Security concerns for confidential files being worked on in insecure environments due to the “work from home” orders to combat Covid-19

University of Northampton Internet technology and Security

***Abstract***

***In this paper I am going to be looking at the security concerns for confidential files being worked on in insecure environments pertaining to the “work from home” orders to combat covid19. To do this I am going to be looking at both symmetric and asymmetric encryption and how he can combine them to create a solution to the identified security concerns which takes the shape of a file encryption program.***

I. INTRODUCTION

On March the 23rd 2020 the UK prime minister Boris Johnson made a public announcement that *“Britons should only go outside to buy food, to exercise once a day, or to go to work if they absolutely cannot work from home. Citizens will face police fines for failure to comply with these new measures.”* [1] This signalled that most work companies if they had not already needed to start making there employs work from home. This came with a multitude of issues which where inherently exacerbated by the fact that it was all being done under a time of uncertainty and on an extremely tight time schedule and in many cases a shoestring budget. All this combined to give us an environment that bred security issues. In this paper I am going to be focusing on one of the security concerns that was brought about by a hasty introduction of remote working. To give this some numbers in January and February about 5.7% of workers where working from home[2] In April the same year (2020) this had risen to 43.1% of workers working from home[2]. As stated before this was done quickly which meant there was no time for proper training or the time to implement secure online working environments. This led to many inexperienced users saving and working on secure company files on their personal computer. In a cyber crime review commissioned by the UK government in October 2013 which was undertaken by Dr. Mike McGuire (University of Surrey) and Samantha Dowling (Home Office Science) found that 33% of people over the age of 16 had reported at least one instance of a computer virus[3].

This meant that there was a real possibility of old or inexperienced users being target on their personal pc’s to gain access to company files that are usually lockdown behind multiple security layers and being monitored by a professional I.T teams. In this paper I am going to be exploring one solution to this problem. To do this going to research how both AES (symmetric) and RSA (asymmetric) encryption can help us secure the files that are being stored and worked on. By using both AES (symmetric) and RSA (asymmetric) encryption we can extract the benefits of each while negating some of limitations of each encryption method.

The major issues faced with project is providing a solution that provides a good level of security but it easy enough that within a small amount of training everyone at a company regardless of their computing knowledge can use the program. This can be accomplished by using a GUI based program that has simple one click encryption for all file types and folders. Another issue is that of protecting the private key used to encrypt the files we get around this by using a asymmetric encryption algorithm (RSA) to encrypt the private key allowing the sharing of a public key to people needing to encrypt files but not decrypt them.

The implementation and conclusion of this paper is only one way to approach the problem at hand. Others have suggested additional solutions Bernardi Pranggono and Abdullahi Arabo published a paper called [5] COIVD-19 pandemic cybersecurity issues they suggested that user education was an extremely important factor and found that only 11% of business have provided cybersecurity training for their employees they also concluded that multifactor authentication the use of VPNs as well a strong company against storing documents or information locally as well as making sure physical devices are logged off and stored in secure locations.

Prof. (Dr). Tabrez Ahmad also came to similar conclusions in his [6] paper Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity another suggestion from this paper was to keep work contained on supplied devices from the company you work for as well as echoing the statements from Bernardi Pranggono and Abdullahi Arabo about keeping devices up to date and well as personnel training.

II. SECURITY CHARACTERISTICS/FEATURES

Now I have identified a security issue we now need to look at potential attack vectors as well as the vulnerability’s that I need to solve with this implementation.

The first attack vector is through a virus based attack against the victim this could be through the use of a RAT (Remote Access Trojan) these as the name may suggest a virus that look like one program but actually contain code that allows an attacker almost complete control over a user’s pc. As well as RATs viruses such as worm can replicate them selves through out a network allowing an attacker to attack one device on the network and then be able to steal data from all devices on the network.

The second attack vector is by an attacker gaining physical access to a device this could be as simple as plugging in a USB and copying important files over to actually stealing the device its self allowing them to look over all the data on the machine at their own convenance.

III. SECURITY MODEL

Now that the possible attack vectors have been identified we now need to build a security model. A security model is used to make sure that the solution is well balanced in all aspects of its security. The first issue that we need to solve is confidentiality for us confidentiality means that we need to make sure an attacker can not use an attack vector to gain access to confidential information we do this by encrypting the data so even if an attacker gets hold of this data he/she cant read or look at it. We also solve confidentiality by making the user input a unique key that is used so that even if one users private key is comprised other users encrypted data is not. The next thing we need to do is make sure if integrity this ensures that any changes that we make are reflected. To do this we make sure that when a file is encrypted a unencrypted version of this file is not left behind that could be stolen in which case we would loose confidentiality as the data could be read to stop this we delete the unencrypted version of the file as soon as the encrypted file/folder is created. Then finally we need to make sure of the availability of the data as its important that the data its self can be access by authorised personal (We know there authorised due to confidentiality checks) We have done this by including a simple one click decryption allowing authorised users to quickly access the data with the lowest amount of hassle necessary.

IV. ENCRYPTION METHODS

The main encryption method I am going to use is AES this is a symmetric encryption method and is perfectly suited to encrypting files due to its increased performance and great compatibility due to its simplicity. In addition to this it is used by the United states government to encrypt sensitive data so we know that it’s been well tested and is secure.

AES also know as Advanced Encryption Standard is a subset of the [4] Rijndael block cipher developed for the United states government in 1997 after their old algorithm DES (Data Encryption standard) became vulnerable to a brute force attack. Which is where a computer tries every possible combination of letters, numbers and symbols depending on what its attacking these attacks only become possible when an algorithm becomes outdated compared the relative computing power of the fastest computers of the time period. AES comes in three different key sizes 128,192 or 256 but all keep the block size of 128.

The AES algorithm works by taking the data as a block and then applying alternating rounds of [figure 1] substitution and permutation. The size of the box is determined by the key sizes with 128 being default and then 192 and 256 being convectively more secure but slower

# 

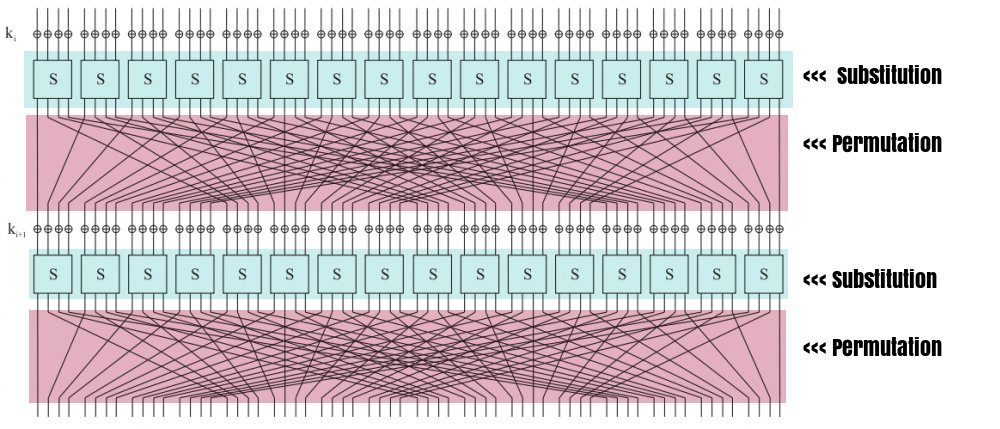


Figure 1

https://crypto.stackexchange.com/questions/8487/the-exact-difference-between-a-permutation-and-a-substitution

We will also be using the RSA encryption method although this is reserved for just encrypting our AES private key this allows us better flexibility with a program by letting us give out a public key which will then let users encrypt files but not be able unencrypt them this is useful if you want an to encrypt a file before you send it to another person at the company but they don’t want to share their private key over an unsecure method such as email the can send you the public key over email you can then encrypt the file and send it to them and then they and unencrypt when they need to use it.

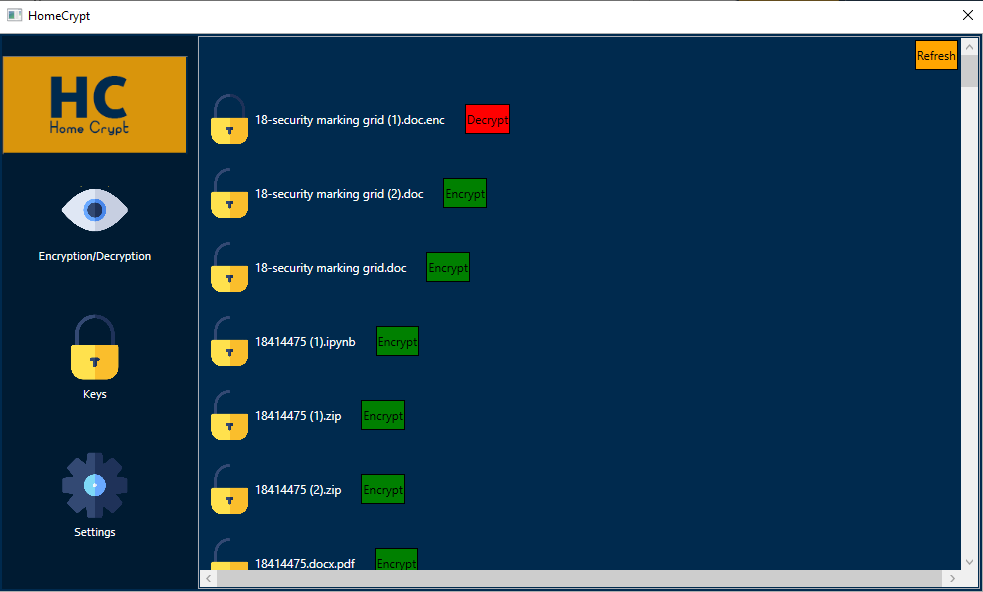
RSA encryption is an asymmetric algorithm which stands for Rivest Shamir Adleman (the surname of the creators Ron Rivest, Adi Shamir and Lenard Adleman). RSA was developed as a secure way to be able transfer information over an unsecure network by solving the issue that symmetric encryptions algorithms have which is to be able to encrypt a message you need to have the private key which can also unencrypt the message and therefor if a hacker/third party gets hold of this key they can unencrypt all communications whereas RSA and other asymmetric algorithms have a public and private key which allows the public key to be given out and if a hacker/third party gets hold of this key it doesn’t matter as it can only be used to encrypt a message not decrypt it which can only be done using the private key that does not need to be shared.

RSA encryption works on the idea that its easy to compute values together but much harder for that compute of values to be reversed this is know as a trap door function. Its implementation in RSA works by generating two prime numbers. The longer the length of each prime number the more secure the encryption is the key sizes range from 1024 to 4096. Something to note here is that is an 829 bit key has been cracked so it may be prevalent to use a higher key size to future proof you encryption.

V. SOLUTION

The final solution is to create a [figure 2]custom file encryption program which uses both AES for the file encryption its self which for fills the confidentiality part of our security model as well as RSA to allow an encryption key that people can use to encrypt there files but not be able to decrypt to be safely give out. Which helps us increase our security by not having to send out a private key which we would have to do if we only used AES. To do this the C# language has been used as it provides excellent support for creating simple and intuitive GUI’s this helps with data integrity and data availability as the GUI can clearly show what data in encrypted and which makes it easy for them to encrypt and decrypt the data allowing for easy access therefore making the data available easily for fulling the availability part of our security model and making sure the users knows what data is encrypted and which isn’t which helps with our data integrity. It also natively supports AES and RSA encryption and decryption using there built in cryptography library. This means we do not need to rely on third party libraries which can contain bugs and add unnecessary bloat to our software. AS well as excellent compatibility and stability on the windows operating system due to it being designed to run on windows. Unfortunately, this means that windows is the only operating system it will run on currently which is ok as windows is by far the most popular operating system but future support for mac os or linux would be a benefit.

Figure 2



The solution works by first getting the user to select a working directory then allowing them to input a AES key or to use the default one it will then create a pair of RSA public and private keys using this AES key once these RSA keys have been generated a one click encrypt and decrypt button will appear next to every file in the [figure 2] GUI and then the user will be simply be able to click encrypt when they have finished working on a document or file and then when they need to work on it again they will simply be able to press the decrypt button and then go back to working on the document or file again. It supports all file types including zip and rar files as well as has support for sub folders that are located in the selected workspace.

V. COMPARISON WITH OTHER FILE ENCYPTION SOFTWARE

Bit locker: An encryption program that comes as standard within the windows operating system can provide partial or full disk encryption but does not allow file by file encryption which is what is ideal for our users due to the possible issues which could crop up due to accidental full disk encryption and the loss of credentials resulting in the loss of data resulting in the loss of availability in our security model.

Vera Crypt: This provides a file encryption service but does not support the use of asymmetric encryption on the private key which is used by the symmetric encryption algorithm (AES) which means we cannot have a public/private key functionality on top of this it is designed for experienced users which gives it great versatility but is not advantages when trying to get massive adoption with novice computer users which could increase mishaps in data integrity from the security model as users may think a file is encrypted when it’s not or a unencrypted version Is left behind.

VI. CONCULSION

In conclusion the solution protects against our potential attack vectors by keep data secure even though its being stored in an insecure location and therefore for evne if an attacker gains access to the files/data they will not be able to break its confidentiality. This solution works as a stop gap by securing the data but a more permeant and well-rounded solution should be worked towards such as the use of an online working environment, so no confidential files are worked on locally. The suggestions of Bernardi Pranggono and Abdullahi Arabo and Prof. (Dr). Tabrez Ahmad of user training as well the as the use of multi factor authentication and VPNs should also be considered as well as these helps provide extra protection when transferring or accessing files and data. For a future direction the auto encrypting of downloaded files/data could make sure files do not sit unencrypted on the user’s computer would enhance the protection of the software as well as more research into possible online solutions such as a dedicated online working environment would be useful.

REFERENCES

[1] <https://bfpg.co.uk/2020/04/covid-19-timeline/>

[2]https://wiserd.ac.uk/sites/default/files/documents/Homeworking%20in%20the%20UK\_Report\_Final\_3.pdf

[3]<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf>

[4] https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf

[5] <https://www.researchgate.net/publication/345262445_COVID-19_pandemic_cybersecurity_issues>

[6] https://www.researchgate.net/publication/340443250\_Corona\_Virus\_COVID-19\_Pandemic\_and\_Work\_from\_Home\_Challenges\_of\_Cybercrimes\_and\_Cybersecurity