M3A1Solution CSS 211/ CS 459 Spring 2020 Covers: Chapter 3 of textbook

DATE Assigned: February 4, 2020 DATE Due: Feb. 10, 2020 POINTS: 40

[A, 10 points ] Multiple Choice:

[A1] A fault is an \_\_\_\_\_\_\_\_\_\_\_\_\_ view of the system. (a)

(a) inside (b) outside

[A2] A failure is an \_\_\_\_\_\_\_\_\_\_\_\_\_ view of the system. (b)

(a) inside (b) outside

[A3] The \_\_\_\_\_\_\_\_\_\_\_\_\_ is a key data structure necessary for interchange of data between procedures. (a)

(a) stack (b)heap

[A4] The \_\_\_\_\_\_\_\_\_\_\_\_\_ provides space for dynamic data. (b)

(a) stack (b)heap

[A5] Input data is best validated on the \_\_\_\_\_\_\_\_\_\_\_\_\_ side. (a)

(a) client (b) server

[A6] Many security problems can be avoided by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ mediation. (a)

(a) complete (b) incomplete

[A7] A word size of 8 bits \_\_\_\_\_\_\_\_\_\_\_\_\_\_ hold an unsigned integer value of 256. (b)

(a) can (b) cannot

[A8]A program that on the surface has a useful purpose, but also has undocumented malicious

features is called a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ . (a)

(a) Trojan horse (b) virus (c) worm

[A9]A malicious program that does harm on one computer and that attempts to spread to other computers is called a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ . (b)

(a) Trojan horse (b) virus (c) worm

[A10] A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ requires a network to spread itself. (c)

(a) Trojan horse (b) virus (c) worm

[B, 30 points ] True/False

For each of the following, state if it is TRUE or FALSE.

[B1] Buffer overflows are usually a result of innocent programmer oversight. (T)

[B2] Buffer overflows cannot be exploited by a malicious programmer to cause harm. (F)

[B3] Buffer overflow attacks are not data driven attacks. (F)

[B4] Java and Python programming languages check bounds before storing data. (T)

[B5] C and C++ programming languages check bounds before storing data. (F)

[B6] The time-of-check to time-of-use (TOCTTOU) flaw can be prevented if the access checking

software owns the request data until the requested action is complete. (T)

[B7] Race conditions, Off-by-one errors, Integer overflows, are innocent programmer oversights that can

lead to failure of security. (T)

[B8] Malicious code is a recent phenomenon ; it started after the web became available. (F)

[B9] Malicious code in interpretive data like a document file or a spreadsheet cannot lead to

failure of security. (F)

[B10] Boot sectors and code libraries are excellent places for malicious code to hide. (T)

[B11] The signature of malicious code can be altered by the malicious code writer, to make detection difficult, by introducing no-ops (no operations) into the code. (T)

[B12] Whereas most requirements say, “the system will do this,” security requirements add the phrase

“and nothing more.” (T)

[B13] Regression testing is not important for security purposes. (F)

[B14] Design by Contract involves stating preconditions, post-conditions and invariants for each module. (T)

[B15] Penetrate-and-Patch is an effective countermeasure. (F)

[B16] Security-through-obscurity is an effective countermeasure. (F)

[B17] Complexity is often the enemy of security. (T)

[B18] Defensive Programming can help improve security. (T)

[B19] Formal methods cannot improve the quality of software. (F)

[B20] Tiger Team Analysis, Penetration Testing, and Ethical Hacking are synonyms. (T)

[B21] A fault can reside in any development or maintenance product. (T)

[B22] Bit patterns can represent data or instructions. (T)

[B23] Security engineers use the term ‘flaw’ to describe both faults and failures. (T)

[B24] A requirements document can contain faults. (T)

[B25] Easter egg code is usually harmful. (F)

[B26] Undocumented access points are not a security risk. (F)

[B27] Null terminated strings can lead to buffer overflows. (T)

[B28] Language libraries may provide unsafe utility programs. (T)

[B29] Race conditions are not a security threat. (F)

[B30] Correct code is a security objective. (T)