浙江大学 2018－2019 学年冬学期

《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 01 月 24 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**	**C**	**A**	**B**	**B**	**D**	**B**	**B**	**C**
11	12	13	14	15	16	17	18	19	20
A	**A**	**B**	**A**	**C**	**D**	**A**	**D**	**C**	**D**
21	22	23	24	25	26	27	28	29	30
B	**C**	**B**	**B**	**D**	**B**	**B**	**B**	**B**	**C**
31	32	33	34	35	36	37	38	39	40
B	**A**	**A**	**B**	**B**	**D**	**C**	**A**	**A**	**A**
41	42	43	44	45	46	47	48	49	50
C	**D**	**B**	**C**	**C**	**A**	**D**	**A**	**C**	**A**

1. Buffer overflow attack works by exploiting which 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 flooding ping command works by exploiting which attack surface?

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

ANS: ________________
A

3. Which of the following is NOT a symmetric encryption algorithm?

A. DES
B. Triple DES
C. SHA-1
D. AES

ANS: ________________
C

4. Which of the following is NOT a public-key cryptography algorithm?

A. MD5
B. RSA
C. Diffe-Hellman
D. Elliptic Curve Cryptography

ANS: ________________
A

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

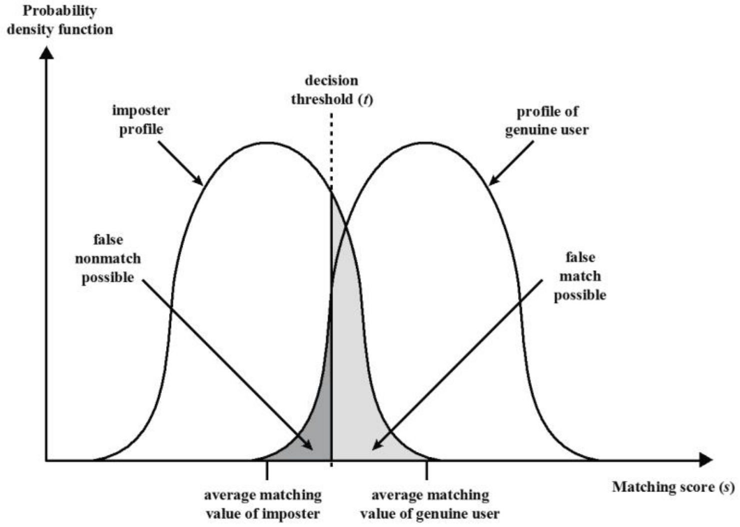


Figure 3.9 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

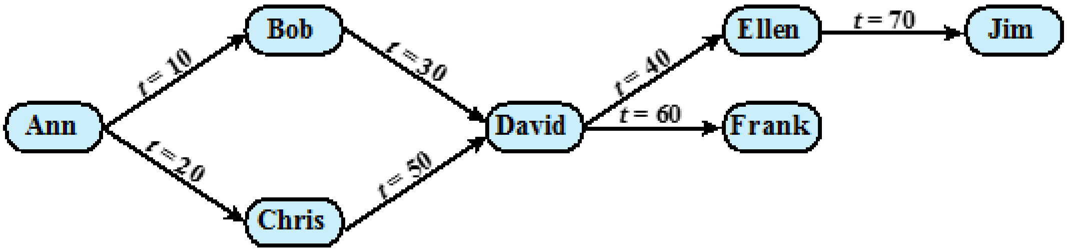
A. There will be more false positives, i.e., genuine users will be more likely to be identified as imposters.
B. There will be more false negatives, i.e., imposters will be more likely to be identified as genuine users.
C. It has no effect on the false positive or false negative rates.
D. None of the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

ANS: ________________
B

6. 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

7. Consider the graph of cascaded granting of access rights below, where Ann grants the access right to Bob at time t = 10 and to Chris at time t = 20, and so on. If sometime later, *Chris revokes access rights from David*, what will happen to the access rights granted by David to Ellen, and access rights granted by David to Frank?



A. Access rights granted by David to Ellen should be revoked, and access rights granted by David to Frank should stay valid
B. Access rights granted by David to Ellen should stay valid, and access rights granted by David to Frank should be revoked
C. Both should be revoked
D. Both should stay valid

ANS: ________________
D

8. *Scanning* traffic is characteristic of which type of malware?
A. Trojans
B. Worms
C. Viruses
D. Spam
E. Clickjacking

ANS: ________________
B

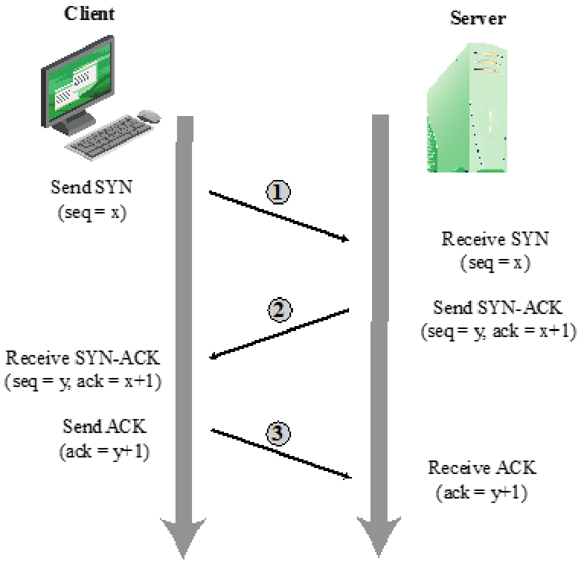
9. Displaying a fake QQ or Alipay login screen to collect user login credentials and send them to the attacker is a form of
A. DoS attack
B. Phishing attack
C. Worm
D. Polymorphic virus
E. Metamorphic virus

ANS: ________________
B

10. 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

11. 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

12. 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: ________________
A

13. 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

14. 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

15. Why does the attacker need to spoof the sender IP address in TCP SYN spoofing attack?

A. So that the backscatter traffic does not overwhelm the attacker’s own network
B. So that the server under attack cannot identify source of the attack
C. Both of the above
D. None of the above

ANS: ________________
C

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

ANS: ________________
D

17. 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

18. Which of the following is NOT true about a stateful inspection firewall?
A. May record information about open TCP connections
B. May inspect data for protocols like FTP commands
C. May keep track of TCP sequence numbers
D. Is more efficient than a packet filtering firewall

ANS: ________________
D

19. 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

20. Where should IPSec 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

21. 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

22. 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

23. 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

24. 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

25. What does the OpenSSL Heartbleed attack do?
A. Install a rootkit in the system
B. Install a Trojan in the system and open up a backdoor for attacks

C. Use buffer overflow to hijack control flow to execute shell code
D. Request a large number of bytes from the server, hopefully containing valuable information.

ANS: ________________

D

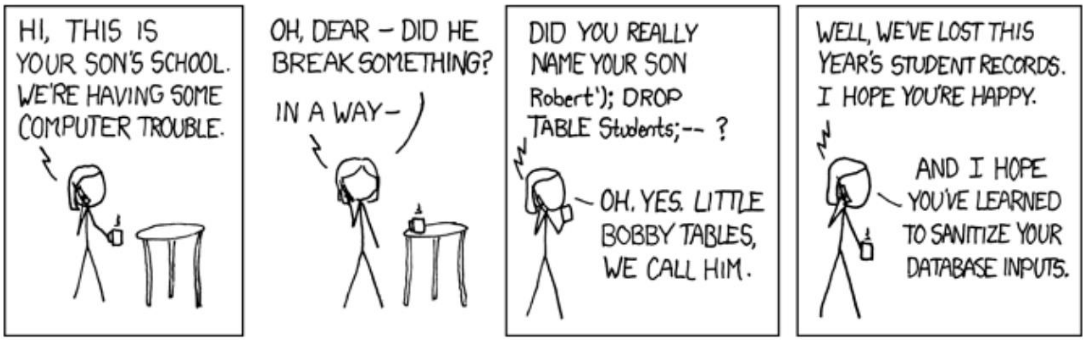
26. Consider the SQL query
SELECT * FROM users WHERE user=$userID AND password=$passwd
What happens if someone enters the input of ***blah' OR true*** in the password field for a specific *userID* (assuming the actual password is not *blah* for *userID*).
A. The password does not match, and the SQL query returns NULL.
B. The password matches, and the SQL query returns the tuple for *userID*
C. It is unknown if the password matches or not.
D. None of the above.

ANS: ________________
B

27. 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 to certain special characters
C. Append backslashes to certain special characters
D. Delete certain special characters

ANS: ________________
B

28. 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. Amplification attack
E. Reflection attack

ANS: ________________
B

29. Why is it necessary to compare source code and assembly/machine code for software security?
A. to ensure that the source code is not modified by the attacker

B. to prevent attacks due to malicious compilers
C. to ensure that the programmer follows good programming conventions.
D. all of the above

ANS: ________________
B

30. Consider the following shell script. It is vulnerable to what type of attack?

```
#!/bin/bash
grep $1 /var/local/accounts/ipaddrs
```

A. SQL injection
B. Modification of the IFS environment variable
C. Modification of the PATH environment variable to point to the attacker's version of grep
D. Modification of the LD_LIBRARY_PATH environment variable to point to the attacker's version of dynamic library
E. Buffer overflow

ANS: ________________
C

31. Consider the following shell script. It is vulnerable to what type of attack?

```
#!/bin/bash
PATH=”/sbin:/bin:/usr/sbin:/usr/bin”
export PATH
grep $1 /var/local/accounts/ipaddrs
```

A. SQL injection
B. Modification of the IFS environment variable
C. Modification of the PATH environment variable to point to the attacker's version of grep
D. Modification of the LD_LIBRARY_PATH environment variable to point to the attacker's version of dynamic library
E. Buffer overflow

ANS: ________________
B

32. What is the security vulnerability of a program that creates temporary files with file names based on process ID plus an incrementing counter?
A. The attacker can easily guess the temp file name and create a fake temp file
B. The temp file may be too large to fit in the directory /tmp
C. The temp file may be overwritten by some other program
D. The temp file may be deleted before it is used

ANS: ________________
A

33. According to the BLP security model:
A. Process at security level k can only read objects at security levels k or lower (read down)
B. Process at security level k can only read objects at security levels k or higher (read up)
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, how can a teacher give read access of an exam document (with high security level) to students (with low security level)?
A. It is not possible
B. It can be done outside of the BLP model by an administrator
C. It can be done within the BLP model
D. None of the above

ANS: ________________
B

35. According to the Biba integrity model:
A. Process at integrity level k can only read objects at integrity levels k or lower (read down)
B. Process at integrity level k can only read objects at integrity levels k or higher (read up)
C. Process at integrity level k can only read objects at integrity level k
D. None of the above

ANS: ________________
B

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

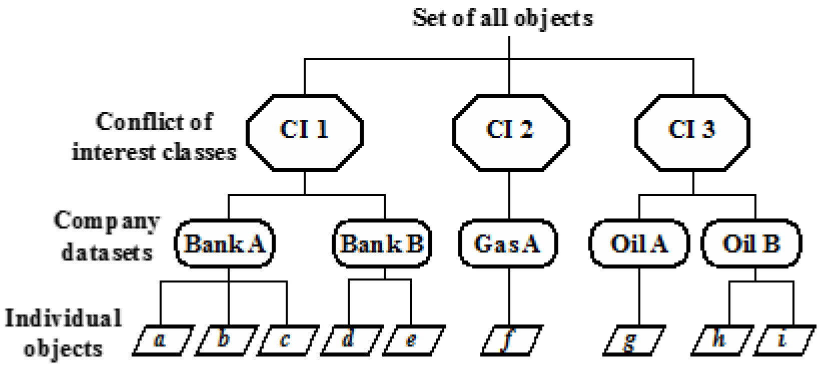
A. Simple security property in BLP model
B. * property in BLP model
C. Simple integrity property in Biba model
D. Integrity * property in Biba model

ANS: ________________
D

37. The Chinese Wall Model is designed to provide:
A. Confidentiality
B. Integrity
C. No conflict of interest
D. Authenticity

ANS: ________________
C

38. Consider the following example datasets for banks, gas companies and oil companies with the Chinese Wall Model. If John has access to dataset of Bank A, then we can infer that:



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

ANS: ________________
A

39. Consider the same datasets above. If John has access to datasets of Bank A and Oil A, then we can infer that:
A. John has read-only access to datasets of Bank A and Oil A
B. John has write-only access to datasets of Bank A and Oil A
C. John has read-write access to datasets of Bank A and Oil A
D. John has no access to dataset of Gas A

ANS: ________________
A

40. Inserting a new row into a database table at a lower security level without modifying the existing row 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

41. 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

42. Which of the following is NOT part of a TPM?

A. Random number generator
B. Crypto coprocessor
C. HMAC engine
D. Virtual machine monitor
E. Key generation

ANS: ________________
D

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

ANS: ________________
B

44. 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

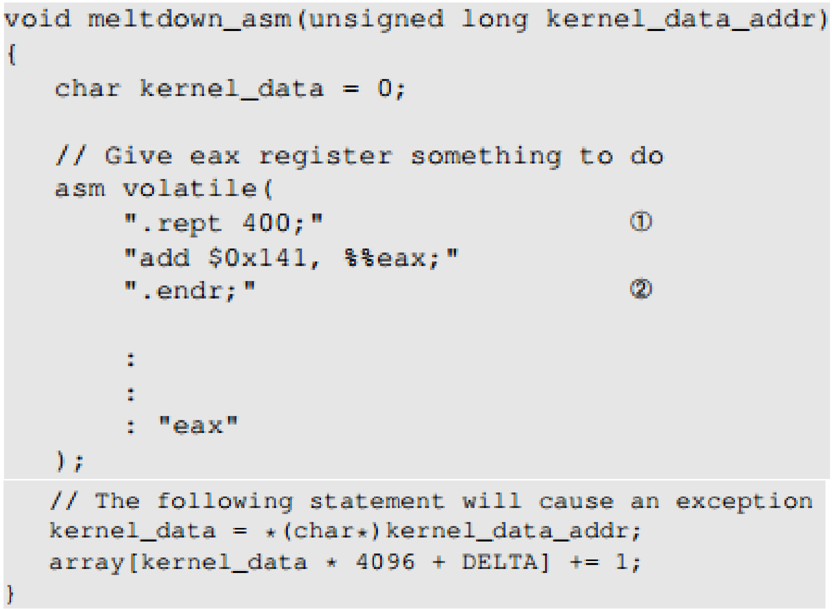
45. In Flush-and-Reload Cache Side Channel Analysis, the purpose of using array[k*4096 + DELTA] instead of array[k*4096] is:
A. To make the array occupy less memory space
B. To prevent array-out-of-bounds errors
C. To add a buffer to absorb any cache prefetching when accessing variables in adjacent memory addresses smaller than &a[0]
D. To make the cache block larger

ANS: ________________
C

46. Meltdown attack can be used to:
A. Read kernel memory from a user-level program
B. Write to kernel memory from a user-level program
C. Read the /etc/passwd file on Linux
D. Delete the passwd file without user's knowledge to have DoS attack
E. Remove the user's access permissions by modifying the capability list

ANS: ________________
A

47. In Meltdown attack, "Task 7.3: Using Assembly Code to Trigger Meltdown", what is the purpose of adding the function meltdown_asm() before the attack?



```
void meltdown_asm(unsigned long kernel_data_addr)
{
   char kernel_data = 0;

   // Give eax register something to do
   asm volatile(
       ".rept 400;"                ①
       "add $0x141, %%eax;"
       ".endr;"                    ②

       :
       :
       : "eax"
   );
   // The following statement will cause an exception
   kernel_data = *(char*)kernel_data_addr;
   array[kernel_data * 4096 + DELTA] += 1;
}
```

A. To delay execution of memory access “array[…]+=1”, and decrease the chance of success of Meltdown attack
B. To delay execution of memory access “array[…]+=1”, and increase the chance of success of Meltdown attack
C. To delay execution of permission check, and decrease the chance of success of Meltdown attack
D. To delay execution of permission check, and increase the chance of success of Meltdown attack

ANS: ________________
D

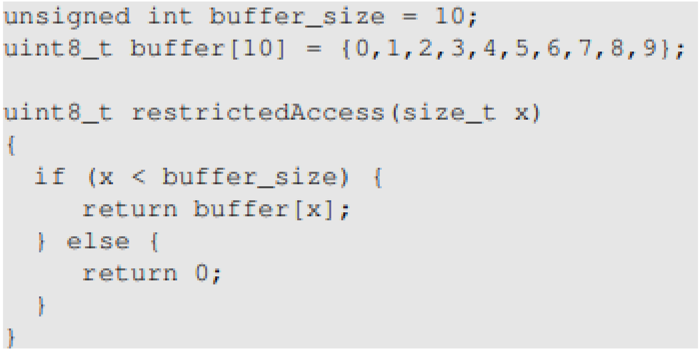
48. Spectre attack can be used to:
A. Read memory addresses not permitted by program logic
B. Write to memory addresses not permitted by program logic
C. Install a micro-architecture rootkit in the CPU
D. Delete the passwd file without user’s knowledge to have DoS attack
E. Add a virus to a legitimate program

ANS: ________________
A

49. Adding array bounds check before accessing array elements can prevent which type of attack:
A. Meltdown attack
B. Spectre attack
C. Buffer overflow attack
D. Integer overflow attack

ANS: ________________
C

50. For the following function restrictedAccess() which statement is true, after the condition (x<buffer_size) has been checked, and if x=10:



```
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 buffer[10]
C. The function sometimes returns buffer[10], and sometimes returns 0
D. The function will give an “array-out-of-bounds” error

ANS: ________________
A