Review Questions

3.1 In general terms, what are four means of authenticating a user's identity?
3.2 List and briefly describe the principal threats to the secrecy of passwords.
3.3 What are two common techniques used to protect a password file?
3.4 List and briefly describe four common techniques for selecting or assigning passwords.
3.5 Explain the difference between a simple memory card and a smart card.
3.6 List and briefly describe the principal physical characteristics used for biometric identification.
3.7 In the context of biometric user authentication, explain the terms, enrollment, verification, and identification.
3.8 Define the terms false match rate and false nonmatch rate, and explain the use of a threshold in relationship to these two rates.
3.9 Describe the general concept of a challenge-response protocol.
Review Questions

4.1 Briefly define the difference between DAC and MAC.
4.2 How does RBAC relate to DAC and MAC?
4.3 List and define the three classes of subject in an access control system.
4.4 In the context of access control, what is the difference between a subject and an object?
4.5 What is an access right?
4.6 What is the difference between an access control list and a capability ticket?
4.7 What is a protection domain?
4.8 Briefly define the four RBAC models of Figure 4.8a.
4.9 List and define the four types of entities in a base model RBAC system.
4.10 Describe three types of role hierarchy constraints.
4.11 In the NIST RBAC model, what is the difference between SSD and DSD?
Review Questions

5.1 Define the terms database, database management system, and query language.
5.2 What is a relational database and what are its principal ingredients?
5.3 How many primary keys and how many foreign keys may a table have in a relational database?
5.4 List and briefly describe some administrative policies that can be used with a RDBMS.
5.5 Explain the concept of cascading authorizations.
5.6 Explain the nature of the inference threat to an RDBMS.
5.7 What are the disadvantages to database encryption?
5.8 List and briefly define three cloud service models.
5.9 What is the cloud computing reference architecture?
5.10 Describe some of the main cloud-specific security threats.
Review Questions

6.1 What are three broad mechanisms that malware can use to propagate?
6.2 What are four broad categories of payloads that malware may carry?
6.3 What characteristics of an advanced persistent threat give it that name?
6.4 What are typical phases of operation of a virus or worm?
6.5 What mechanisms can a virus use to conceal itself?
6.6 What is the difference between machine executable and macro viruses?
6.7 What means can a worm use to access remote systems to propagate?
6.8 What is a “drive-by-download” and how does it differ from a worm?
6.9 How does a Trojan enable malware to propagate? How common are Trojans on computer systems? Or on mobile platforms?
6.10 What is a “logic bomb”?
6.11 What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware?
6.12 What is the difference between a “phishing” attack and a “spear-phishing” attack, particularly in terms of who the target may be?
6.13 List some the different levels in a system that a rootkit may use.
6.14 Describe some malware countermeasure elements.
6.15 List three places malware mitigation mechanisms may be located.
6.16 Briefly describe the four generations of anti-virus software.
Review Questions

7.1 Define a denial-of-service (DoS) attack.
7.2 What types of resources are targeted by such DoS attacks?
7.3 What is the goal of a flooding attack?
7.4 What types of packets are commonly used for flooding attacks?
7.5 Why do many DoS attacks use packets with spoofed source addresses?
7.6 What is “backscatter traffic”? Which types of DoS attacks can it provide information on? Which types of attacks does it not provide any information on?
7.7 Define a distributed denial-of-service (DDoS) attack.
7.8 What architecture does a DDoS attack typically use?
7.9 Define a reflection attack.
7.10 Define an amplification attack.
7.11 What is the primary defense against many DoS attacks, and where is it implemented?
7.12 What defenses are possible against nonspoofed flooding attacks? Can such attacks be entirely prevented?
7.13 What defenses are possible against TCP SYN spoofing attacks?
7.14 What defenses are possible against a DNS amplification attack? Where must these be implemented? Which are unique to this form of attack?
7.15 What defenses are possible to prevent an organization’s systems being used as intermediaries in a broadcast amplification attack?
7.16 What do the terms slashdotted and flash crowd refer to? What is the relation between these instances of legitimate network overload and the consequences of a DoS attack?
7.17 What steps should be taken when a DoS attack is detected?
7.18 What measures are needed to trace the source of various types of packets used in a DoS attack? Are some types of packets easier to trace back to their source than others?
Review Questions

8.1 List and briefly define four classes of intruders.
8.2 List and briefly describe the steps typically used by intruders when attacking a system.
8.3 Provide an example of an activity that may occur in each of the attack steps used by an intruder.
8.4 Describe the three logical components of an IDS.
8.5 Describe the differences between a host-based IDS and a network-based IDS. How can their advantages be combined into a single system?
8.6 What are three benefits that can be provided by an IDS?
8.7 What is the difference between a false positive and a false negative in the context of an IDS?
8.8 Explain the base-rate fallacy.
8.9 List some desirable characteristics of an IDS.
8.10 What is the difference between anomaly detection and signature or heuristic intrusion detection?
8.11 List and briefly define the three broad categories of classification approaches used by anomaly detection systems.
8.12 List a number of machine-learning approaches used in anomaly detection systems.
8.13 What is the difference between signature detection and rule-based heuristic identification?
8.14 List and briefly describe some data sources used in a HIDS.
8.15 Which of anomaly HIDS or signature and heuristic HIDS are currently more commonly deployed? Why?
8.16 What advantages do a Distributed HIDS provide over a single system HIDS?
8.17 Describe the types of sensors that can be used in a NIDS.
8.18 What are possible locations for NIDS sensors?
8.19 Are either anomaly detection or signature and heuristic detection techniques or both used in NIDS?
8.20 What are some motivations for using a distributed or hybrid IDS?
8.21 What is a honeypot?
8.22 List and briefly define the two types of honeypots that may be deployed.
Review Questions

9.1 List three design goals for a firewall.
9.2 List four characteristics used by firewalls to control access and enforce a security policy.
9.3 What information is used by a typical packet filtering firewall?
9.4 What are some weaknesses of a packet filtering firewall?
9.5 What is the difference between a packet filtering firewall and a stateful inspection firewall?
9.6 What is an application-level gateway?
9.7 What is a circuit-level gateway?
9.8 What are the differences among the firewalls of Figure 9.1?
9.9 What are the common characteristics of a bastion host?
9.10 Why is it useful to have host-based firewalls?
9.11 What is a DMZ network and what types of systems would you expect to find on such networks?
9.12 What is the difference between an internal and an external firewall?
9.13 How does an IPS differ from a firewall?
9.14 What are the different places an IPS can be based?
9.15 How can an IPS attempt to block malicious activity?
9.16 How does a UTM system differ from a firewall?
Review Questions

10.1 Define buffer overflow.

10.2 List the three distinct types of locations in a process address space that buffer overflow attacks typically target.

10.3 What are the possible consequences of a buffer overflow occurring?

10.4 What are the two key elements that must be identified in order to implement a buffer overflow?

10.5 What types of programming languages are vulnerable to buffer overflows?

10.6 Describe how a stack buffer overflow attack is implemented.

10.7 Define shellcode.

10.8 What restrictions are often found in shellcode, and how can they be avoided?

10.9 Describe what a NOP sled is and how it is used in a buffer overflow attack.

10.10 List some of the different operations an attacker may design shellcode to perform.

10.11 What are the two broad categories of defenses against buffer overflows?

10.12 List and briefly describe some of the defenses against buffer overflows that can be used when compiling new programs.

10.13 List and briefly describe some of the defenses against buffer overflows that can be implemented when running existing, vulnerable programs.

10.14 Describe how a return-to-system-call attack is implemented and why it is used.

10.15 Describe how a heap buffer overflow attack is implemented.

10.16 Describe how a global data area overflow attack is implemented.
Review Questions

11.1 Define the difference between software quality and reliability and software security.
11.2 Define *defensive programming*.
11.3 List some possible sources of program input.
11.4 Define an injection attack. List some examples of injection attacks. What are the general circumstances in which injection attacks are found?
11.5 State the similarities and differences between command injection and SQL injection attacks.

11.6 Define a cross-site scripting attack. List an example of such an attack.

11.7 State the main technique used by a defensive programmer to validate assumptions about program input.

11.8 State a problem that can occur with input validation when the Unicode character set is used.

11.9 Define input fuzzing. State where this technique should be used.

11.10 List several software security concerns associated with writing safe program code.

11.11 Define race condition. State how it can occur when multiple processes access shared memory.

11.12 Identify several concerns associated with the use of environment variables by shell scripts.

11.13 Define the principle of least privilege.

11.14 Identify several issues associated with the correct creation and use of a lockfile.

11.15 Identify several issues associated with the correct creation and use of a temporary file in a shared directory.

11.16 List some problems that may result from a program sending unvalidated input from one user to another user.
Review Questions

22.1 List four functions supported by S/MIME.
22.2 What is radix-64 conversion?
22.3 Why is radix-64 conversion useful for an e-mail application?
22.4 What is DKIM?
22.5 What protocols comprise SSL?
22.6 What is the difference between and SSL connection and an SSL session?
22.7 What services are provided by the SSL Record Protocol?
22.8 What is the purpose of HTTPS?
22.9 What services are provided by IPsec?
22.10 What is an IPsec security association?
22.11 What are two ways of providing authentication in IPsec?
Review Questions

23.1 What are the principal elements of a Kerberos system?
23.2 What is Kerberos realm?
23.3 What are the differences between versions 4 and 5 of Kerberos?
23.4 What is X.509?
23.5 What key elements are included in a X.509 certificate?
23.6 What is the role of a CA in X.509?
23.7 What different types of X.509 certificates exist?
23.8 What alternatives exist to check that a X.509 certificate has not been revoked?
23.9 What is a public key infrastructure?
23.10 How do most current X.509 implementations check the validity of signatures on a certificate?
23.11 What are some key problems with current public key infrastructure implementations?
23.12 List the key elements of the PKIX model.
Review Questions

24.1 What is the basic building block of an 802.11 WLAN?
24.2 Define an extended service set.
24.3 List and briefly define IEEE 802.11 services.
24.4 Is a distribution system a wireless network?
24.5 How is the concept of an association related to that of mobility?
24.6 What security areas are addressed by IEEE 802.11i?
24.7 Briefly describe the four IEEE 802.11i phases of operation.
24.8 What is the difference between TKIP and CCMP?