جامعة الأميرة سمية للتكنولوجيا
PSUT
Princess Sumaya University for Technology

Information Systems Security (11464)
Final Exam, Fall 2017/2018

Jan 30, 2018

Time Allowed: 60 minutes

Instructor Name: .....

Section Time: _____

Student Name: _____

Student Number: | | | | | | | | |

Question	Points	Score
1	9	
2	5	
3	3	
4	8	
5	5	
6	4	
7	6	
Total	40	

Note that try to show your calculations for needed questions

Question (1): Circle the correct answer:**(9 Points)**

1. **_____ controls access based on comparing security labels with security clearances.**
   a) MAC b) DAC c) RBAC
   d) ABAC e) All of the above

2. **In which model is a user is granted permissions to a resource by being placed on an access control list (ACL)?**
   a) MAC b) DAC c) RBAC
   d) ABAC e) All of the above

3. **which model is based on resource ownership?**
   a) MAC b) DAC c) RBAC
   d) ABAC e) All of the above

4. **. _____ is based on the roles the users assume in a system rather than the user's identity.**
   a) MAC b) DAC c) RBAC
   d) ABAC e) All of the above

5. **_____ implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance.**
   a) Audit control b) Resource control c) System control
   d) Access control e) All of the above

6. **_____ is the granting of a right or permission to a system entity to access a system resource.**
   a) Authorization b) Authentication c) Control
   d) Monitoring e) All of the above

7. **The principal attraction of _____ compared to RSA is that it appears to offer equal security for a far smaller bit size, thereby reducing processing overhead.**
   a) MD5 b) Al-Gamal c) ECC
   d) Diffie-Hellman e) None of the above

8. **_____ control determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.**
   a) Behavior b) User c) Service
   d) Direction e) None of the above

9. **One of the following cannot be considered as behavioural biometric.**
   a) Gait b) Voice c) Iris Pattern
   d) Typing pattern e) All of the above

10. A single encryption error in one block is cascaded through to the following blocks, this is a drawback of:

a) CBC b) ECB c) Stream ciphers

d) Block cipher e) All of the above

11. The science of breaking codes and ciphers is _____

a) Cryptography b) Cryptology c) Encryption

d) Cryptanalysis e) All of the above

12. The branch of science concerned with the concealment of information

a) Cryptography b) Cryptology c) Encryption

d) Cryptanalysis e) All of the above

13. _____ take a long time to break, but they also tend to be more difficult to use.

a) Caesar Ciphers b) Transposition Ciphers c) Strong Ciphers

d) Weak Ciphers e) All of the above

14. Encryption provides mechanisms for checking the _____ of data to ensure that it has not been tampered with.

a) Security b) confidentiality c) secrecy

d) integrity e) All of the above

15. How many different arrangements would be possible using the letters of the word "product" ?

a) 5040 b) 2520 c) 1260

d) 840 e) All of the above

16. _____ encryption uses a key that is identical in length to the plaintext, and is used only once.

a) one-time b) traditional c) one-time pad

d) one-time key e) All of the above

17. Encryption provides mechanisms for _____ ensuring that the identities of people are correct.

a) security b) confidentiality c) authentication

d) integrity e) All of the above

18. Using a computer that can perform 10^{12} calculations a second, roughly how long would it take to try all possible permutations of 10 different letters?

a) 3.6 microsecond b) 1.8 microsecond c) 3.6 nanosecond

d) 1.8 nanosecond e) None of the above

Question (2): (5 Points)

a) Explain the principle of least privilege

b) What does the following protocol prove to Bob about the party claiming to be Alice? What does it prove to "Alice" about Bob? (KAB is a shared key between Alice and Bob)

A→B: "I'm Alice"

B→A: E (K_{AB}, R)

A→B R

Answer:

Question (3): (3 Points) LinkedIn confirmed that it had experienced a data breach that likely compromised the e-mail addresses and passwords of 6.5 million of its users. This confirmation followed the posting of the password hashes for these users in a public forum. One criticism of LinkedIn is that they used unsalted password hashes. In this question, we'll explore this criticism. Assume that each stolen password record had two fields in it: [user_email, Hash (password)] and that a user login would be verified by looking up the appropriate record based on user_email, and then checking if the corresponding hashed password field matched the hash of the password inputted by the user trying to log in. By contrast, if LinkedIn had used a salted scheme, then each record would have had three fields: [user_email, salt, Hash (password + salt)] and login verification would similarly require looking up the salt and using it when matching hashes. Given this:

a) Suppose the attacker's goal is to break your password via a dictionary attack. Does the lack of salting in LinkedIn's scheme make this goal substantially easier?

b) Suppose the attacker's goal is to break at least half of the passwords via a dictionary attack. Does the lack of salting in this scheme make this goal substantially easier?

c) Suppose you are contacted by the attacker and given a set of password hashes (that's it, no user_name, no salt). Assuming the hash function is known, is there a measurement you could make in order to infer if the hashes are likely salted or not?

Topic: Access Control

Question (4) (8 Points): Choose two questions from (a, b or c)

a) What is the difference between authentication and authorization. (2 Point)
Answer:

b) List and define the three classes of subject in an access control system. (2 Points)
Answer:

c) By using MAC answer the following question. Suppose that the clearance for "data.txt" file is CONFIDENTIAL [A, B, C, D]. Identify the status of each subject if he can read and/or write that file. (2 Points)

Clearance for subjects	Read	Reason, if can't	Write	Reason, if can't
SECRET [A, B, C, E]				
UNCLASSIFIED [A, C]				
TOP SECRET [A, B, C, D]				
CONFIDENTIAL [A, B, C]				
SECRET [A, B, C, D]				

d) Alice can read and write to the file filex.sys, can read the file filey.sys, and can execute the file filez.sys. Bob can read and write to filey.sys, and cannot access filez.sys or filex.sys.

i. Write the associated access control matrix? **(2 Points)**

ii. Write a set of access control lists for this situation. Which list is associated with which file? **(1 Points)**

iii. Write a set of capability lists for this situation. With what is each list associated? **(1 Points)**

Topic: Firewall

Question (5) (**5 Points)**

a) Discuss the three design goals for a firewall. (3 Points)

b) What is the difference between a packet filtering firewall and a stateful inspection firewall? (2 Points)

Topic: Modern Encryption Technique (SDES, AES)

Question (6): (4 Points)

Using S-DES key generation, generate the k1 and K2 using the key (0110110101), Show intermediate results after each function. **(3 Points)**

Topic: Public Key Cryptography (RSA, Diffie-Hellman and Number Theory)

Question 7: (6 Points)

Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root $\alpha = 2$. Answer the following questions: (4 Points)

a) **Show that 6 is a primitive root of 11**

b) **If user A has private key $X_A = 3$, What is A's public key Y_A ?**

c) **If user B has private key $X_B = 6$, What is B's public key Y_B?**

d) **What is the shared secret key?**

Appendix:
The English alphabitcal order: a b c d e f g h i j k l m n o p q r s t u v w x y z

S-DES

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

E/P							
4	1	2	3	2	3	4	1

P4			
2	4	3	1

S0 =

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	**3**	2

S1 =

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	**2**	1	0	3