CS 458 A1

Patrick Wong 20317267

Contents: Q1-3, description of sploit3 and sploit4

[Question 1]

(a) Confidentiality and privacy are compromised. Spying software violates the definition of confidentiality: "access to systems or data is limited to authorized parties." The software circumvents the requirement that the phone's access is limited to authorized parties. Furthermore, victim's private information is now accessed illicitly.
(b) Privacy is compromised. A person's demographic is highly sensitive information and it is given away without consent.
(c) Confidentiality and privacy are being compromised. An unauthorized person bypasses the website's security systems (confidentiality violated) and then acquires sensitive personal information about the website's users (privacy violated).
(d) Confidentiality and integrity are being compromised here. The car is being accessed by unauthorized people – a violation of confidentiality, and the integrity of the car's system has changed, which may also change expected results during normal usage of the car – a violation of integrity.
(e) Integrity is being compromised. Users receive unexpected and undesirable results – the subjection of unwanted malware.
(f) Availability is compromised. The world is reliant on the internet at every second of the day, and this availability is being violated by lizards.

[Question 2(a)]

Theft of Medication

People who are not the intended recipient of some medication may steal it for their own personal use or profit. This is the **interception** of the delivery of medication. Example: the abuse of painkillers for recreational use - NFL coach Sean Payton named in a lawsuit alleging abuse of Vicodin.

Dwindling Supply

Some medications may experience shortages due to problems arising during production. People will suffer from these shortages if they are reliant on their medication being used at regularly scheduled intervals. This is the **interruption** of the delivery of medication. Example: an experimental drug's production cancelled, despite the existence of a person who benefits from said drug.

Diluted Medication

People who receive a medicine intravenously may have their dosage diluted due a variety of factors, i.e. difficulty in measuring the dosage, patient discomfort, monetary reasons. This is the **modification** of a medication's dosage or contents. Source: Institute for Safe Medicine Practices.

Counterfeit Medicine

People may procure fake medication for illicit reasons, i.e. financial gain. This is the **fabrication** of medication. Example: criminals profiting on the uneducated and/or people seeking cheaper alternatives.

[Question 2(b)]

Defense against theft – Detection

Through accounting and monitoring the channels where medicine is delivered, it can be determined where and who is receiving the medication. Faulty points in the channel can be inspected if it is suspected of theft, and suitable actions can be taken after and during the investigation.

Defense against dwindling supply – Deflection

If it is known that a particular medication may experience shortage, there should be alternative treatments available to the affected.

Defense against diluted medication – Prevention

Government regulations and hospital protocols need to be followed to ensure the correct delivery of medication to patients. Penalties should exist to deter those diluting medication, i.e. malpractice lawsuits.

Defense against counterfeit medication – deterrence

The production of counterfeit is a crime for various reasons – and the penalties from running counterfeit operations are lengthy prison sentences and severe fines.

[Question 3]

Duqu (2011)

Duqu is a Trojan, as it creates a backdoor in Windows computers and gives attackers elevated privileges. The methods of infection are unknown. It targets a Microsoft Word vulnerability in its TrueType font parsing engine to execute its code.

ZeuS

ZeuS is a Trojan. It is downloaded when compromised websites are accessed, or through phishing scams via email or social media in which unsuspecting people click on links in the email or social media.

Conficker

Conficker is a worm. One method of propagation is from an already infected Windows computer, spreading to computers that are on the same network. It can also spread by attaching itself to USB devices and when the USB device is used on another computer, it infects the new coputer.

Cryptowall

Cryptowall is ransomware. Its method of infection is by Trojan, attached in spam emails.

sploit3

sploit3 exploits a format string vulnerability in submit's check_forbidden function. The attack is a format string, prefixed with the address of printf's stack pointer. The middle contains the shellcode, followed by offsets from the address of the stack pointer which points to the beginning of the shell code. This address is written in two parts, because $n can only write half of the address, and it is written at the address of the initial stack pointer.

sploit4 (incomplete)

sploit4 exploits a format string vulnerability in submit's print_version function. The method of attack is the same as sploit3, a format string containing the address of printf's stack pointer, followed by shell code, and offsets that point to the location of the shell code in memory, writing it at the address of the stack pointer.