President's Corner: Computer Security
By Eric Moore
June 9, 2018

Overview

I usually write a monthly President's Corner covering the topic I present on at the monthly general meetings. However, time has not allowed me to write a column since January 2018. This month I will give a quick summary of some of the topics I have presented during the past several months. My goal is to educate you about these threats and to remind you always to keep your computer up-to-date and to be cautious of the software you install, websites you visit, and spam that you open. By being more cautious and suspicious, you will reduce the chances of becoming a victim.

Meltdown and Spectre

Meltdown and Spectre are vulnerabilities that most modern computer chips share. They were first disclosed by researchers on January 8, 2018. What they discovered is that features of modern processors—Speculative Execution (SE) and pipelining—can be exploited by specially crafted software to gain access to otherwise private data in the CPU. Both features are desirable as they speed up the execution of computer instructions. In summary, they entail the ability to execute instructions in parallel and out of order, so they will not be eliminated to address these vulnerabilities.

Meltdown was named for the fact that it effectively "melts" the privacy of data between the operating system (OS) and application. It affects Intel and ARM processors, but not AMD processors. An application exploiting Meltdown can gain access to data that it should be able to access, such as passwords and cryptographic keys. OS and firmware updates have been released to mitigate the vulnerability, although they can impact system performance by slowing the OS and applications. The best way to protect yourself is to keep your OS, firmware, applications, and anti-virus software up-to-date. (Firmware updates are provided by your computer/hardware manufacture.) You are also advised about what software you install and use, as hackers may be looking for ways to trick users into installing applications that use this exploit.

Spectre is an exploit that allows one application to access the private data of another application. It affects Intel, AMD, and ARM processors. While it is more difficult to protect against, it is also more difficult to exploit. It can be exploited with JavaScript code on websites. Once again, you are advised to keep your OS, and applications, and anti-virus software updated, and to be cautious of what software you install and the websites you visit. Be cautious of clicking links in spam, as they can be used to trick the unwary into being attacked by one of these vulnerabilities.

A free Spectre detection tool named InSpectre is provided by Gibson Research Corporation. It can test your processor to determine if you are at risk. If your computer has an Intel processor, the tool can also determine if Intel has released a microcode patch to fix the vulnerability.

WannaCry and NotPetya Ransomware

Also referred to as "WannaCrypt," WannaCry was new ransomware released on May 12, 2017. It uses the NSA's EternalBlue exploit to encrypt the user's data files. Once installed, it requests a ransom of $300 in Bitcoin to decrypt the files, and it attempts to spread itself to other computers. The vulnerability it exploits in the Windows operating system had been patched by Microsoft on March 14,

2018, but many computers around the world were affected, as they had not been kept up-to-date. Microsoft considered the threat so great, that they even released patches for Windows XP, which they do not otherwise support or patch anymore.

NotPetya was released on June 27, 2017, primarily affecting Russia and Ukraine. It is a variant of Petya, which was first discovered in 2016, and uses the EternalBlue exploit. It infects the master boot record (MBR) of the victim's computer and encrypts the master file table, rendering the computer unbootable. A ransom of $300 in Bitcoin to decrypt the files.

The best defense against WannaCry and NotPetya is to keep Windows and anti-virus software updated; make regular, redundant backups of your important files to offline storage such as the cloud or to external drive; and to be cautious of visiting unfamiliar websites and clicking on links in spam. Be careful of flash drives and external drives that are connected to your computer, as they could be encrypted, not to mention local copies of files you synchronize with a cloud storage service such as Google Drive, OneDrive, and Dropbox.

KRACK

KRACK (**K**ey **R**einstallation Att**ack**) is an exploit affecting WPA2 Wi-Fi protocol first reported in October 2017. It allows an attacker to defeat the encryption of the WPA2 protocol, allowing him to "eavesdrop" on a victim's website traffic. The attacker can eavesdrop on the victim's email, passwords, financial data, etc. Most operating systems are affecting. Android and Linux are especially vulnerable.

To protect yourself, you should ensure your wireless router has the latest firmware. Firmware updates are provided by the router manufacturer, so check the user's manual or the manufacturer's website for the availability of updates and how to apply them. If you rent your modem from your ISP, consult with the ISP on how to ensure it is up-to-date.

Other recommendations are to avoid using Wi-Fi when possible, especially in public places. Using your cell phone carrier's network is an option to consider (depending on your data usage costs). Always use AES with WPA2, as it offers the strongest encryption for Wi-Fi traffic. Using an older, weaker protocol such as WEP is inadvisable.

VPNFilter

VPNFilter is malware discovered in May 2018. It is designed to infect routers. Once installed, it performs a man-in-the-middle attack to inject data and malware into the web traffic as it passes through the router. It can also steal passwords and other sensitive data. Various makes and models of routers are vulnerable. Click here for a list.

Although the FBI did seize a key server used for VPNFilter, the botnet still exists. Infected routers are still unsafe to use. Since there is no easy way to determine if a router is infected, the safest step is to perform a factory reset of the router. Doing so will clear the SSID and password of your Wi-Fi network, so you will need to reset them, as well as the administrator password. (Do always use strong passwords for both.)

Secunia
Secunia was a good program that Ron Mettler and I have talked about in the past. It was a free program designed to scan for and report on outdated software. The list of programs it checked included Firefox, Chrome, Flash, and Microsoft Office. It could also download and apply the appropriate updates for you. Sadly, this useful tool was discontinued by Flexera on April 20, 2018.

If you have used it, you should uninstall the software as it is no longer functional. As a replacement, I advise that you enable updates for your operating system and watch for notices from your applications when updates become availability. Not all applications automatically check for updates, so you may need to do so manually. It may be an option listed under the Help menu or somewhere else such as "Options" or "Tools." When all else fails, check the help information (press F1) or consult the software vendor's website for information on how to update it.