M1A1Solution CSS 211/ CS 459 Spring 2020 Covers: Chapter 1 of textbook

DATE Assigned: January 21, 2020 DATE Due: January 27, 2020 POINTS: 30

[A, 20 points ] Multiple Choice:

[A1] Computer system assets that have value and deserve security protection are: \_\_\_\_\_\_\_\_\_\_\_\_\_\_. (d)

(a) Hardware (b) Software (c) Data (d) Hardware, Software and Data

[A2] Off the shelf hardware and software assets are \_\_\_\_\_\_\_\_\_\_\_\_\_ . (a)

(a) replaceable (b) irreplacable

[A3] Individual applications, and data are \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) replaceable (b) irreplaceable

[A4] A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a weakness that can be exploited to cause harm. (a)

(a) vulnerability (b) threat

[A5] A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a set of circumstances that could cause harm. (b)

(a) vulnerability (b) threat

[A6] A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ prevents a threat from exercising a vulnerability. (a)

(a) control (b) worm (c) virus

[A7] The Confidentiality requirement from the CIA triad suffers if the following harm occurs:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) interception (b) interruption (c) modification or fabrication

[A7] The Integrity requirement from the CIA triad suffers if the following harm occurs:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (c)

(a) interception (b) interruption (c) modification or fabrication

[A8] The Availability requirement from the CIA triad suffers if the following harm occurs:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) interception (b) interruption (c) modification or fabrication

[A9] When a person, process, or program is (or is not) authorized to access a data item in a particular

way, we call the person, process or program a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) subject (b) object (c) access mode (d) policy

[A10] When a person, process, or program is (or is not) authorized to access a data item in a particular

way, we call the data item an \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) subject (b) object (c) access mode (d) policy

[A11] When a person, process, or program is (or is not) authorized to access a data item in a particular

way, we call the kind of access an \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (c)

(a) subject (b) object (c) access mode (d) policy

[A12] When a person, process, or program is (or is not) authorized to access a data item in a particular

way, we call the authorization a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (d)

(a) subject (b) object (c) access mode (d) policy

[A13] Threats are caused by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (c)

(a) humans (b) non-humans (c) both humans and non-humans

[A14] Threats caused by humans fall into two categories: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) benign or malicious (b) direct or indirect

[A15] Malicious threats caused by humans fall into two categories: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) directed or random (b) direct or indirect

[A16] Risk management becomes necessary because funds available for computer security are

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) limited (b) more than adequate

[A17] Amount of money spent on computer security depends on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (c)

(a) impact of potential harm (b) likelihood of potential harm

(c) impact and likelihood of potential harm

[A18] Locks, human guards, sprinklers and fire extinguishers are examples of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ controls. (a)

(a) physical (b) procedural or administrative (c) technical

[A19] Laws, regulations, policies, copyrights and contracts are examples of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ controls.(b)

(a) physical (b) procedural or administrative (c) technical

[A20] Network Protocols, firewalls, and encryption are examples of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ controls.(c)

(a) physical (b) procedural or administrative (c) technical

[B, 10 points ] True/False

[B1] A paradigm of Computer Security is Access Control. (T)

[B2] All attackers match a single pattern. (F)

[B3] Hackers are honest, law-abiding persons. (T)

[B4] Many hackers display characteristics of Aspberger Syndrome. (T)

[B5] Attacks can be launched by individuals, organized groups, organized crime groups, or terrorists. (T)

[B6] Impact of potential harm can be measured precisely. (F)

[B7] Likelihood of potential harm can be measured precisely. (F)

[B8] In the absence of a method, an attack cannot succeed. (T)

[B9] In the absence of an opportunity, an attack cannot succeed. (T)

[B10] In the absence of a motive, an attack cannot succeed. (T)