FEATURE: ENCRYPTION MADE EASY: THE BASICS OF KEEPING YOUR DATA SECURE

April, 2016

Reporter
76 Or. St. B. Bull. 19 *

Length: 3115 words

Author: By Sharon D. Nelson & John W. Simek

The authors are the president and vice president of Sensei Enterprises, a legal technology, information security and digital forensics firm based in Fairfax, Va. Reach them at (703) 359-0700 (phone) or http://www.senseient.com.

Text

[*19] Before you can protect your data, you need to know where it is. That seems pretty obvious, but a lot of lawyers are unaware of all the locations where their data resides. We're aware that we need to protect the data on the disks that exist in our desktop computers, laptops and servers. We know that there may be confidential data on external media such as USB hard drives and flash drives. However, many attorneys forget about data stored on voicemail systems and their smartphones. Data on backup media needs to be protected too. So let's dive in and get to the basics of protecting your data securely.

Encryption **Is Your Friend**

Lawyers tend to cringe when they hear the word encryption. To most lawyers, encryption is a dark art, full of mathematical jargon and incomprehensible to the average human being.

[*20] When South Carolina suffered a major data breach of taxpayer data, what did Gov. Nikki Halley say? "A lot of banks don't encrypt. It's very complicated. It's very cumbersome. There's a lot of numbers involved with it." Leaving aside the laughable notion that a lot of banks don't encrypt data, the rest of her quote is in keeping with what we hear from lawyers. What we hear always translates into the same thing: Encryption is hard.

So let's make this more fun with some things you can relate to.

Encryption is designed to secure data from prying eyes. It keeps secrets secret. Think about your childhood. Did you play with invisible ink? Did you watch the mailbox for a magic decoder ring? Perhaps you spoke Pig Latin with a sibling so your parents remained clueless about what you were plotting.

You've seen secrets hidden in the movies -- remember the World War II Navajo code talkers in "Windtalkers"? Cryptography has been featured in many movies, including the "National Treasure" movies, "Sneakers" and, perhaps most famously, in "The Da Vinci Code."

In the simplest terms, cryptography is the science of secret communication. It involves transmitting and storing data in a form that only the intended recipient can read. Encryption is one form of cryptography.

Encryption is the conversion of data into a form, called a ciphertext (or code), that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form (plain text) so it can be understood.

The goal of encryption (and think how many forms of encryption have been broken) is to make obtaining the information too work-intensive or time-intensive to be worthwhile. There is no such thing as perfect encryption that can never be broken. In the early days, people carved messages into wood or stone and the recipient had the "key" to know how to translate them. Today, cryptography is far more advanced and is found in streams of binary code that pass over wired networks, wireless networks and Internet communications pathways.

At the end of the day, encrypting data will keep it secure. Since that is our ultimate goal, let's cover some of the ways that we can encrypt the data whether at rest or in transit.

Electronic Communications

The most used method of electronically communicating today is via email. Some may argue that text messaging is the number one method and that may be true for the younger generation, but businesses are primarily communicating with some sort of email service. The issue that we need to tackle is whether our electronic communications are secure (or need to be) and how to securely communicate if needed.

- **Gmail**

Many attorneys use Google's email service for their practice. Google is currently in the process of modifying all of its services to provide encryption by default. Documents disclosed by Edward Snowden reported that the NSA had tapped the undersea fiber optic cable that runs between two of Google's data centers. The data moving over the fiber was in clear text and being intercepted by the NSA. Ever since then, Google has been moving on a forced march to encrypt all of the communications and services it provides.

You may have noticed that search results are now being encrypted by Google. Just do a normal Google search. Notice that the URL automatically switches to *https://* and the returned results are encrypted. Google is doing this to protect the privacy of the returned information. Besides search results, Google is forcing *https://* connections to Gmail. This will encrypt the communications between your computer and Google's servers. In addition, the default is for Google to use TLS (Transport Layer Security), which is the successor to SSL, for server to server communication.

In June, Google announced a new tool called End-to-End. It's a Chrome browser extension that will keep the data encrypted until the recipient decrypts it. The code is available to those technically inclined and uses OpenPGP. Once the Chrome extension is tested and ready for primetime, Google will make it available in the Chrome Web Store.

- **Microsoft Exchange Server**

By default, Exchange is configured to automatically attempt to communicate with other servers using TLS. This means that the server-to-server communications travel in an encrypted state. You can also configure Exchange so that communications between two domains is required to be encrypted using TLS. If the same encryption level does not exist between the two domains, [*21] the messages are returned and a nondelivery report (NDR) is generated. Obviously, this would be a very secure configuration and something that may be considered between the firm and specific clients. However, implementing such configurations is best left to the technology professionals. We are pretty sure we won't see any attorneys attempting to do this on their own.

Exchange can also be configured to require TLS encryption for clients. This means that any software (e.g., Outlook) must use TLS in order to access a mailbox. Again, your I.T. person is probably better equipped to configure the TLS requirement for clients.

- **Email** Encryption

This topic can be complicated and confusing for most lawyers. Up to this point, we have discussed ways to encrypt the traffic from Outlook to the Exchange server and the communications between servers. But what if you only need

to encrypt a single message? The data flow is the same as if you were encrypting a file. Instead the "file" is an email message.

Configuring your email client to send encrypted messages is beyond the scope of this article, but there are much easier and less complicated ways to send an encrypted message. A very cost-effective solution that is worth considering are the email encryption services of the Zix Corp. ZixCorp is the only email encryption provider with SOC3/SysTrust certification, SOC2 accreditation and PCI Level 1, DSS V2.0 certification. The encryption service is easy to install and very simple to use.

Most attorneys will subscribe to the ZixCorp service through a reseller. The reseller will setup the mail flow so that messages in and out are routed through the ZixCorp servers. This is similar to many spam and antivirus services. The user installs an Outlook add-in that provides for one button click encryption. Compose your message and just click the button to encrypt. The message is then sent to the ZixCorp servers. If the recipient has a secure connection available, such as TLS described above with an Exchange server, the message is delivered to their inbox and automatically decrypted when they open it in Outlook. If no secure connection is available, they will receive a link to the message on the ZixCorp servers. The recipient will have to create a login ID or login to their account if they have already created one. They then retrieve the message. In other words, a non-ZixCorp user will be viewing the decrypted messages via a web browser once they have logged in. It couldn't be easier.

To say that lawyers using Zixcorp are delighted with the simplicity of its use is a vast understatement. No need to know the [*22] math behind the encryption. All they do is click on an "Encrypt and Send" button.

Wireless Communications

Besides protecting email communications, we should protect the transmission of any data over a wireless network. There are three methods available to encrypt a Wi-Fi network. WEP (Wireless Equivalent Privacy) encryption is very weak and susceptible to interception and cracking. There are many free tools available on the Internet to crack WEP encryption in a matter of minutes. The message: Don't use WEP encryption.

A second method for wireless encryption is WPA (wi-fi protected access). WPA has also been cracked although it takes a little longer than cracking WEP. The message again: don't use WPA. The only encryption method that has not been broken is WPA2, which is a stronger encryption than WPA or WEP.

The recommendation is to use only WPA2 for encrypting wireless networks. The increased security of the encryption algorithm ensures the confidentiality of the transmitted data. Make sure you check all your wireless devices and verify that they are configured for WPA2 encryption. If WPA2 is not available for the wireless device, get a replacement device.

Configuring your wireless access point or wireless router for WPA2 is very simple to do. Access the configuration interface for your wireless router. This is normally done by using a web browser and entering a specific I.P. address as the URL. Navigate to the section that deals with wireless security. You should see selections for the type of wireless encryption. Typically, the selections will be WEP, WPA or WPA2. Make the selection for WPA2. You'll also need to enter a passphrase for access to the wireless network. It is a best practice to make this passphrase complex and long, which follows the same recommendations as a login password. You will need to give this passphrase to anyone authorized to access your wireless network.

If you have a wireless network at home, make sure it is protected as well, especially if you work from home!

Smartphones and Tablets

The attributes that make smartphones and tablets great productivity tools also make them risky. They are mobile, compact, powerful, have large storage capacity and have multiple avenues of connectivity. But they can be lost or stolen, hacked, infected by malware and have their communications intercepted -- all exposing confidential data. As discussed previously, encryption is a "no-brainer" solution that provides strong protection in the event of loss or theft. On today's smartphones and tablets, encryption is generally easy to set up and use.

Current iPhones, iPads, Android phones and tablets, BlackBerry devices and some Windows mobile phones all have built-in encryption that is easy to use. It's either automatic (with a password or PIN) or simply requires turning encryption on.

If you are an iOS user (iPhone, iPod Touch or iPad), all you have to do is configure a PIN as a lock code. Once you do that, encryption is automatically enabled on the device. We would highly recommend that you NOT use the default 4 digit PIN for an iOS device. There are tools available (around $ 200-$ 300) that are specifically designed to crack the four-digit PIN within minutes to several hours. Turn off simple passcodes and use a passphrase or much longer PIN to secure your iOS device.

Android users just need to go to the settings and check that box to encrypt the device and expansion memory card. Make sure that you have your charger connected since the encryption process could take some time. If you are still one of those diehard BlackBerry users, you enable encryption by selecting content protection or through the security settings on the BlackBerry Enterprise Server.

Cloud Services

It seems like everybody is talking about "the cloud" and what new uses it provides for lawyers and law firms. All this talk got us thinking about how little the typical lawyer knows about cloud services. Many attorneys can't really even describe what "the cloud" is. You would be amazed at how many lawyers think "the cloud" is somehow impacted by the weather. We can't really blame them; the definitions for "the cloud" are all over the place. Our focus here is security of data held by a cloud service provider and data in transit between an attorney or law firm and a cloud service provider.

Generally, services that are provided in the cloud are provisioned by technology that is not physically located in your office. In other words, it is remote and off-premises. You can certainly own the equipment yourself and house it at a data center with everything under your control. There are a lot of other options for cloud computing, as well. You could purchase computing [*23] "space" on equipment owned or operated by someone else. Think of Amazon's Web Services, where Amazon owns the hardware and network and you purchase computing capacity and storage from them. Finally, you can purchase application access from the vendor, where it provides all the equipment, network, storage and the application software, too. Think of Google Docs, where you can create documents on Google's hardware via an Internet connection.

Probably the first place that lawyers go for cloud services is off-site storage. According to the ABA 2014 Legal Technology Survey Report, 56 percent of respondents reported using online storage for law-related tasks. The explosion of iPad usage drove hordes of lawyers to Dropbox. Dropbox is the 800-pound gorilla of cloud storage. It seems that software developers provide integration with Dropbox storage before any other cloud provider. However, the tide is starting to shift and other providers like Box, OneDrive and Google Drive are taking part of the market share from Dropbox. Security is a major concern for attorneys, and more scrutiny is being placed upon the cloud providers, especially storage providers.

In addition to storage providers, cloud-based case management applications are very popular. Document management is also growing in popularity as lawyers look for ways to reduce their expenses and increase productivity.

Encryption controlled by the end-user can be used to protect the confidentiality of the data since the encryption key is only known to the creator of the data. It is also important to make sure the data is transferred to the cloud provider over a secure encrypted connection such as *https://* and that the cloud provider implements strong encryption for data at rest. Finally, no system is secure if you use weak login credentials. You should be using a strong password (complexity and length) for authentication and enable two-factor authentication if available.

But which cloud storage service should you use? This is a question we get asked quite frequently. All too often we hear that law firms and corporations are transmitting client confidential information and even evidence via Dropbox. This is not a good thing, especially if you have read the terms of service (TOS) instead of continually clicking *I accept* and *I accept*. The reality is that most of the cloud storage providers have a way to decrypt your data stored

on its servers. If you read the TOS for OneDrive, Dropbox, iCloud, Box, Google Drive, etc., you will see a provision that states that the cloud provider will turn over the data to law enforcement or any other entity if served with proper court documents. This means they can decrypt the data in storage.

The exception and our recommendation is Spider Oak. Spider Oak is a "zero knowledge" service. You control the encryption keys when you create your I.D. and password. Spider Oak can't decrypt the data since there is "zero knowledge" of the encryption key. To securely store your data in any cloud service, the user should be the one controlling the encryption key and NOT the vendor. If you want the world to see your nude selfies, go ahead and use iCloud -- otherwise, select a secure storage service.

There are also "add-on" products such as BoxCryptor or Viivo that can be used to encrypt the data before you send it off to the storage provider. These products work by using a user-defined encryption key to encrypt the data first and then sending it to the storage provider (Dropbox, One Drive, etc.) in an encrypted form. This way, the user controls the encryption key and still gets the advantage of using the off-site cloud storage provider.

Securing Documents

Protecting individual documents is another area of concern for lawyers. Perhaps you need to store a confidential document in Dropbox and haven't obtained one of the pre-encryption services previously discussed. You can secure documents and other files very easily. Merely locking the file with a password encrypts the contents. Just like other authentication methods, you need to make sure you are using a complex password to secure the document. The password should be long (14 characters or more), contain lower and upper case letters, contain numbers and perhaps some symbols, too. Having a weak password makes it fairly easy to achieve a brute force crack.

So what files are typically password protected? Putting an open password on any Microsoft Office file (e.g., Word document, Excel spreadsheet, PowerPoint presentation, etc.) encrypts the contents. Office 2010 files are encrypted using AES-128 bit encryption and Office 2013 files are encrypted using AES-256 bit encryption. Perhaps the increased encryption strength is a good reason to upgrade to Office 2013 if you haven't done so already. Besides Office files, setting an open password for an Adobe Acrobat file encrypts the file, too. You can encrypt files within a WinZip archive also.

Encrypting a single file is another way to send confidential information via email. Put the confidential data into a Word document and set the open password. The document will be encrypted and can be safely sent via email as an attachment. No special email encryption software is required. Just don't send the open password in the same email message. Pick up the phone (what a novel thought) and call the recipient to tell them the password.

Summary

As you can see, encryption is your friend and will go a long way in making sure that your data is secure and safe from prying eyes. Make no mistake about it -- more and more clients and insurance companies are demanding that law firms use encryption. So all that balderdash about encryption being hard? Those days are over. Using encryption is easy -- and the ethical way to protect your data and that of your clients.