浙江大学 2018－2019 学年夏学期

《信息系统安全》课程期末考试试卷

课程号：_21190160，开课学院：_计算机

考试试卷：√A 卷、B 卷

考试形式：闭、√开卷，允许带___任何纸张__入场

考试日期：_2019_年 06 月 26 日,考试时间：120 分钟

诚信考试，沉着应考，杜绝违纪。

考生姓名：______________学号：______________所属院系：_____________

总 分	
评卷人	

Instructions: each question has exactly one correct answer. Please fill in your answers in the table below. GRADING IS BASED ON THE TABLE, NOT what you write on the questions.

1	2	3	4	5	6	7	8	9	10
C	**A**	**B**	**B**	**B**	**E**	**B**	**F**	**B**	**A**
11	12	13	14	15	16	17	18	19	20
B	**B**	**C**	**D**	**C**	**A**	**C**	**B**	**A**	**D**
21	22	23	24	25	26	27	28	29	30
D	**A**	**D**	**C**	**D**	**B**	**C**	**A**	**B**	**B**
31	32	33	34	35	36	37	38	39	40
B	**B**	**A**	**E**	**F**	**B**	**D**	**C**	**E**	**C**
41	42	43	44	45	46	47	48	49	50
A	**A**	**C**	**D**	**B**	**C**	**A**	**C**	**C**	**A**

1. Buffer overflow attack exploits what attack surface?

A. Network attack surface
B. Human attack surface
C. Software attack surface
D. All of the above

ANS: ________________
C

2. DoS attack by ping flood (ICMP flood) exploits what attack surface?

A. Network attack surface
B. Human attack surface
C. Software attack surface
D. All of the above

ANS: ________________
A

3. Spear-phishing attack exploits what attack surface?

A. Network attack surface
B. Human attack surface
C. Software attack surface
D. All of the above

ANS: ________________
B

4. In the following figure for biometric authentication, what is the effect of moving the *decision threshold t* more to the **left side**?

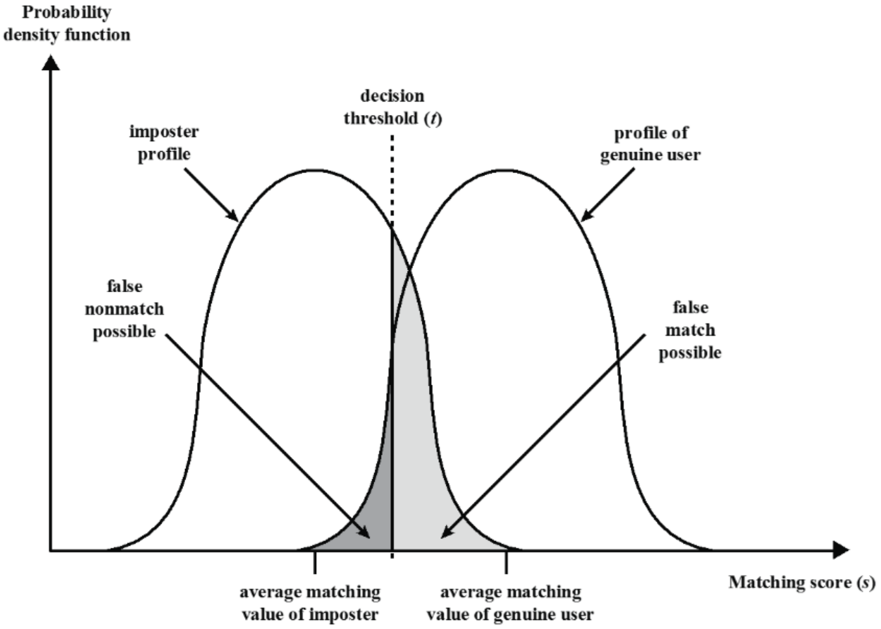


Figure 3.9 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (*s*) is greater than a preassigned threshold (*t*), a match is declared.

A. There will be more false positives, i.e., genuine users will be more likely to be identified as imposters.
B. There will be more false negatives, i.e., imposters will be more likely to be identified as genuine users.
C. It has no effect on the false positive or false negative rates.
D. None of the above

ANS: ________________
B

5. Which of the following is NOT one of the purposes of *salt* in the UNIX password file?
A. increase difficulty of offline dictionary attacks
B. improve performance of the authentication process at runtime
C. prevents duplicate passwords from being visible in the password file
D. makes it difficult to find out whether a person with passwords on two or more systems has used the same password on all of them

ANS: ________________
B

6. Consider Discretionary Access Control (DAC) on a UNIX system. Suppose user Alice is the owner of file foo, and she has control authority over user Jim (there is an entry in the Access Control Matrix "A[Alice, Jim]=control"). Which of the following commands can Alice issue?
A. grant r* to Jim, foo
B. delete r from Jim, foo
C. destroy subject Jim
D. destroy object foo
E. All of the above
F. None of the above

ANS: ________________
E

7. Consider Discretionary Access Control (DAC) on a UNIX system. Suppose user Alice is the owner of file foo, and issues the command "grant r* to Bob, foo". User Tom is another user unrelated to either Alice or Bob. Which of the following commands can Bob issue?
A. grant r* to Tom, foo
B. transfer r* to Tom, foo
C. delete r from Alice, foo
D. destroy object foo
E. All of the above
F. None of the above

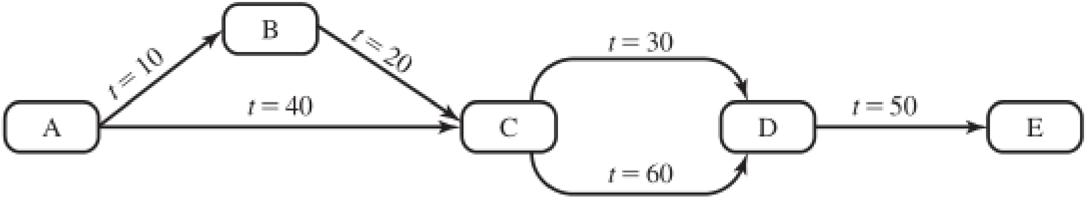
ANS: ________________
B

8. Consider Discretionary Access Control (DAC) on a UNIX system. Suppose user Alice is the owner of file foo, and issues the command "grant r to Bob, foo". User Tom is another user unrelated to either Alice or Bob. Which of the following commands can Bob issue?
A. grant r* to Tom, foo
B. transfer r* to Tom, foo
C. delete r from Alice, foo

D. destroy object foo
E. All of the above
F. None of the above

ANS: ________________
F

9. Consider SQL database access control. The graph of cascaded granting of access rights to a database table is shown below. Assume that at t = 70, B revokes the access right from C. What will happen to the downstream access rights?



A. All downstream access rights will stay valid
B. All downstream access rights will be revoked
C. The grant from C to D will stay valid; the grant from D to E will be revoked
D. The grant from D to E will stay valid; the grant from C to D will be revoked;

ANS: ________________
B

10. Consider the same graph above. Assume that at t = 70, A revokes the access right from C. What will happen to the downstream access rights?
A. All downstream access rights will stay valid
B. All downstream access rights will be revoked
C. The grant from C to D will stay valid; the grant from D to E will be revoked
D. The grant from D to E will stay valid; the grant from C to D will be revoked;

ANS: ________________
A

11. *Scanning* traffic is characteristic of which type of malware?

A. Trojans
B. Worms
C. Viruses
D. Spam
E. Clickjacking

ANS: ________________
B

12. Displaying a fake QQ or Alipay login screen to collect user login credentials and send them to the attacker is a form of
A. DoS attack
B. Phishing attack
C. Worms
D. Polymorphic virus
E. Metamorphic virus

ANS: ________________

B

13. A software developer implements a hidden functionality in an application that listens on port #12345 of the host, and accepts any incoming connection requests and commands to that port. This is an instance of

A. Virus
B. Rootkit
C. Backdoor
D. Logic bomb
E. Worms

ANS: ________________
C

14. A software developer with username “bob” implements a hidden functionality in an application that checks his home directory /home/bob upon startup, and formats the hard drive if that directory is deleted. This is an instance of

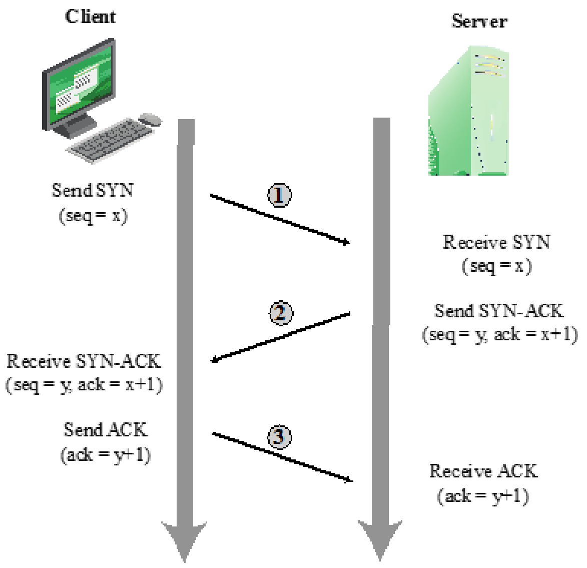
A. Virus
B. Rootkit
C. Backdoor
D. Logic bomb
E. Worms

ANS: ________________
D

15. What is a DNS amplification attack?
A. Launch a flooding attack against a DNS server, to render it unavailable to provide DNS service to DNS clients.
B. Change the DNS server configuration and redirect traffic from correct to the wrong sites in order to perform phishing attacks
C. Use a DNS server as the reflector intermediary to launch a flooding attack on some other target machines.
D. None of the above

ANS: ________________
C

16. Consider the three-way handshake protocol for TCP connection setup shown below. What is the target of the *TCP SYN spoofing* attack?



A. Server
B. Client
C. Host at the spoofed source address
D. Random host on the internet

ANS: ________________
A

17. What is the target of the *TCP SYN flood* attack?
A. Server
B. Client
C. Host at the spoofed source address
D. Random host on the internet

ANS: ________________
C

18. True or false: in *TCP SYN spoofing* attack, the attacker's network must have higher bandwidth than the victim's network in order to carry out the attack successfully.
A. True
B. False

ANS: ________________

B

19. True or false: in *TCP SYN flood* attack, the attacker's network must have higher bandwidth than the victim's network in order to carry out the attack successfully.
A. True
B. False

ANS: ________________

A

20. Which types of memory locations in the address space of a process may be target of buffer overflow attack?
A. The stack
B. The heap
C. The data section
D. All of the above
E. None of the above

ANS: ________________
D

21. Possible consequences of a buffer overflow attack include:
A. Corruption of data used by the program
B. Unexpected transfer of control flow in the program
C. Possible memory access violation
D. All of the above

ANS: ________________
D

22. What does the *tiny fragment* attack do?
A. Intruder uses IP fragmentation to create very small packets, in order to circumvent filtering rules that depend on TCP header information.
B. Intruder uses IP fragmentation to create very small packets, in order to circumvent filtering rules that depend on IP header information.
C. Intruder uses IP fragmentation to create very small packets, in order to increase the packet handling workload on the server to launch a DoS attack
D. Intruder uses IP fragmentation to create very small packets, in order to cause a buffer overflow on the server

ANS: ________________
A

23. Which of the following is NOT true about a stateful inspection firewall?
A. May keep track of open TCP connections
B. May keep track of TCP sequence numbers of open TCP connections
C. Has higher runtime overhead than a packet filtering firewall
D. Has lower runtime overhead than a packet filtering firewall

ANS: ________________
D

24. For a company with both an internal firewall and an external firewall, which of the following is NOT one of the purposes of the internal firewall?
A. Adds more stringent filtering capability, compared to the external firewall
B. Provides two-way protection with respect to the DMZ
C. Protect the external firewall from DDoS attacks
D. Multiple internal firewalls can be used to protect portions of the internal network from each other.

ANS: ________________
C

25. Where should IPSec (tunnel mode) functionality be placed with regard to firewalls?
A. Should be outside the external firewall

B. Should be inside the external firewall, but outside the internal firewall
C. Should be inside the internal firewall
D. Should be implemented as a functionality within the firewall machine

ANS: ________________
D

26. Which of the following is NOT one of the areas protected by a Host-based Intrusion Protection System?
A. System calls
B. Deep packet inspection
C. File system access
D. System registry settings
E. Host input/output

ANS: ________________
B

27. Which of the following is NOT one of the methods for identifying malicious packets by a network-based Intrusion Prevention System?
A. Pattern matching
B. Stateful matching
C. System call inspection
D. Traffic anomaly
E. Statistical anomaly

ANS: ________________

C

28. Which of the following statement describes Snort and Snort Inline?
A. Snort is an intrusion detection system, while Snort Inline is an intrusion prevention system
B. Snort is an intrusion prevention system, while Snort Inline is an intrusion detection system
C. They are both intrusion detection systems
D. They are both intrusion prevention systems
E. They are attack kits that can be used to assemble powerful attacks

ANS: ________________
A

29. Which of the following is NOT true about a high-interaction honeypot, compared to a low-interaction honeypot?
A. provides a more realistic target that may occupy an attacker for an extended period
B. requires much less resources, hence easier to set up
C. if compromised could be used to initiate attacks on other systems
D. is a real system with full OS, services and applications

ANS: ________________

B

30. Which of the following is NOT one of the data sources for a Host-based Intrusion Detection System?
A. System call traces

B. Packet IP address and port number
C. Audit logs
D. File integrity checksums
E. Registry access

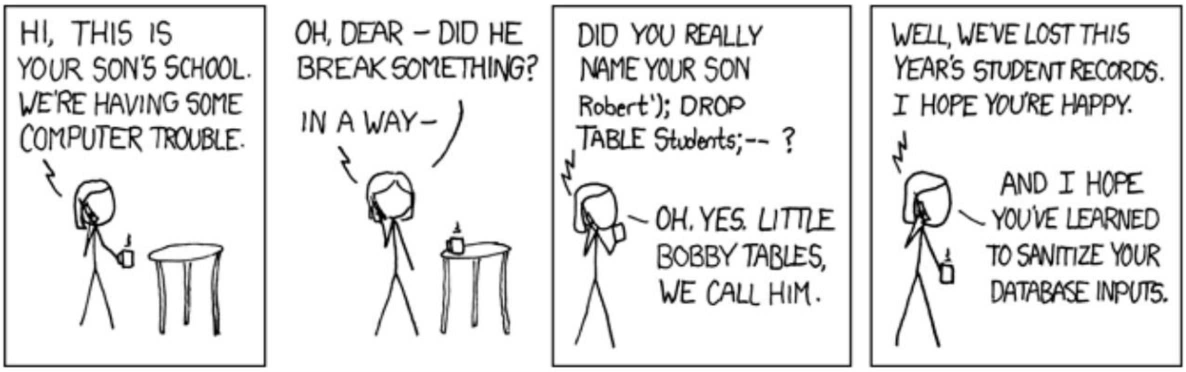
ANS: ________________

B

31. What does the call *mysql_real_escape_string()* do, in order to prevent injection attacks?
A. Perform input validation, and die if the string contains unexpected characters
B. Prepend backslashes before certain special characters in the input string
C. Append backslashes after certain special characters in the input string
D. Delete certain special characters from the input string

ANS: ________________
B

32. The following cartoon illustrates what type of attack?


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

A. TCP syn flood attack
B. SQL injection attack
C. SiP flood attack
D. Phishing attack
E. Spear phishing attack

ANS: ________________
B

33. The BLP security model stipulates that:
A. Process at security level k can read objects at security levels k or lower
B. Process at security level k can read objects at security levels k or higher
C. Process at security level k can only read objects at security level k
D. None of the above

ANS: ________________

A

34. In a system that implements the BLP security model (Fig. 13.2), how can the teacher Dirk (with high security level c1-t) create an exam document *based on an existing template file at high security level*, and give read access to the student Carla (with low security level c1-s)?
A. This is not possible

B. Dirk can access the system in Student role and create the exam document at low security level c1-s
C. Dirk can access the system in Teacher role and create the exam document at low security level c1-s
D. Dirk can access the system in Teacher role and create the exam document at high security level c1-t, then downgrade it to low security level c1-s
E. Dirk can access the system in Teacher role and create the exam document at high security level c1-t, then ask the administrator to downgrade it to low security level c1-s
F. Either B or E is OK
G. Either C or D is OK

ANS: ________________
E

35. In a system that implements the BLP security model (Fig. 13.2), how can the teacher Dirk (with high security level) create a new exam document *from scratch (not based on any template file)* and give read access to the student Carla (with low security level)?
A. This is not possible
B. Dirk can access the system in Student role and create the exam document at low security level c1-s
C. Dirk can access the system in Teacher role and create the exam document at low security level c1-s
D. Dirk can access the system in Teacher role and create the exam document at high security level c1-t, then downgrade it to low security level c1-s
E. Dirk can access the system in Teacher role and create the exam document at high security level c1-t, then ask the administrator to downgrade it to low security level c1-s
F. Either B or E is OK
G. Either C or D is OK

ANS: ________________
F

36. The Biba integrity model stipulates:
A. Process at integrity level k can read objects at integrity levels k or lower
B. Process at integrity level k can read objects at integrity levels k or higher
C. Process at integrity level k can only read objects at integrity level k
D. None of the above

ANS: ________________
B

37. If a high-integrity process reads low-integrity file and writes high-integrity file, which of the following property is violated?

A. Simple security property in BLP model
B. * property in BLP model
C. Simple integrity property in Biba model
D. Integrity * property in Biba model

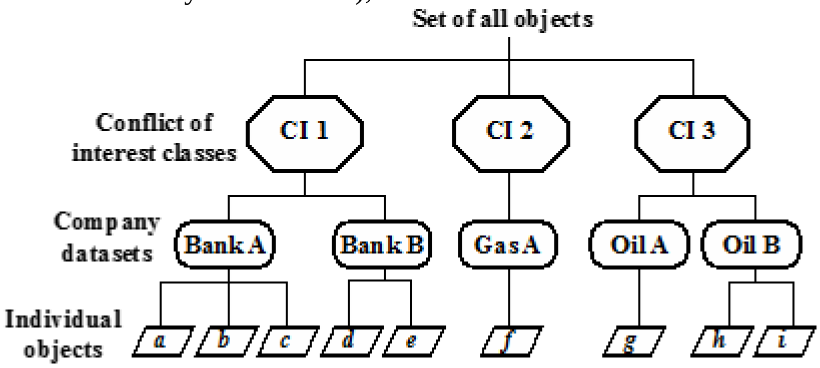
ANS: ________________
D

38. The Chinese Wall (CW) Model is designed to provide:

A. Confidentiality
B. Integrity
C. No conflict of interest
D. Authenticity

ANS: ________________
C

39. With the CW model, consider the following example datasets for banks, gas companies and oil companies. If John has access to dataset of Bank A (we don't know if he has access to any other dataset), then we can infer that:



A. John has read-only access to dataset of only Bank A
B. John has read-write access to dataset of only Bank A
C. John has read-only access to datasets of Bank A and Oil A
D. John has read-write access to datasets of Bank A and Oil A
E. John has no access to dataset of Bank B

ANS: ________________
E

40. Consider the same model and datasets above. If John has access to datasets of both Bank A and Oil A (we don't know if he has access to any other dataset), then we can infer that:
A. John has read-only access to dataset of only Bank A
B. John has read-write access to dataset of only Bank A
C. John has read-only access to datasets of Bank A and Oil A
D. John has read-write access to datasets of Bank A and Oil A
E. John has no access to dataset of Gas A

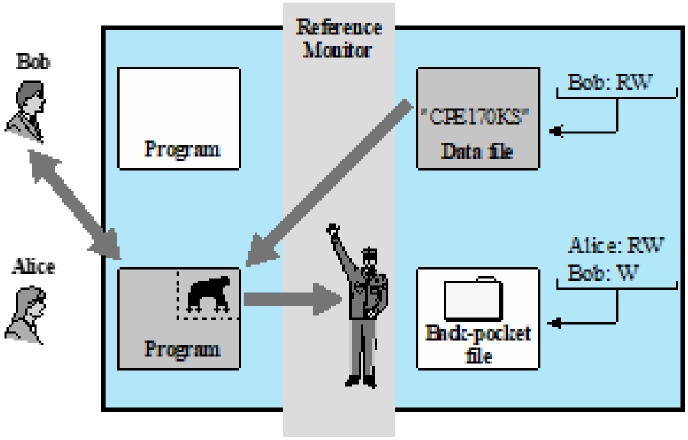
ANS: ________________
C

41. Inserting a new row into a database table at a lower security level, without modifying the existing row with the same primary key at the higher security level, is known as:

A. Polyinstantiation
B. ss-property
C. * property
D. Discretionary Access Control
E. Mandatory Access Control

ANS: ________________
A

42. In CH13, Figure 13.8(d), one link of the Trojan horse copy-and-observe-later chain is broken by the reference monitor. There are two other possible angles of attack by Alice: (1) Alice logging on and attempting to read the string directly from the data file, and (2) Alice assigning a high security level of sensitive to the back-pocket file. Does the reference monitor prevent these attacks?



(d)

A. Yes, it prevents both attacks
B. No, it does not prevent these attacks
C. It prevents (1), but not (2).
D. It prevents (2), but not (1).

ANS: ________________
A

43. Which of the following is NOT one of the services of the Trusted Platform Module (TPM)?

A. Authenticated boot
B. Certification
C. Host-based firewall
D. Encryption
E. Decryption

ANS: ________________
C

44. Which of the following is NOT part of a TPM?
A. Random number generator
B. Crypto coprocessor
C. HMAC engine
D. Virtual Machine Monitor or hypervisor
E. Key generation

ANS: ________________
D

45. Meltdown and Spectre are CPU bugs at which level
A. Device and circuit level
B. CPU Micro-architecture level
C. OS-level
D. Virtualization-level

E. Communication middleware-level

ANS: ________________
B

46. Flush-and-Reload Cache Side Channel Analysis can be used to
A. Install rootkit or other malware in the victim’s machine
B. Turn the victim’s machine into a zombie to launch DDoS attacks
C. Find out a secret value held by the victim by measuring variable access time
D. Find out a secret value held by the victim by guessing his/her password
E. Find out the victim’s password by rainbow attack on the passwd file

ANS: ________________
C

47. Meltdown attack can be used to:
A. Read from kernel memory addresses from a user-level program
B. Write to kernel memory addresses from a user-level program
C. Read memory addresses not permitted by program control flow
D. Write to memory addresses not permitted by program control flow
E. All of the above

ANS: ________________
A

48. Spectre attack can be used to:
A. Read from kernel memory addresses from a user-level program
B. Write to kernel memory addresses from a user-level program
C. Read memory addresses not permitted by program control flow
D. Write to memory addresses not permitted by program control flow
E. All of the above

ANS: ________________
C

49. Adding array bounds check before accessing array elements can prevent which type of attack?
A. TCP SYN spoofing attack
B. DDoS attack
C. Buffer overflow attack
D. Meltdown attack
E. Spectre attack

ANS: ________________
C

50. In Spectre attack, for the following function, assuming variable x=10. Which statement is true, after the function finishes execution?

```
unsigned int buffer_size = 10;
uint8_t buffer[10]={0,1,2,3,4,5,6,7,8,9};
uint8_t restrictedAccess(size_t x) {
if (x < buffer_size)
{ return buffer[x]; }
else { return 0;
}
```

A. The function always returns 0
B. The function always returns the memory content at buffer[10]
C. There is a race condition, and the function sometimes returns buffer[10], and sometimes returns 0,
D. The function will give an “array-out-of-bounds” exception

ANS: ________________
A