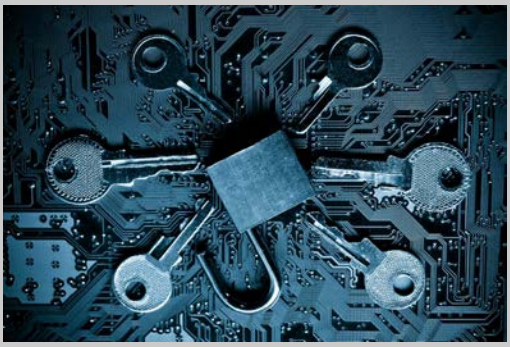
WINTER 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their e-discovery, computer forensics and cybersecurity needs. With increasing encryption usage and the recent news of the government requesting Apple to provide "backdoor" access to iPhones, we chose to theme this E-Newsletter on the impact data encryption has on attorneys, litigation support professionals and investigators.

THE SHIFTING LANDSCAPE OF DATA ENCRYPTION



TrueCrypt, a free on-the-fly full disk encryption product, was the primary cross-platform solution for practitioners in the electronic discovery and computer forensics sector. Trusted and widely adopted, TrueCrypt's flexibility to perform either full disk encryption or encrypt a volume on a hard drive was an attractive feature. When TrueCrypt encrypted a volume, a container was created to add files for encryption. As soon as the drive was unmounted, the data was protected. The ability to add a volume to the original container, where any files or the folder structure could be hidden within an encrypted volume, provided an additional benefit to TrueCrypt users. However, that all changed in May 2014 when the anonymous team that developed TrueCrypt decided to retire support for TrueCrypt. The timing of TrueCrypt's retirement is most often credited to Microsoft's ending support of Windows XP. The TrueCrypt team warned users that without support for Windows XP, TrueCrypt was vulnerable. Once support for TrueCrypt stopped, trust continued to erode as independent security audits uncovered specific security flaws. In the wake of TrueCrypt's demise, people were forced to look for other encryption solutions. TrueCrypt's website offered instructions for users to migrate to BitLocker, a full disk encryption program available in certain editions of Microsoft operating systems beginning with Windows Vista.

BitLocker works much as TrueCrypt did offering the flexibility to encrypt the entire drive or partition. While BitLocker is the predominant option for encrypting Windows-based computers, depending on the computer manufacturer, there could be other pre-installed disk encryption programs. One such example is Credant (currently known as Dell Data Protection), which comes installed on newer Dell computers. Dell bought Credant Technologies to encourage enhanced integration of encryption across multiple computers within an organization's network. As for Apple computers, OSX has built-in encryption software called FileVault. The current version of Apple's encryption software is FileVault 2, which can perform full disk encryption as well as volume-based encryption by creating a separate partition on the same hard drive. Open-source, free encryption software solutions replacing TrueCrypt also exist. One free software package,

Veracrypt, is based off of TrueCrypt code and has fixed the security issues that were found in the TrueCrypt independent audits. Another free software package is DiskCryptor, which also functions much like TrueCrypt.

Most federal government agencies chose hardware encryption as a solution, and hardware-encrypted drives that comply with FIPS 140-2 became the standard. One benefit of a hardware-encrypted drive is that the encryption key is generated and stored in the self-contained enclosure and not within the CPU. If a "bad actor" attempts to crack the PIN through numerous failed attempts or if tampering occurs with the physical enclosure itself, the hardware locks down, destroys the encryption key, and erases corresponding data in response. Albeit while offering an extraordinary level of protection, the cost of hardware-encrypted drives may seem prohibitive relative to less expensive, often free, software solutions.

As for smart devices such as iPhones, iPads, Android phones, and tablets, there are encryption solutions based on the applicable operating system of each device. For iOS/Apple devices, on-the-fly file level encryption is handled through hardware encryption as well as the user passcode. Backups of the iOS devices that are password protected are also encrypted, and all transmissions from the device are encrypted as well. For Android devices, there is built-in full disk encryption software, but also applications that handle volume and file level encryption. One such application is Secret Space Encryptor or SSE, which is free to download. In light of the removable storage media, such as SD cards, generally found in Android devices, encryption applications are welcome and helpful security add-ons. Please note that if a computer forensics professional creates a forensic image of a smartphone or tablet, these images may be transported using BitLocker or hardware-encryption depending on the case requirements. Imaging a drive does not automatically decrypt the data.

While TrueCrypt's retirement dust appears to have settled, proponents of data security fear that current disk encryption solutions may be vulnerable to backdoors that the FBI, NSA or other government entities could potentially exploit. Currently, there isn't much legislation regarding data encryption backdoors, but there is a battle between government agencies and technology companies over providing backdoor access, and this may well become the dominant encryption issue of the future. Tech companies argue that creating backdoors fosters a slippery slope problem where eventually no data could be securely encrypted. Recently, in light of the San Bernardino shooting last December, an order signed by a California magistrate judge orders Apple to create a "backdoor" to disable the feature which causes the data on an iPhone to automatically erase after a number of unsuccessful tries to log in using a PIN. To persuade the court, the FBI stated that after two months, they still have not been able to access the shooter's iPhone on which the FBI believes there is valuable information relevant to the San Bernardino attack and prevention of future attacks. In response, Apple CEO Tim Cook wrote that Apple does not have the ability to disable that feature currently, and that developing an alternative access method is itself "too dangerous to create."

As of this date, there isn't sufficient evidence that backdoors exist within the code of encryption software. For example, independent audits of the aforementioned TrueCrypt showed that the source code was free of backdoor access to encrypted data. The current lack of encoded backdoors does not mean that none exist. Rootkits are one example of malware designed to create backdoors where one wasn't designed to exist. Fortunately, manufacturers such as Apple rely on sophisticated hardware and software methodologies to keep prying eyes from spying on personal data and continuous improvements evidence their commitment to a secure future.

UPCOMING INDUSTRY EVENTS

February-March 2016

RSA Conference, San Francisco: February 29 - March 4

March 2016
Fifth Annual ASU-Arkfeld
eDiscovery and Digital Evidence Conference, Tempe: March 9-11

ABA Techshow 2016 Conference and Expo, Chicago: March 17-19

April 2016
The Masters Conference, San Francisco: April 19

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: