Enkryptr – The File Encryption Program

Brett Somerville, Avi Oppenheimer, Collin Galvez

Abstract – File security is a very important aspect of cybersecurity. Sending unencrypted important files across the internet poses a risk to those files. Even leaving important files unencrypted on a computer can be dangerous, as someone can use a vulnerability, or even physically break into a system. Enkryptr is a file encryption program, that allows you to encrypt many different types of files, as well as unencrypt those same files. Enkryptr allows for several different kinds of encryption to be used, while allowing the user to select what type of encryption they want to use on their files. This program will dispense a key to the user after encryption, that the user can use to unencrypt the files they have encrypted. This ensures both file security and file integrity, as the encryption allows security, while also allowing people that only have the key to be able to unencrypt the important files.

Keywords: ecryption, file, Enkryptr

Introduction

Both file security and file security are very important today simply because technology is drastically expanding in our society. Only people who are authorized to see specific files should be able to do so and most files are unencrypted on computers. If a computer is broken into, such as an office computer for a company, it can be costly for that company because it leaves those files unprotected and vulnerable to attacks. The same pertains to files being sent through emails. If someone has access to someone's email when they do not have permission to, they can view those unencrypted files.

File Encyrption

A. *What is file encryption?*

To begin with, file encryption can protect individual files or file systems by encrypting them with a specific key. This makes it accessible to only the keyholder and the goal of this is to prevent malicious or unauthorized parties from accessing the files. The programming for file encryption can be created into the operating system or file system. File encryption is also a way to secure files and make their contents unreadable. There is a lot of ransomware that uses file encryption methods for malicious purposes but using this type of encryption software can secure the files contents, by only making sure the people with the key can see it.

B. Pros and cons of Data Encryption

There are many pros and cons of data encryption. One pro is that your data is safe for the most part. When it comes to breaking the encryption for a set of data is the same meaning as how long it will take to crack it by using brute force. Some of the methods of using encryption have become so much easier because of the use of technology. For certain websites, HTTPS encryption no longer requires high levels of web admin. A con would be that there are performance penalties. When using encryption there is an extra step involved in data retrieval and the transmission process. Also, using encryption involves the application of mathematical operations to every little piece of data. This puts extra pressure on the processor. Checking the sort of performance impact encryption will have on whatever machine is being used is essential to where encryption can be used. Performance of various encryption methods is different so the need for speed and security must be balanced against one another. Another downside to data encryption is that if the key to the file is lost, the file can be rendered unusable and unrecoverable. This, however, is both an advantage and disadvantage of data encryption. It provides a deep layer of security and is hard to break, but if someone were to lose their encryption key, the file would become useless.

C. Types of Data Encryption

When it comes to protecting data there is one thing to consider. "What type of encryption to use?" There are different types to choose from. We need to know how Data encryption works. The idea is one has a plaintext that needs to be encrypted so then it goes through the cipher process. Then the document is encrypted. In order decrypt the same key needs to be used to figure out the plaintext. The most common encryption methods are first the Advanced Encryption Standard (AES) that uses 128 bits at a time. While using up to 256 bits to decrypt a message. Second method is the Rivest-Shamir-Adleman (RSA). It is based on the factoring of the product of two usually big prime numbers. Third is Triple DES known from encrypting data using a 56-bit key. How this algorithm works is applying a cipher three times to each data block. Lastly, there is the Twofish encryption method. The cipher uses 128 bits and widely considered as more versatile than Blowfish (another encryption method). The notable thing about Twofish is it encrypts data in 16 rounds and regardless of its key size.

D. Implementation

Enkryptr's use will be to implement a style of encryption best suited for file encryption. The program will be able to encrypt several file types. The current supported file types will be Microsoft Word Documents, text files, PDFs, and Microsoft Excel Documents. These are common types of files that often need to be encrypted. Enkryptr will take these files in, encrypt them, and produce an unreadable file. This unreadable file will be inaccessible to those individuals without the key. After the encryption process is finished and an unreadable file is produced, a key will be securely provided to the user. Enkryptr will also provide the user a way to unencrypt the file using the key. Once the user receives their key, it will be their responsibility to keep that key safe. As of right now, there may not be a key recovery system implemented. The purpose of Enkryptr is to make files unreadable and secure. If a key was easy to recover, then that would be a security issue that would lead to exploitation for malicious purposes.

It is currently unknown the type of encryption algorithm that will be used to encrypt the files. As stated earlier, the encryption method will be like methods used by ransomware, only without the malicious intent of those programs. More research is needed going forward in terms of encryption methods that will be implemented within the program. As of right now, Enkryptr will not have the ability to encrypt picture or video files. Potentially in the future, Enkryptr will have the ability to encrypt other different file types, however as of right now, Enkryptr will only have the ability to encrypt the file types that were listed above.

Enkryptr is also a program that will be open-sourced, so the source code be modified and viewed by other users. One completed, Enkryptr will be placed online for other users.

References

[1] M. Allan, "6 types of encryption that you must know about!," GoodCore , 09-Jul-2021. [Online].

[2] Butler , S. (2018, August 20). The Pros and cons of Data Encryption. TechNadu. Retrieved February 11, 2022, from https://www.technadu.com/pros-and-cons-of-data-encryption/38599/

[3] Z. Capers , 4 Common Encryption Methods to Shield Sensitive Data From Prying Eyes, 22-Jul-2021

[4] Stieglitz, J. (2020, November 29). Encryption: Pros and cons: Imperva. Blog. Retrieved February 11, 2022, from https://www.imperva.com/blog/encryption-pros-and-cons/

[5] What is encryption? Data Encryption defined. IBM. (n.d.). Retrieved February 12, 2022, from https://www.ibm.com/topics/encryption