M8A1Solution CSS 211/ CS 459 Spring 2020 Covers: Chapter 8 of textbook

DATE ASSIGNED: March 17, 2020 DATE DUE: March 30, 2020 POINTS: 25

[A, 14 points] Multiple Choice

[A1] If you have constant high-bandwidth data transfers between your local servers and your cloud, you

should prefer a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ cloud. (a) private

(a) private (b) public

[A2] If your data and functions have very strict confidentiality and integrity requirements, you should prefer a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ cloud. (a) private

(a) private (b) public

[A3] The most standardized of the three service models is the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ service model. (a)IaaS

(a) Iaas (b)PaaS (c) SaaS

[A4] The Cloud Revolution is driven mostly by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.(a)economics

(a)economics (b)technology

[A5] During the cloud migration process, perhaps the most fundamental security-related decision is

choosing a cloud \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ model. (a)

(a) deployment (b) service

[A6] For protecting data confidentiality in a public cloud, the minimum requirement is a \_\_\_\_\_\_\_\_\_\_

key encryption algorithm with an individual encryption key for each user. (b) symmetric

(a)asymmetric (b)symmetric

[A7] FIdM uses \_\_\_\_\_\_\_\_\_ to handle authentication , authorization, and single sign-on for users and systems. (a) SAML

(a) SAML (b) OAuth 2.0

[A8] FIdM uses \_\_\_\_\_\_\_\_\_ to authorize third-party applications to access API’s on a user’s behalf. (b) OAuth 2.0

(a) SAML (b) OAuth 2.0

[A9] OIDC is built on top of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b) OAuth 2.0

(a) SAML (b) OAuth 2.0

[A10]OAuth 2.0 and OIDC support \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ . (b) browsers as well as native applications

(a) browsers (b) browsers as well as native applications

[A11] Service models for the cloud are : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) IaaS, Paas, SaaS (b) Public, Private, Hybrid, Community

[A12] Deployment models for the cloud are: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) IaaS, Paas, SaaS (b) Public, Private, Hybrid, Community

[A13] Cloud providers embracing the “Trust No One” (TNO)philosophy do not store \_\_\_\_\_\_\_\_\_ to

access encrypted user data. (a)

(a) keys (b) passwords

[A14] Cloud storage can be thought of as a service, with the acronym \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) STaaS (b) SaaS (c) PaaS

[B, 11 points] For each of the following, state if it is TRUE or FALSE.

[B1] Cloud computing does not suffer from the “single point of failure” problem. (T)

[B2] A private cloud is usually more expensive than a public cloud. (T)

[B3] Vendor lock-in cannot become a security issue for cloud applications. (F)

[B4] Migrating your application to the cloud cannot improve the security of the application.(F)

[B5] Email filtering is a task suitable for a cloud-based security service. (T)

[B6]Cloud-based Security Services can protect your Cloud Application from a DDoS attack. (T)

[B7] Cloud-based Security Services can provide Network Monitoring for your Cloud. (T)

[B8] Logical data controls are usually adequate to prevent customers of a cloud service provider from

accessing one another’s data. (F)

[B9]Cloud identity challenges can be dealt with effectively, using Federated Identity Management. (T)

[B10] SAML assumes that its clients are browsers. (T)

[B11] SLAs usually guarantee service uptime as a percentage of total time. (T)