CS 458 — Assignment 1

Thomas Lim Jun Wei - 20700973

January 25, 2017

Question 1

Part A

Confidentiality. Attacker have access to system that is for authorised party to perform its DDOS attack.

Part B

Integrity. Test results should be right and correct to the pharma company to improve the drugs.

Part C

Privacy. Banking password is considered informational self-determination. Hence, it should be only for the user to control information about themselves. Leaving the attacker to brute force guesses password and viewing the user record is a compromise of this scenario.

Question 2

Threat 1

Interception: In TCP/IP layer, where packets would travel across network between the authors and system, there might be hijacking occurring by attacker where they intercepts the network traffic and gather sensitive information. To resolve, one defence can be protecting the data packet by secure encryption to make it unreadable for unauthorised parties.

Threat 2

Interruption: Attacker perform a distributed denial of service (DDOS) attack on the system. Where it interrupt the flow for an author to submit their confidential papers, making it unavailable. Deterring such attack can be done by ISP/hosing company to divert malicious packets before they are sent to the system web server.

Threat 3

Modification: An attacker with unauthorised access the system and modify systems integrity and tamper with information of authors confidential paper thru brute force password guessing. This alteration would result to denying certain user to access the system by changing password, etc. Prevention can be done by introducing hardware control such as smart token to generate one time pin as secondary login control to prevent authorised access from attacker

Threat 4

Fabrication: Web bugs such as adware message prompted to user can be a threat to the system as it might post fake message by attacker to create loss of authenticity and integrity of a message. To prevent such threat, the system might impose software control such as virus scanners behind the system to watch for web bugs.

Question 3

Part A

Based on a statistical data from average cost of cybercrime in selected countries from https://www.statista.com/ cyber-crime-costs-to-companies-in-selected-countries/ , the average cost of cybercrime in United States cost roughly $17.36 million, compared to the article quote of 15.4$ million. These numbers are consider rather unrealistic as another source from CBS addressing there are roughly 1.5 million annual cyber-attacks in the year 2015 and nearly three attacks every minute. This articles clearly address and demonstrated the numbers and costs might be unrealistic.

Part B

One key practices that the article misses out is importance of cryptography. Applying such method do help to ensure data integrity by making data unreadable and only users authorised users with digital signature are able to access. For e-commerce sectors, one good practice can be applying cryptographic protocol to authenticate each transaction made.

Part C

IoT is defined as Internet of Things, in this case, the article is addressing the home appliance being pervasive to intrusion of privacy. In this case, it could be manifested by attacker gaining access by penetrating through brute-force. Once entered, its relatively easy to access other physical devices that are connected to same network.

Part D

Patch and updating everything and maintain up-to-date are difference in small aspect such as patching is mainly for OS and applications and maintain up-to-date is for antivirus software. An antivirus-software is a subset of an application. Hence its part of small aspect while its similarity is its characteristic of keeping the application updated with patches to deter any new bugs.

Sploits

Sploit 1

This is a buffer overflow exploit. Firstly, I setup the payload size to be 280. Next, by configuring args[0] to be fill the array of size 280 and its sfp with garbage. After which, by adding additional of 4 more byte to the array, where it contain the address of VM's shellcode. args[1] will contain "-h". The shellcode itself will be set to args[2]. This vulnerability can be fixed by patching its array size limit to not be greater than is memory size

Sploit 2

This is a format string exploit. The target section is aimed at "sprintf" function for msg[80+1] line. the payload size is set to 280 similar to sploit 1. Together with 90 NOP, i padded 4 btyes of "A" to the string target at stack address of 135 and 136.However, I am unable to complete and exploit to root and spent more than 14 hours in figuring out to attack setuid via format string vulnerability. To protect against this vulnerability, I would suggest the use checks to accept format strings before output.

Sploit 3

Even though I do not have time to developed the 3th sploit, I would suggest that an possible attack is to another format string exploit at check$_forbidden$().