CMPT 479 Assignment 1

Written Assignment

1. [12 points] Read each of the following news stories about malware:
    a. ENISA reports a 30% increase in crypto-jacking incidents year-on-year in 2020, and they have only increased since. Crypto-jacking uses the victim's computing resources (usually CPU) to mine cryptocurrencies for the attacker. Crypto-jacking can be done by background scripts on a webpage. Webpages that are otherwise useful to visit are particularly powerful attack vectors. The resources stolen is not large enough to be noticeable to a victim.
        i. The violated CIA principle is integrity, because the victim's system gets malware and behaves incorrectly with actions not intended by the system owner. The method of spread is worm, as it spreads across the internet using background programs. A counter-measure to defeat or prevent the attack is to perform behavior-based malware scanning to detect system irregularities.
    b. In 2013, the New York Times reported that the Dual EC DRBG random number generator has a potential backdoor. The NSA is the sole editor of this algorithm's standard. The backdoor allows an attacker to fully compromise cryptography based on this tool. RSA Security started using Dual EC DRBG as its standard RNG for some of its software after accepting $10 million from the NSA.
        i. The violated CIA principle is confidentiality. The system's cryptography gets compromised by the attacker through the backdoor, and compromised cryptography means the system's data is no longer safe nor private as the attacker holds the confidential information. This is a planted malware as the backdoor could be installed intentionally for system testing, or installed by other malwares. A counter-measure to defeat or prevent the attack is to perform code analysis and software testing to find vulnerabilities in the code. Once any security vulnerability is found, the system can publish new patches to fix the vulnerabilites in the software.
    c. Pegasus is a powerful piece of malware developed by the NSO Group that has frequently been used for surveillance on high-profile targets such as politicians and human-rights activists. Attackers exploited a zero-day vulnerability in the Safari Webkit by sending a file to a victim that appears to be a GIF file, but clicking on it would cause surveillance software to be installed on their iPhone. A 2021 report by Amnesty International shows that it has been used in thousands of attacks over the three preceding years.
        i. The violated CIA principle is integrity. The system gets malware and behaves incorrectly with actions not intended by the system owner. If the attacker steals any confidential information using the surveillance software, then it also violates the CIA principle of confidentiality. The malware is a type of trojan, as the attacker tricks the user into installing the malware by clicking on the GIF file.
    d. The Meris botnet broke several records for DDoS volume in 2021. It compromises MikroTik routers with a directory traversal vulnerability that allows remote attackers to steal the admin password of the device to gain full control over it. With 250,000 such routers, Cloudflare estimates that Meris targeted approximately 50 different websites a day, demanding ransoms and DDoSing websites that refused to pay.
        i. The violated CIA principles is availability, as the attackers were able to control over the attacked devices using the botnet, making the system not usable to its owner. Confidentiality and integrity could also be violated because attackers were able to steal admin passwords and log in to the system as admins. The malware is a type of

worm, as it is spread using network across different routers with the botnet. A possible counter-measure to defeat such an attack is to perform signature-based malware scanning to detect malwares, patterns/signatures that matches the attack signature.

For each of the above news stories, answer the following questions and explain:

- i. [4 points] Which of the CIA principles is being violated?
- ii. [4 points] Classify the malware by method of spread (not payload).
- iii. [4 points] Suggest a reasonable counter-measure to defeat or prevent the attack.

2. [10 points] State whether each of the following statements is true or false. For each, explain why.
   - a. [2 points] One major reason in why we continue to use C and C++ despite its vulnerabilities is the Saltzer-Schroeder principle of “work factor”.
     - i. False, C and C++ has a very common software flaws – buffer overflow – that is powerful and relatively easy to exploit. Such an software flaw does not match the Saltzer-Schroeder principle of “work factor”, as the effort that an attacker needs to expend to attack the system is minimized. The major reason that we continue to use C and C++ is because they have already been very widely used language.
   - b. [2 points] Buffer overflow attacks are made more powerful because of poor implementation of the principle of least privilege.
     - i. True, buffer overflow attack is very powerful as it gives root access and often allows full control to the attacked system. The buffer overflow exploitation, “Return-to-Libc”, allows the attacker to use the shared library libc functions uncontrollably once the vulnerability is exploited.
   - c. [2 points] Stack canaries are an example of the principle of fail-safe defaults.
     - i. True. Fail-safe defaults principle refers to the system reverting to a secure default upon failures detected. Stack canaries, on the other hand, is used to detect stack buffer overflow before the execution of bad code. Stack canaries are an example of the principle because once the buffer overflow is detected prior to code execution, the program crashes, or returns, as “failure” (overflow) is detected.
   - d. [2 points] XSS attacks usually require the attacker to gain full control over the web server first.
     - i. False. Attackers do not need full control over the web server to perform XSS attacks, rather they only need the server to parse a line of code to attack the vulnerability. In that sense, other users can be running the malicious lines of codes simply by clicking on malicious links that contains the code execution.
   - e. [2 points] The vulnerability behind Heartbleed is more serious than what would have been caused by a format string vulnerability.
     - i. False, format string vulnerability is as serious as any buffer overread vulnerability like the Heartbleed bug. Buffer overread vulnerabilities exist due to failure to perform stable bound checks, and format string vulnerabilities exist due to developers failing to perform reliable input validation checks. While the Heartbleed bug allows anyone on the Internet to read the protected system memory of the vulnerable versions of the OpenSSL software, format string vulnerabilities could also cause data corruption, program crash, or malicious code execution.
3. [13 points] In 2015, Ion et al. investigated the differences between security practices recommended by experts and non-experts. Experts included hacker conference attendees, professionals and researchers, while non-experts were recruited from MTurk.

i. [4 points] The biggest difference in security practices between experts and nonexperts was to "update software". 35% of experts included this in their top three suggestions while only 2% of non-experts did so. Give two examples of real attacks that could have been prevented if software updates were taken more seriously.
   a. The SQL Slammer worm attack in 2003 could have been prevented if software updates were taken more seriously. The Slammer worm is a malware that exploits SQL Server buffer overflow using a packet, where it generates random addresses and sends itself by UDP. Although patch was published after Blackhat warning, but users were too lazy to restart and update, which resulted the system infections. If SQL server were able to force update on all installed devices, or if users taken software updates more seriously, many of the infections could have been avoided.
   b. The Heartbleed bug in 2015 could have also been prevented if software updates were taken more seriously. The bug is buffer overread vulnerability in OpenSSL caused by memcpy, malloc, and prints, as memcoy does not check the size of payload being copied to the pointer retuning to the client, so that attacker can simply declare a large size payload to read more memory than it should. The bug allows anyone on the internet to read the memory of the system protected by the software's vulnerable versions. The problem could be fixed simply by updating the system's OpenSSL library to the latest version, as patches with bound checking were released after the bug were found.

ii. [5 points] The top advice from non-experts was to use antivirus software, but experts do not agree. Experts rate the effectiveness of antivirus software much lower than non-experts. Why is that? Explain with reference to current malware capabilities.
   a. Antivirus software is becoming less effective as mlawares have been continuously evolving. Advanced persistent threat (APT) explains the extent of current malware capabilities, as such an attack is usually focued, long-duration attack that combines multiple infection vectors and spreading strategies. It is more difficult to identify APTs as attackers can remain undected for an extended period of time with access to network, where confidential data can be compromised in that period. The Flame attack in 2012 is an example of spyware that attacked Microsoft Windows systems to spy on user actions like keystrokes, camera, and screen. This malware is able to detect the attacked system's installed antivirus software, and then customize its own behavior to hide its trace. Therefore, the use of antivirus software in such an attack is minimized as the malware was able to adapt its behavior depending on the antivirus software.

iii. [4 points] Experts and non-experts viewed password management differently. Generally, experts recommend using a password manager, while non-experts advocated for rotating passwords frequently, choosing strong passwords, and writing down passwords. Many more experts say they don't remember all their passwords than non-experts (83% vs 48%). Explain the difference in practices with reference to two Saltzer-Schroeder design principles.
   a. Experts' recommendation of using a password manager practices Saltzer-Schroeder's principle of Separation of Privileges. Separation of privileges refers to the system granting permission based on multiple conditions. A password manager could have 2-factor authentication is considered more secure as the account can only be accessed if the user passer the two verificaiton step (Master password and authentication code). On the other hand, frequent password rotation does not aligns to the principle of separation of privileges. Constantly changing passwords still posts risks in password

being compromised by attackers, as they are permitted to access the account once they guess the correct user password.

Most importantly, password manager aligns with Saltzer-Schroeder's principle of work factor, where the effort for an attacker to access user account increases with the use of such tool. The cost for the attacker to break through the password manager and access the user account is much higher than breaking frequently rotated user password. Using the 2-factor authentication as the password manager again, the attacker would have to do twice as much work to compromise both the master passwords and the authenticaiton code to access the account.