim’s system. Cite a situation in which someone who is not an attacker**

**could use a port scanner for a nonmalicious purpose.**

**18. One argument in the security community is that lack of diversity is itself a**

**vulnerability. For example, the two dominant browsers, Mozilla Firefox and**

**Microsoft Internet Explorer, are used by approximately 95 percent of Internet users.**

**What security risk does this control of the market introduce? Suppose there were**

**three (each with a significant share of the market). Would three negate that security**

**risk? If not, would four? Five? Explain your answers.**

**19. Compare copper wire, microwave, optical fiber, infrared, and (radio frequency)**

**wireless in their resistance to passive and active wiretapping.**

**20. Explain why the onion router prevents any intermediate node from knowing the**

**true source and destination of a communication.**

**21. Onion routing depends on intermediate nodes. Is it adequate for there to be only**

**one intermediate node? Justify your answer.**

**22. Suppose an intermediate node for onion routing were malicious, exposing the**

**source and destination of communications it forwarded. Clearly this disclosure would**

**damage the confidentiality onion routing was designed to achieve. If the malicious**

**node were one of two in the middle, what would be exposed. If it were one of three,**

**what would be lost. Explain your answer in terms of the malicious node in each of**

**the first, second, and third positions. How many nonmalicious nodes are necessary to**

**preserve privacy?**

**23. A problem with pattern matching is synonyms. If the current directory is bin, and**

**. denotes the current directory and .. its parent, then bin, ../bin, ../bin/., .././bin/../bin**

**all denote the same directory. If you are trying to block access to the bin directory in**

**a command script, you need to consider all these variants (and an infinite number**

**more). Cite a means by which a pattern-matching algorithm copes with synonyms.**

**24. The HTTP protocol is by definition stateless, meaning that it has no mechanism**

**for “remembering” data from one interaction to the next. (a) Suggest a means by**

**which you can preserve state between two HTTP calls. For example, you may send**

**the user a page of books and prices matching a user’s query, and you want to avoid**

**having to look up the price of each book again once the user chooses one to purchase.**

**(b) Suggest a means by which you can preserve some notion of state between two**

**web accesses many days apart. For example, the user may prefer prices quoted in**

**euros instead of dollars, and you want to present prices in the preferred currency next**

**time without asking the user.**

**25. How can a website distinguish between lack of capacity and a denial-of-service**

**attack? For example, websites often experience a tremendous increase in volume of**

**traffic right after an advertisement displaying the site’s URL is shown on television**

**during the broadcast of a popular sporting event. That spike in usage is the result of**

**normal access that happens to occur at the same time. How can a site determine when**

**high traffic is reasonable?**

**26. Syn flood is the result of some incomplete protocol exchange: The client initiates**

**an exchange but does not complete it. Unfortunately, these situations can also occur**

**normally. Describe a benign situation that could cause a protocol exchange to be**

**incomplete.**

**27. A distributed denial-of-service attack requires zombies running on numerous**

**machines to perform part of the attack simultaneously. If you were a system**

**administrator looking for zombies on your network, what would you look for?**

**28. Signing of mobile code is a suggested approach for addressing the vulnerability**

**of hostile code. Outline what a code-signing scheme would have to do.**

**29. The system must control applets’ accesses to sensitive system resources, such as**

**the file system, the processor, the network, and internal state variables. But the term**

**“the file system” is very broad, and useful applets usually need some persistent**

**storage. Suggest controls that could be placed on access to the file system. Your**

**answer has to be more specific than “allow all reads” or “disallow all writes.” Your**

**answer should essentially differentiate between what is “security critical” and not, or**

**“harmful” and not.**

**30. Suppose you have a high-capacity network connection coming into your home**

**and you also have a wireless network access point. Also suppose you do not use the**

**full capacity of your network connection. List three reasons you might still want to**

**prevent an outsider from obtaining free network access by intruding into your**

**wireless network.**

**31. 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 backend office**

**processing, one for testing new code, and one for system management?**

**32. For large applications, some websites use load balancers to distribute traffic**

**evenly among several equivalent servers. For example, a search engine might have a**

**massive database of content and URLs, and several front-end processors that**

**formulate queries to the database manager and format results to display to an**

**inquiring client. A load balancer would assign each incoming client request to the**

**least busy front-end processor. What is a security advantage of using a load balancer?**

**33. Can link and end-to-end encryption both be used on the same communication?**

**What would be the advantage of that? Cite a situation in which both forms of**

**encryption might be desirable.**

**34. Does a VPN use link encryption or end-to-end? Justify your answer.**

**35. Why is a firewall a good place to implement a VPN? Why not implement it at the**

**actual server(s) being accessed?**

**36. Does a VPN use symmetric or asymmetric encryption? Explain your answer.**

**37. What is the security purpose for the fields, such as sequence number, of an IPsec**

**packet?**

**38. Discuss the trade-offs between a manual challenge response system (one to which**

**the user computes the response by hand or mentally) and a system that uses a special**

**device, like a calculator.**

**39. A synchronous password token has to operate at the same pace as the receiver.**

**That is, the token has to advance to the next random number at the same time the**

**receiver advances. Because of clock imprecision, the two units will not always be**

**perfectly together; for example, the token’s clock might run 1 second per day slower**

**than the receiver’s. Over time, the accumulated difference can be significant. Suggest**

**a means by which the receiver can detect and compensate for clock drift on the part**

**of the token.**

**40. ACLs on routers slow throughput of a heavily used system resource. List two**

**advantages of using ACLs. List a situation in which you might want to block (reject)**

**certain traffic through an ACL on a router; that is, a situation in which the**

**performance penalty would not be the deciding factor.**

**41. What information might a stateful inspection firewall want to examine from**

**multiple packets?**

**42. Recall that packet reordering and reassembly occur at the transport level of the**

**TCP/IP protocol suite. A firewall will operate at a lower layer, either the Internet or**

**data layer. How can a stateful inspection firewall determine anything about a traffic**

**stream when the stream may be out of order or damaged?**

**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?**

**44. The FTP protocol is relatively easy to proxy; the firewall decides, for example,**

**whether an outsider should be able to access a particular directory in the file system**

**and issues a corresponding command to the inside file manager or responds**

**negatively to the outsider. Other protocols are not feasible to proxy. List three**

**protocols that it would be prohibitively difficult or impossible to proxy. Explain your**

**answer.**

**45. How would the content of the audit log differ for a screening router versus an**

**application proxy firewall?**

**46. Cite a reason why an organization might want two or more firewalls on a single**

**network.**

**47. Firewalls are targets for penetrators. Why are there few compromises of**

**firewalls?**

**48. Should a network administrator put a firewall in front of a honeypot (introduced**

**in Chapter 5)? Why or why not?**

**49. Can a firewall block attacks that use 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?**

**50. Why does a stealth mode IDS need a separate network to communicate alarms**

**and to accept management commands?**

**51. One form of IDS starts operation by generating an alert for every action. Over**

**time, the administrator adjusts the setting of the IDS so that common, benign**

**activities do not generate alarms. What are the advantages and disadvantages of this**

**design for an IDS?**

**52. Can encrypted email provide verification to a sender that a recipient has read an**

**email message? Why or why not?**

**53. Can message confidentiality and message integrity protection be applied to the**

**same message? Why or why not?**

**54. What are the advantages and disadvantages of an email program (such as Eudora**

**or Outlook) that automatically applies and removes protection to email messages**

**between sender and receiver?**