Encryption Made Simple for Lawyers

By David G. Ries, Esq. and John W. Simek

Encryption is a topic that most attorneys don't want to touch with a 10-foot pole, but it is becoming a more and more important part of security. Encryption is an electronic process to protect data. It has now reached the point where all attorneys should generally understand encryption, have it available for use when appropriate, and make informed decisions about when encryption should be used and when it is acceptable to avoid it. Fortunately, easy to use options are available today for encryption. Most attorneys will need technical assistance to install and set up encryption, but it's generally easy from there.

Encryption uses a formula to transform readable data into unreadable data. The formula is an algorithm (called a cipher), the readable data is called plaintext, and the unreadable data is called ciphertext. Decryption is the reverse process that uses a key to transform the encrypted data back to readable data. As long as the decryption key is protected, the data is unreadable and secure. While the technical details of how encryption works are complex, it is not necessary for attorneys who use encryption to understand them.

Encryption can be used to protect data at rest (on desktops, laptops, servers or portable media) and data in motion (over wired or wireless networks and the Internet). Anyone who has access to encrypted data cannot read or use it unless they have access to the decryption key.

Attorneys have ethical and legal duties to protect information relating to clients. Encryption is an important consideration in addressing these duties.

Laptops and Portable Media

The attributes that make laptops and portable devices useful also make them very dangerous from a security perspective: they're compact and portable. Add to that the fact that their costs have been decreasing over the years, their capacities have been dramatically increasing, and they have become more and more compact. Laptops are available with 1TB (terabyte) and larger hard drives. USB thumb drives with capacities of 256 GB or more are now available. Portable hard drives of a TB or more, the same as desktop computers, are now available. A massive amount of data, in compact media, can be easily lost or stolen. With these devices, attorneys and employees can lose or steal the equivalent of a truckload of information.

Not properly protected, laptops and portable media can be recipes for a security disaster. One survey reported that 70% of data breaches resulted from the loss or theft of off-network equipment (laptops, portable drives, PDAs and USB drives). Strong security is a must. Encryption in now a standard security measure for protecting laptops and portable devices and attorneys should be using it.

In fact, a joint U.S./UK research team has written that full disk encryption is so effective that law enforcement and federal agencies are complaining that they are unable to retrieve the encrypted data in criminal investigations. Federal courts are

struggling with the issue of whether compelled disclosure of passwords and passphrases for decryption is protected by the Fifth Amendment.

After the high-profile theft of a Department of Veterans Affairs laptop and external hard drive containing personal information on more than 28 million veterans in 2006, security guidelines for federal agencies added the requirement of encryption of all data on laptops and portable devices, unless it is classified as "non-sensitive." This was six years ago.

In January 2007, 18 laptops were stolen from the offices of a law firm in Orlando. The laptops were reportedly protected by encryption, and the incident received very little publicity. In discussing this incident, the SANS Institute, a leading information security organization, noted, "[l]aptop thefts aren't going away, but by this time next year, this type of item (laptop stolen, but the data was protected) shouldn't be newsworthy." That was over five years ago.

In a recent data breach report, a Maryland law firm lost an unencrypted portable hard drive that contained medical records of patients in a lawsuit against its client hospital. One of the law firm's employees took home the hard drive containing backup data. This was the firm's method of ensuring that it had an offsite backup. She took the light rail system home and left the drive on the train. When she came back a few minutes later, it was gone. Backup is a good practice, but not if it exposes confidential data. If the drive had been encrypted, it would have had a strong level of protection. As it was, it had little or none. It is not uncommon for

backup software to have the ability to encrypt the backed up information. Generally, it is just a simple matter to check an option for the backup to be encrypted.

As these examples demonstrate, encryption is particularly important for laptops and portable media. A lost or stolen laptop or portable device that is encrypted is protected unless the decryption key has been compromised. There are three kinds of encryption for protecting laptops and portable devices: hardware encryption, encryption in operating systems (like Windows and Apple OS X), and encryption software.

There are two basic approaches to encrypting data on hard drives: full disk encryption and limited encryption. As its name suggests, full disk encryption protects the entire hard drive. It automatically encrypts everything and provides decrypted access when an authorized user properly logs in. Limited encryption protects only specified files or folders or a part of the drive. With limited encryption, the user has to elect to encrypt the specific data.

All of the hard drive manufacturers now offer hard drives with hardware full disk encryption built in. The major laptop manufacturers all offer models with these drives. Hardware encryption is generally easier to use and administer than encryption software. Some examples are Seagate Secure and Hitachi Self-Encrypting Drives. Secure use just requires enabling encryption and setting a strong password or passphrase. The contents of the drive are automatically decrypted when an authorized user logs in. It is automatically encrypted when the user logs off or the laptop is turned off.

Since most encryption programs are tied to a user's password, secure passwords or passphrases are essential, and a forgotten password can lead to lost data. Automatic

logoff, after a specified time, is critical so that unencrypted data will not be exposed if a user goes away from a computer or forgets to turn it off. In an enterprise environment, like a law firm, access by an administrator, ability to reset passwords, backup and key recovery are essential. Installing encryption and administering it, particularly in a large enterprise, can be a challenge.

Current business versions of Windows and current versions of Apple OS X have built in encryption capability.

Windows Vista Enterprise and Ultimate and Windows 7 Enterprise and Ultimate include an encryption feature called BitLocker. BitLocker works below the operating system and encrypts an entire volume on the hard drive. BitLocker requires either a computer that is equipped with a Trusted Platform Module (TPM) chip on the motherboard or use of an external USB drive to hold the decryption key. If an intruder gains access to a USB key, the encryption can be defeated. Setup of both EFS and BitLocker is fairly technical. For most attorneys, it will be necessary to obtain technical assistance to implement them.

The business versions of Windows also include an encryption function called Encrypted File System (EFS). It allows encryption of files and folders. An authorized user who is logged in has access to decrypted data. It is encrypted and unreadable to anyone else (unless they can defeat the login process). EFS is considered a fairly weak encryption method that is easily cracked using forensic tools. You are better off using BitLocker or one of the other third party encryption products discussed below.

OS X has built-in file encryption in FileVault. Newer versions have full disk encryption available in FileVault 2. Follow Apple's instructions for turning it on. After a password is set, it just requires turning on the FileVault button in System Preferences. Recent advances have attacked Apple's encryption scheme and the Passware software suite claims to be able to defeat FileVault 2 in less than an hour.

Some commonly used third-party encryption software products for hard drives include those offered by Symantec (PGP and Symantec Endpoint), McAfee, Check Point, Guardian Edge, and Utimaco (Sophos). A common open source encryption program that is free and relatively easy to use is TrueCrypt.

Hardware-encrypted drives and encryption software are available for USB drives and portable hard drives. Microsoft's BitLocker to Go can be used to encrypt portable devices. Individual USB drives with built-in encryption capability are also available, like the IronKey (Immation), KanguruMicro, Kingston, and SanDisk Cruzer Professional and Cruzer Enterprise. The IronKey is a favorite of the authors. It includes strong encryption, wiping if the wrong credentials are entered too many times and strong physical construction, with wiping from physical tampering. As an added bonus, several of the models contain a password management application called Identity Manager, which stores all of your 12+ character passwords in a secured, encrypted "vault." Of course you can store any length password, but the current recommendation is 12 or more characters.

To avoid the loss of data, it is important to understand how the encryption works, to back up data that is encrypted, and to keep a copy of the recovery key in a secure place. Enterprise controls are available to centrally manage encryption.

Smartphones and Tablets

Smartphones and tablets are basically small computers, with substantial computing power and high storage capacity. Like laptops and other mobile devices, they can be easily lost or stolen and should be protected with encryption.

BlackBerry devices have long been the “gold standard” for secure communications when speaking about cellular phones. If you use the BlackBerry Enterprise Server (BES) the communications are automatically encrypted. Encrypting the device itself is accomplished by enabling Content Protection. You can find that choice by navigating to Options -> Security Options -> Encryption. This is where you will set encryption for the device memory, encryption strength, contacts, media files and expansion memory card. In addition, you will need to set a password for the phone as well as the inactivity timer to lock the phone. The password and timouts are set by going to Options -> Password. A lot of law firms use BES to manage their BlackBerry devices. This centralized management will push the desired security settings to the phones with no user interaction.

For iPhones and iPads, hardware encryption was implemented in iOS 4. All files are automatically encrypted and decrypted when the device is unlocked. It provides little protection unless Simple Passcode is turned off, Require Passcode is turned on,

and a strong passcode is selected. Require Passcode should be set for a short time and Erase Data should be turned on. iOS also includes a feature called Data Protection. It secures e-mails and attachments stored on the device and data in other apps that are designed to work with it.

Android OS has included encryption for tablets (starting with Honeycomb) and for phones (starting with Ice Cream Sandwich). Earlier versions require third-party apps for encryption, like WhisperCore, Droid Crypt, or AnDisk Encryption. Also, Motorola and Samsung market enterprise phones with built-in encryption capability. Follow the device manufacturer's instructions for turning on encryption. It generally requires touching the Encrypt or Encrypt Tablet button in Settings. A strong PIN or password and automatic logoff after a set time are also important to keep the data encrypted.

Again, it is important to follow the manufacturer's instructions when setting up encryption. Get help if you need it. First time encryption takes some time when a device has already been in use, so make sure that the battery is fully charged before starting.

Weaknesses have been reported in the encryption for both iOS and Android, so it is important to consider multiple levels of security. Despite some limitations, smartphones and tablets are more secure with encryption and attorneys should be using it.

It is also important to make sure that secure methods are used for getting files on and off smartphones and tablets and for sharing files. There is substantial concern about the security of services like Dropbox and iCloud. Their terms of use provide limited protection and they control the encryption. They control the encryption keys so their employees can get access and protection from unauthorized third parties depends on how well they protect the decryption keys. Use of alternatives like BoxCryptor (with Dropbox), Box, and SpiderOak provide stronger security because the end user controls the decryption keys.

Wireless Networks

Communication via wireless connections needs to be secured as well in order to protect the transmission. Encrypting the wireless network will protect the data from being intercepted and viewed. There are many free “sniffer” applications that can be used to view the contents of unencrypted data streams. Essentially, there are three commonly available types of encryption schemes for your wireless network. WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2 (second generation WPA) encryption methods are available on all currently available wireless access points. WEP is very weak encryption and is fairly easy to crack. There are plenty of free tools available that can crack WEP in a matter of minutes. WEP should not be used in any wireless network because of its insecurity. WPA is a stronger form of encryption, but it has also been cracked. Therefore, WPA is not recommended either. WPA2 is secure and should be the encryption method of

choice for wireless networks. As with other forms of password management, the WPA2 passphrase should be long and complex.

In addition to making sure that their wireless networks are secure, attorneys should ensure that third-party wireless networks that they use for client matters are protected by encryption. They should be protected by WPA2 and require a user name and password for access. This is particularly the case for public networks. Many security professionals and US-CERT have recommended that public networks should not be used for confidential communications. If public networks are to be used, attorneys obtain technical assurance that they are being securely used through protection like a virtual private network (VPN). A recent ethics opinion concluded that an attorney has an ethical duty to evaluate the security of a wireless network, home or public, *before* it is used for client communications and to take appropriate precautions in using it. California Formal Opinion No. 2010-179.

E-mail

Particularly important to attorneys is the confidentiality and integrity of e-mails. Respected security professionals have for years compared e-mail to postcards or postcards written in pencil. They can be viewed or altered by third parties. While some ethics have been incorrectly interpreted as saying that e-mail encryption is never required, current ethics opinions continue to stress the requirement of reasonable and competent safeguards. For example, California Formal Opinion No. 2010-179 states “encrypting email may be a reasonable step for an attorney in an effort to ensure the confidentiality of such communications remain so when

circumstances for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous." Encryption is increasingly required in areas like banking and health care and by new state data protection laws. As these requirements continue to increase, it will become more and more difficult for attorneys to justify their avoidance of encryption.

For e-mail, the term *encryption* is generally used to mean both encryption and the authentication process that are used, in combination, to protect e-mail. Encryption protects the confidentiality of e-mail. Authentication identifies the sender of an e-mail and verifies its integrity.

Encryption is a process that translates a message into a protected electronic code. The recipient (or anyone intercepting the message) must have a key to decrypt it and make it readable. While it still takes some technical knowledge to set up, e-mail encryption has become easier to use over time.

Encryption generally uses a pair of keys to encrypt the e-mail. The sender uses the recipient's public key to encrypt the e-mail and any attachments. Since the public key only encrypts the e-mail, it does not matter that it is available to the public or to various senders. The recipient then uses his or her private key to decrypt the e-mail. It needs to be safeguarded because anyone who has access to it can use it for decryption.

The process is easy to use once the keys are set up in an e-mail program like Outlook. The most difficult process is getting the keys (digital IDs) and making the

public key available to senders. Once it is set up in Outlook, the sender just has to click on the Message tab in the Options group and click the Encrypt Message Contents and Attachments button. At the recipient's end, the message will automatically be decrypted if his or her private key has been installed.

Digital authentication of e-mail also generally uses a key pair. The sender uses his or her private key to digitally sign the e-mail. The recipient then uses the sender's public key to verify the sender and integrity of the message. In Outlook, after installation of the private key, the sender clicks the Options tab in the Permission group and clicks Sign Message. After the sender's public key has been installed in the recipient's compatible e-mail program, the recipient will receive an automatic notice of verification of the sender and integrity.

For protection of confidentiality and authentication, the sender's and recipient's key pairs are used in combination. The sender uses both the Encrypt Message and Attachments command button (that uses the recipient's private key) and the Sign Message command (that uses the sender's private key). At the receiving end, the e-mail program automatically uses the recipient's private key to decrypt the messages and automatically uses the sender's public key to verify authenticity and integrity.

Again the challenging part is obtaining key pairs, exchanging public keys and setting them up in the e-mail program for encryption. Keys are available from commercial public key authorities like Verisign (now part of Symantec). Public key authorities have online directories where their customers' public keys are available.

Another form of e-mail encryption is Transport Layer Security (TLS) encryption. It automatically encrypts e-mail between two e-mail gateways. If a law firm and client each have their own e-mail gateways, TLS can be used to automatically encrypt all e-mails between them. TLS encryption protects e-mails between e-mail gateways only. It does not protect e-mails within the sender's and recipient's networks and does not protect e-mail that is misaddressed or forwarded through other e-mail gateways.

Secure e-mail is also available from managed messaging service providers like Zixcorp, Mimecast, and Data Motion. They provide e-mail encryption without the complexity of setting up and exchanging keys.

As an alternative to encryption, confidential information can be protected by putting it in a password-protected attachment rather than in the body of the e-mail. File password protection in some software, like current versions of Microsoft Office, Adobe Acrobat and WinZip uses encryption to protect security. It encrypts only the document and not the e-mail, so the confidential information should be limited to the attachment. It is generally easier to use than complete encryption of e-mail and attachments. However, the protection can be limited by the use of weak passwords that are easy to break or "crack."

It has now reached the point (or at least is reaching it) where most attorneys should have encryption available for use in appropriate circumstances. In addition to complying with any legal requirements that apply, the most prudent approach to the ethical duty of protecting confidentiality of electronic communications is to

have an express understanding with clients about the nature of communications that will be (and will not be) sent by e-mail and whether or not encryption and other security measures will be utilized.

Conclusion

Encryption is now a generally accepted practice in information security for protection of confidential data. Attorneys should understand encryption and use it in appropriate situations. All attorneys should use encryption on laptops, portable storage media, smartphones, and tablets that contain information relating to clients. They should make sure that transmissions over wireless networks are secure. Attorneys should have encryption available for e-mail and use it when appropriate. While most attorneys will need technical assistance to install and set up encryption, use of encryption after that is generally easy.

Encryption is now a generally accepted practice in information security for protection of confidential data. Attorneys should understand encryption and use it in appropriate situations.

Attorneys should always use encryption on laptops, portable storage media, smartphones, and tablets that contain information relating to clients.

While most attorneys will need technical assistance to install and set up encryption, use of encryption after that is generally easy.