M2A1Solution CSS 211/ CS 459 Spring 2020 Covers: Chapter 2 of textbook

DATE Assigned: January 28, 2020 DATE Due: Feb. 3, 2020 POINTS: 41

[A, 35 points ] Multiple Choice:

[A1] The property of accurate identification is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.(a)

(a) authentication (b) access control (c) cryptography

[A2] Allowing only authorized accesses is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.(b)

(a) authentication (b) access control (c) cryptography

[A3] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a tool that can transform data so only intended receivers could

decipher it. (c)

(a) authentication (b) access control (c) cryptography

[A4] Asserting who a person is, is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) Identification (b) authentication

[A5] Verifying that a person is who he says he is, is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) Identification (b) authentication

[A6] Identities are \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) public (b) private

[A7] Authentication should be \_\_\_\_\_\_\_\_\_\_. (b)

(a) public (b) private

[A8] Authentication using passwords is based on something one \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) knows (b) has (c) is

[A9] Authentication using biometrics is based on something one \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (c)

(a) knows (b) has (c) is

[A10] Authentication using badges, physical keys, or a driver’s license is based on something one \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) knows (b) has (c) is

[A11] Operating systems store passwords in their \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ form. (b)

(a) public (b) encrypted

[A12] n-factor authentication , with large n, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ lead to reduced security. (a)

(a) can (b) cannot

[A13] False positive means \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) incorrectly confirming an identity (b) incorrectly denying an identity

[A14] False negative means \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) incorrectly confirming an identity (b) incorrectly denying an identity

[A15] To overcome copying of physical tokens,\_\_\_\_\_\_\_\_\_\_\_\_ should be used. (b)

(a) static (b) dynamic

[A16] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ unifies the identification and authentication process for a group of systems. (a)

(a) Federated Identity Management (b) Single sign-on

[A17] \_\_\_\_\_\_\_\_\_\_\_\_\_ takes over sign-on and authentication to several independent systems for a user. (b)

(a) Federated Identity Management (b) Single sign-on

[A18] Limiting who can access what in what ways , is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (d)

(a) Authentication (b)Identification (c) Access Mode (d) Access Control

[A19] A reference monitor is a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) notion (b) tool that you can buy and plug into a port

[A20] In an Access Control Matrix, rows correspond to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) subjects (b) objects (c) access rights

[A21] In an Access Control Matrix, columns correspond to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) subjects (b) objects (c) access rights

[A22] In an Access Control Matrix, entries correspond to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (c)

(a) subjects (b) objects (c) access rights

[A23] An access control list is a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of the access control matrix. (b)

(a) row (b) column

[A24] A capabilities list is a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of the access control matrix. (a)

(a) row (b) column

[A25] Role based access control lets us associate access privileges with \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) individuals (b) groups

[A26] In symmetric encryption ,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) a single key is used for both encryption and decryption

(b) one key encrypts, a different key decrypts

[A27] In asymmetric encryption ,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) a single key is used for both encryption and decryption

(b) one key encrypts, a different key decrypts

[A28] \_\_\_\_\_\_\_\_\_\_\_\_\_\_ encryption requires a means of key distribution. (a)

(a) Symmetric encryption

(b) Asymmetric encryption

[A29] Encryption and decryption algorithms are \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) kept secret (b) widely publicized

[A30] The DES and AES algorithms deal with \_\_\_\_\_\_\_\_\_\_\_\_\_ key encryption and decryption. (a)

(a) symmetric (b) asymmetric

[A31] The RSA Public Key system employs \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ key encryption and decryption. (b)

(a) symmetric (b) asymmetric

[A32] To encrypt and decrypt large amounts of data, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ key cryptography should

be used. (a)

(a) symmetric (b) asymmetric

[A33] To encrypt and decrypt small amounts of data, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ key cryptography can

be used. (b)

(a) symmetric (b) asymmetric

[A34] Checksums and one-way hash functions are used for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) error detection (b) authentication

[A35] Digital signatures are used for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) error detection (b) authentication

[B, 6 points ] True/False

[B1] Biometric authentication is not perfect, but is used as long as the rate of false positives and

false negatives is low. (T)

[B2] A reference monitor can be bypassed. (F)

[B3] A reference monitor cannot be tampered with. (T)

[B4] A reference monitor can be verified. (T)

[B5] An access control matrix is usually not a sparse matrix.(F)

[B6] Public key cryptography can be used to exchange symmetric keys or secret keys. (T)