President's Corner: June, 2014
Discontinuation of TrueCrypt Support
By Eric Moore

Four years ago I gave a presentation on the topic of how to encrypt files on your computer as a safeguard against private or sensitive information falling into the wrong hands. As more criminals are designing malware in an effort to capture computer users' data—usually for the purpose of stealing money from bank accounts, credit cards, and other accounts—computer users more than ever should take care to protect themselves from theft, fraud, and identity theft. One of the tools to assist in this matter is software for encrypting data.

Among the technologies I discussed in 2010 were EFS, BitLocker, AxCrypt, and TrueCrypt. Each has its strengths and weaknesses, advantages and disadvantages. EFS and BitLocker are integrated with Microsoft Windows 2000 and later (in the case of EFS) and Windows Vista and later (in the case of BitLocker). As such, no separate software installation or purchase is required, but they are only available in the higher-end editions of Windows, as opposed to less-expensive versions such as Windows Home. AxCrypt is a handy third-party application for encrypting individual files, but not entire directories or drives, as can be done with EFS and BitLocker.

TrueCrypt is another third-party application that can be used to encrypt an entire drive or partition, such as a hard drive or flash drive. As it can be used with any version of Windows, it is a useful substitute for BitLocker, which is only available with the Ultimate and Enterprise editions of Windows Vista and 7, and the Pro and Enterprise editions of Windows 8. I use TrueCrypt regularly for protecting sensitive data on a flash drive that I keep handy for whenever I need it (as opposed to locking it away when I am not using it). When I need to look up some information, I plug in the flash drive, open the TrueCrypt software, select the option to “mount” the encrypted drive, and then provide the password to unlock the contents of the flash drive. When I am finished with the flash drive, I “unmount” the drive so it is secure again.

Unfortunately, the persons who created the TrueCrypt software announced on May 28, 2014 that they have discontinued support and development of the product. They recommended ceasing to use the product because of undisclosed security concerns and using another product such as EFS or BitLocker. According to Gibson Research Corporation, the persons who created TrueCrypt were no longer interested in maintaining it. No other sources that I have checked can provide more information about the security concerns at this time. I will consider my options as to whether I continue to use TrueCrypt or look for another product to replace place.

An important consideration in all this is that as useful as encryption tools are, none is invincible. For every technology meant to protect you, someone will develop a technology to defeat it. The recent debacle with OpenSSL (see my column for the May edition of Random Access) was the result of inadequate oversight in the software code, leaving a glaring hole that could be exploited to gain access to private data on servers that are otherwise protected by SSL and TLS. Other ways to defeat encryption software include keylogger devices that can capture your encryption keys, algorithms to capture your key while it is still in RAM, and malware that can capture keystrokes much like a keylogger. The encryption algorithms themselves may be defeated as researchers and criminals study, prod, and poke at them to test just how secure they are against brute force attacks.

Data encryption is still important and useful, whether you are protecting a collection of passwords for

your favorite websites, financial data, or other sensitive information. Just be certain you do not take it for granted that once the data is encrypted it is secure. An encrypted flash drive or laptop may still yield its secrets to a determined criminal who steals the device. Security applications can contain bugs and security holes that may be exploited by criminals. Bugs in you web browser and operating system can be exploited as backdoors into your computer. So, take care to protect your devices and be certain to install recommended updates for any applications you use. Be sure also to keep your operating system and anti-virus software up-to-date. (Secunia is an online resource that can perform a "health check" on your Windows-based computer and alert you to any insecure programs that should be updated.) The more you do so, the safer you will be from becoming a victim.