.Introduction to Cryptography for Non-Technical Personnel, Part 2

.How Real Is The Threat Of Someone Snooping Into My Information (Files)?

The answer to this question will vary, depending upon your particular situation. This white paper describes possible scenarios of unauthorized access (snooping) into your information. Whether these scenarios apply to you can only be answered by yourself or an expert in computers and/or security in your organization.

..Competition

It is realistic to assume that your competitors may attempt to obtain your proprietary information. Your competitor may call you on the phone and ask you questions or your competitor may surreptitiously try to steal your information.

If you do not openly reveal your information to competitors, then guarding your information is vital. If the information exists in a computer file (word processor document, spread sheet, drawing, images, etc.) then it can be protected by file encryption, using a program such as KetuFile. Files that have been encrypted will be both ‘safe at rest’ and ‘safe in transit’. Specifically, whether someone tries to look into your computer’s hard disk or intercept your email, if the information is encrypted, then it is much safer.

..Accidents

Ask any attorney in a legal practice about the time someone in the law firm sent a letter to a client, but it was the wrong client. Sometimes it could have been an adversarial client! It does happen. Critical and often damaging information is accidentally revealed to the wrong person or organization. If that information had been encrypted first, then the unintended recipient would not have been able to unscramble it, and no compromise would have occurred.

If you handle critical information, then guarding your information from unintentional disclosure is vital. If the information exists in a computer file, then it can be guarded/protected by file encryption, using a program such as KetuFile. It is a simple and efficient approach to helping to prevent accidental disclosures.

..Personal Files (Including Medical and Financial Records)

Most people have a private part of their lives. They may close the door of their office when speaking with family members. They close the doors of their house, and may draw the blinds shut. They may not have anything that they consider to be ‘secret’ from the rest of the world, but they still want some privacy. Guarding of information is both common and natural.

In many organizational settings, guarding of information is both of paramount importance as well as a legal requirement. Many businesses must adhere to strict government regulations to protect information. This ranges from the medical profession’s files of their patients’ health matters to financial organizations’ files of the finances and their clients.

Regardless of whether you desire to keep information guarded for general principles or because it is required by law, if the information exists in a computer, then it can be guarded/protected by file encryption, using a program such as KetuFile. It is a simple and efficient approach to prevent disclosures and accommodate non-disclosure requirements.

..National Defense - Homeland Security

There are many government contractor and other entities that must heavily guard the information they handle each day, as required by federal law. If the information that must be protected exists in a computer file, then it can be guarded/protected by file encryption, using a program such as KetuFile. As described later in this whitepaper, the KetuFile encryption program utilizes the latest encryption standard of the U.S. government.

. How Effective Is The KetuFile Encryption Program?

..Introduction
When discussing the effectiveness of an encryption technology, we can approach the topic by posing the question, ‘How easy is it to attack an encrypted file?’.

..Attacks
When an attack is made on an encrypted file (message), this is referred-to as 'cracking'. Cracking means that someone is trying to de-encrypt your encrypted file (message) without having your key. In attempting to crack a particular technique of encryption, one could divide the approaches into two categories: brute force attacks, and intelligent attacks

..Attacks - Brute Force
In a brute force attack, also known as an exhaustive key search, every possible key (numbers and letters, for example) will be tried to crack the encrypted file (message). Using today’s electronic systems, it is trivial to make the number of key combinations so large that a brute force attack will be entirely unrealistic with the technology available in the next 10 years or so.

..Attacks - Intelligent
In an intelligent attack, mathematicians use number theory to find a faster way to crack than the brute force attack.

..Evolution Of Attacks
As time goes on, mathematicians will develop new theories and approaches to make intelligent attacks on the latest encryption techniques. It may therefore happen that after a period of time, any given encryption technique is no longer robust, i.e. someone with enough funding can use the newly-developed intelligent approach and assemble the necessary electronics to crack a file (message) in some reasonable period of time.

..Why KetuFile?
KetuFile is an encryption utility program that acknowledges both of the above possible attacks. Specifically:

- a large key, 256 bits or 512 bits, to make a brute force attack take an astronomical amount of time with technology of today and the foreseeable future.

- the latest U.S. standard for encryption, the Advanced Encryption Standard (AES), to offer what is one of the strongest resistances against intelligent attacks in the world today.

..Robustness Of AES
There is a large and highly competent community of mathematicians and other scientists in the world today that can offer considered opinions on the robustness of AES and compare AES to older encryption techniques. AES is the result of a global competition for the new U.S. standard.

..Robustness Of KetuFile
The robustness of KetuFile rests on the robustness of AES, the randomness of the key that the user selects and the fact that there are no 'back doors' whatsoever in KetuFile and additionally, there are no built in 'key recovery' features. Said another way, if you lose your key and ask the KetuFile manufacturer for help in recovering the original of the encrypted message, there is nothing we can do for you. Please read on.

..Back Doors
'Back Door' is a widely used term-of-art. In the case of KetuFile, it would refer to the existence of a de-encryption process that can be applied to a given encrypted file (message), that does not need the original encrypting key. If an encryption product has such a back door it is crippled. There are no 'back doors' whatsoever in KetuFile.

..Key Recovery

'Key Recovery' means that there is a way that the user's key can be deduced from either the encrypted file (message), i.e. the key is secretly buried in the encrypted file (message), or some other approach allows a third party to get or generate any users key. If an encryption product has such a key recovery feature, it is crippled. There are no 'key recovery' features whatsoever in KetuFile.

On the other hand, if you scour the literature for papers on one of the most popular encryption techniques of today, you will find a reference to the inclusion of key recovery in that product.

..A Few Notes On Key Selection

You should only use random keys. This means using sequences of letters and numbers that don't make any sense. Don't use words, phrases, or terms from any language or from any industry or discipline. People who are specialists in cracking encrypted files (messages) have a wealth of dictionaries that contain all of these terms and phrases. If you use such words, phrases or terms it can be billions of times easier (faster) to crack your encrypted file (message). Using a dictionary as just described is called a 'dictionary attack'.

Do not use existing numbers in your key. These include all aspects of personal data (phone, street address, SSN, etc.) as well as model numbers of some favorite piece of equipment, and other catchy or familiar numbers.

..Conclusions

There are many reasons to guard your information ranging from simple personal preference to the dictates of governmental laws. If the information that you need to guard exists on a PC, then it is almost certainly a file and can be protected with a file encryption program. The KetuFile encryption program provides a very strong file encryption based upon the latest U.S. government standard.