Quiz #5

Security and Privacy
Oct. 11, 2018

Name: **Student Number:**

1. Users can generally trust the identity in a certificate more because _____.

(A) the identity is protected in the certificate for confidentiality 10 (19%)
(B) the identity can never be obtained by unauthorized users
(C) the certificate is signed by a certificate authority (CA) 43 (81%)
(D) the identity can never be modified while it is in use
(E) none of the above

2. The main reason for applying a hash function to protecting passwords that reside in the server storage is because the hash function can _____.

(A) compute very fast
(B) be easily obtained
(C) be used to encryption and decrypt passwords 6 (12%)
(D) help to prevent attackers from getting the original passwords 47 (88%)
(E) none of the above

3. Authentication with a password that is generated using a random number generator belongs to the method of _____.

(A) what the user knows 22 (42%)
(B) what the user has 26 (49%)
(C) what the user is 5 (9%)
(D) where the user is
(E) none of the above

4. Which of the following is definitely NOT a sensible way of protecting passwords from the point of view of the user?

(A) Assigning a random password to the user. 42 (79%)
(B) Asking the user to answer some alternative security questions when the supplied password is determined to be incorrect. 6 (12%)
(C) Requiring the user to choose a longer password.
(D) Requiring the user to compose a complex password
(E) None of the above 5 (9%)

5. In Challenge and Response, the use of a mobile phone to calculate a response to be sent to the authentication system based on a challenge from the authentication system for authentication belongs to the method of _____.

(A) what the user knows 9 (17%)
(B) what the user has 27 (51%)
(C) what the user is 8 (15%)
(D) where the user is 8 (15%)
(E) none of the above 1 (2%)

6. **In the Kerberos authentication protocol, the ticket sent by a user to a server for authentication to the server is constructed by _____.**

(A)	the user	
(B)	the server to be accessed	10 (19%)
(C)	a server that acts as a trusted third party	42 (79%)
(D)	none of the above	1 (2%)

7. **In the Kerberos authentication protocol, the authenticator sent by a user to a server for authentication to the server is constructed by _____.**

(A)	the user	46 (86%)
(B)	the server to be accessed	1 (2%)
(C)	a server that acts as a trusted third party	6 (12%)
(D)	none of the above	

8. **In the Kerberos authentication protocol, a user would successfully pass the authentication to a server by _____.**

(A)	sending the correct password to AS for verification	3 (6%)
(B)	asking the AS to send the password to the user for verification	2 (4%)
(C)	possessing the correct password or key that is shared with the server	48 (90%)
(D)	none of the above	

Honor List (in alphabetical order): 15 (28%)

Crown 毕诗旋 蔡亦华 冯泽琛 李雨承 马天嘉 苗雨驰

Raman 苏立梓 孙兢谦 陶宁 王品 王涛 吴亦锟 周佳慧

Absentees (in alphabetical order): 2 (4%)

王飞鸿 吴瑀

Best performance: 5 quizzes in total

4 times: 冯泽琛 苏立梓

3 times: 蔡亦华 李雨承 姚健菁