Assignment 1

1)

a.

- Integrity is being violated because the malware overwrites “rm” binary to prevent user from uninstalling the malware.

- The method of spread is Trojan by tricking the user into running it and giving it administrator privileges.

- The effect on the system of the malware is the same as Rootkits where granting control over computational cycle and overwriting “rm” binary.

b.

- Integrity and availability are being violated because the attackers encrypted all data that cause users access the files.

- The method of spread is Worm which it spreads with the EternalBlue exploit by using specially crafted packet targeting vulnerable background daemons.

- The effect on the system of the malware is like Ransomware that causes disruption to the service and must pay money to the attacker.

c.

- Confidentiality is being violated because the attackers receive secret information of victim employees’ actions and steal unlock codes for AT&T phones.

- The method of spread is planted malware which bribed AT&T employees to install malwares in the company’s computers.

- The effect on the system of the malware is type of Spyware because the malware installs to allow recording employees’ actions on computers and sending them to attackers.

2)

a. True. Based on Saltzer and Schroeder’s Principle of Secure Design, the cryptoprotocols rely on open design to allow community to find bugs and fix them immediately. Hackers could access your code even if you did not make it public so that it would damage your source code in case you did not find your bugs before them.

b. True. The buffer overflow attacks caused by memory management of programs written in a specific language. Since all programs share the same common mechanism, the attacks become more powerful. For example, the virus exploits a buffer overflow in glibc which will cause all programs written in C produces the virus.

c. False. The Android and iOS follow the least privilege principle which allow minimum access to normal user and grant maximal access only for root user. When the app need accesses to OS-owned app such as Calendar, Phone, Notes they need to ask user for permissions for accessing them.

d. False. The attacker does not have to gain full control of the web server. The attacker just needs to obtain identity of existing user then insert malicious coding into a link where it sends GET request with user identity to your bank account, for example, to take your money.

e. True. A format string vulnerability gives buffer and buffer overflow since attacker exploits memcpy function that read oversized input as well as overwrite the input into the next memory locations.

3)

In the 1900, computers were not widely used in every household because it was luxurious to own one and restricted in use in some countries. Computers read floppy disks or CDs in order to interact with the world to obtain information. The only method malwares could spread during this time was embedded in disks. This was a reason during the early 2000 where most floppy disks and CDs contain viruses or worms that could harm computers. Until the development of WorldWideWeb and web browsers where users could search for information, write personal blogs, share professional documents in a faster way. Computer became popular all over the world in the 2000s. Viruses and worms started to die out because users no longer used disks to insert new data. From the boom of WorldWideWeb to now, all information is available online through applications where users could download directly. The Zeus Trojan was released which taking over thousands of banking details and stealing million dollars in the 2008. It caused significant damages to users and brought attention to cyber security aspect of web applications. People are more aware of cyber attacks as well as the importance of protecting their personal data. In recent years, developments on data security show good progress on keeping us safe. Web applications are encrypted and applied multi-factor authentication to combat against attackers. Data transmitting protocols offer both secret keys and public keys encryptions. In the last 20 years, security features are becoming significant part of all computer systems that follow Saltzer and Schroeder's Principle of Secure Design which encourage open design to public for bugs finding, web hostings from several data centers, give minimum privileges to users on controlling

systems. The NSA also established 10 cybersecurity mitigation strategies for individuals to tackle attacks which minimize the loss of data and money. These strategies raise awareness into every individual in the community and online users becomes cautious on what they are about to download or click on.