The Legal Intelligencer

Litigation Support

# Modern Encryption Systems and Why Passwords Matter

Kevin Baker, The Legal Intelligencer

Read more: http://www.thelegalintelligencer.com/id=1202754280618/Modern-Encryption-Systems-and-Why-Passwords-Matter#ixzz45ioABU00

April 6, 2016

The FBI's request for Apple to unlock the San Bernardino, California, shooter's iPhone, as well as requests in other cases, has increased the media frenzy surrounding data security, passwords, privacy and our rights under the Constitution. Passwords are convenient and the most commonly used method to secure data, but simple steps must be taken to mitigate their inherent weaknesses. Understanding the process of how modern encryption systems work will provide an explanation of why passwords matter and the fine line the FBI asked Apple to cross by unlocking the cellphone.

Encryption is a complex mathematical process that is performed on data. When you encrypt a file, hard drive or other device, that data is transformed in a way that the data is unreadable without a specific code known as a decryption key. There are several factors that determine how secure a particular encryption method is, but the encryption used by any of the modern encryption systems cannot be reversed, cracked, hacked, or in some other way defeated without knowing the decryption key. However, most encryption systems rely on a user-supplied password to protect the decryption key, which in almost all circumstances is weaker than the encryption itself. When someone talks about cracking encryption, they are actually talking about recovering the password used to protect the decryption key.

The reason encryption is effective at securing data has to do with the magnitude of possible decryption keys. A decryption key is the code or number that is used to "unlock" the encrypted data. Keys can be displayed in a variety of formats, but no matter how a decryption key is displayed, mathematically speaking, it is just a number, and often, it is an extremely large number. Think of a decryption key as the three-digit number that might open a locker, briefcase, or luggage lock, just with many more digits. The strength of encryption is determined by the key length. The key length is given in the number of bits, which is the number of 1s and 0s a number contains. In other words, 128-bit encryption refers to encryption that uses a 128-bit encryption key, which is a number with 2,128 possibilities or a number between 0 and 340,282,366,920,938,463,463,374,607,431,768,211,456. That is a 39-digit number, so you can think of 128-bit encryption as a locker with a 39-digit lock instead of three.

The key length (number of digits) in modern encryption systems is long enough that even an entire network of computers trying to decrypt a file would take trillions of years. To give you an idea of the magnitude of modern decryption keys, if all 7 billion people on Earth tried a trillion decryption keys a second, it would still take 1,541,469,010 years to try all the possible decryption keys in 128-bit (39-digit) encryption, and that is the weakest encryption that's commonly used. Many encryption systems use 256-bit (78 digits), 512-bit (155 digits) or 1,024-bit (308 digits) decryption keys.

# Weakest Link

The problem now lies with the inability for someone to remember such a large number to unlock their computer or cellphone; instead, a simple password or pin is used. Passwords are the weakest link in modern encryption systems because they have significantly fewer possible combinations than encryption keys. Passwords can sometimes contain numbers (10), upper or lower case letters (52), and punctuation/special characters (33), resulting in only 95 possibilities for each character. So an eight-character password only has 958 possibilities or a 16-digit number of possibilities. That is a lot less than the 39 digits in 128-bit encryption.

The limited number of possible passwords creates several opportunities for attacks. In cryptography, the simplest password attack is a brute-force attack. This method tries every combination of characters until the password is recovered. A more efficient and common password attack is called a dictionary attack, where words from the dictionary are used to attack the password. This attack is very effective because many users and businesses select passwords that are based on a word in a dictionary.

Manufacturers are aware of the weakness of passwords and have created hardware and software-based security containers to prevent the recovery of passwords through brute-force or dictionary attacks. In order for the password attacks to work, there must be a way to try the password or compare the result of a password calculation to ascertain if the correct password has been found. For the most part, encrypted files can be attacked directly and are open to the above attacks. When trying to recover the password for an encrypted hard drive or a mobile device it may be impossible to attack the password because the security container blocks direct access to the password. The container itself is also designed to be secure against tampering or attack.

Modern computers have a special chip that controls the decryption keys, known as the Trusted Platform Module (TPM). If you remove an encrypted hard drive from a laptop with a TPM chip, the only way to recover data from the hard drive is to recover the full decryption key (39-plus digits). Even when the hard drive is in the laptop, the TPM is designed to prevent password recovery attacks. Depending on the configuration, after a number of incorrect passwords the chip prevents further attempts for a certain amount of time, defeating brute-force or dictionary attacks.

Most cellphones have a similar security container that stores the decryption keys, except that many of them are configured to completely destroy the decryption keys after too many unsuccessful attempts. Since modern encryption cannot be cracked without the ability to recover the decryption keys by attacking the much weaker password, the data is effectively destroyed

when the decryption keys are destroyed. This is why the FBI asked Apple to create a specially modified version of the iPhone encryption container that would not delete the keys after 10 incorrect attempts. With a simple six-digit pin, it would take seconds to recover the pin if it could be attacked directly. The concern is that if this modified security container were ever stolen from Apple or the FBI, it could be used to easily defeat the security of millions of other iPhones. It appears that the FBI has found an alternative way to access the iPhone in the San Bernardino case, but the same issues will be raised in other cases and with other manufacturers.

Whatever method the FBI used, it allowed them to recover the password and not defeat the actual encryption, because passwords are inherently weaker than the underlying encryption. However, passwords will continue to be used because they are an easy and convenient way to secure data. To keep data secure it is important to recognize and account for their inherent weakness. There are many simple steps you can take to keep your data secure. Use longer, more complex passwords that are not based on a word found in the dictionary and use different passwords across different types of devices. While your computer may be secured using a TPM chip, using the same password to secure files may defeat the TPM's added protection. If you receive an email stating there is a problem with your account, type the website address into your Web browser instead of clicking on any links in the email, or call the company where your account is located. Generally, no one should ever request your password. If a situation occurs where your password is required, it should be provided over the phone and not by email. These few steps can help protect you and your clients' data.

*Kevin Baker is a senior manager and head of the digital forensics practice in Marcum LLP's Philadelphia office.*