Volume-2, Issue-7, November-2018: 326-336
International Journal of Recent Innovations in Academic Research ISSN: 2635-3040

Anti-Keylogging Software Using Asymmetric Key Encryption Algorithm for Non-Hybrid Keyloggers

Francis Balazon, DIT

Batangas State University Lipa City
E-mail: fbalazon@yahoo.com

Abstract: The study entitled Anti-Keylogging Software Using Asymmetric Key encryption Algorithm for Non-Hybrid Keyloggers focused on blocking the keylogger in capturing sessions and keystrokes. The reseracher analyzed different studies to develop a system to eliminate the threat of information and data theft. The proposed system utilized Asymmetric-Key encryption, the best algorithm in securing data and messages. The software development methodology used in developing the system was rapid application development (RAD). In addition, the software development tool used was Visual Studio 2015.The respondents rated the system as highly acceptable in terms of intercepting keystrokes recorded by the keylogger. The proposed system Anti-Keylogging Sofware using Asymmetric-Key Encryption can block approximately 99% of logs and activites for non-hybrid keyloggers via keystrokes. This proposed system helps computer users in protecting their sensitive information or transaction online.
Keywords: Cipher text, cryptography, decryption, encryption, blowfish.

Citation: Francis Balazon. 2018. Anti-Keylogging Software Using Asymmetric Key Encryption Algorithm For Non-Hybrid Keyloggers. International Journal of Recent Innovations in Academic Research, 2(7): 326-336.

Introduction

Anti-Keystroke Logger is a type of software specially designed for the detection of keystroke logger software records [1]. Families and business people use key loggers legally to monitor the network usage without their users' direct knowledge [2]. However, malicious individuals can use key loggers on public computers to steal passwords or credit card information. Browser nowadays may be vulnerable to a web based attack, and by visiting a malicious website, the malicious website may cause computer to download and install malware, Trojan and keylogger. Technically, a keylogger is only a piece of code that logs keystrokes. It could be a part or only a feature of a Trojan horse or a malware.

Because malware can easily intrude comptuers in numerous ways [3], counter measures such as Anti-Keyloggers are developed to thwart keylogging systems. However, there are only often effective when used properly. Antiviruses helps keystroke logging software in recording keystrokes but they do not provide 100% security from keyloggers. An antivirus works on the basis of known signatures, and if the new keylogger signature is unknown, the antivirus will not report it. Since Anti-keyloggers have been designed specifically to block keyloggers, they are potentially more effective than conventional anti-virus software because

some anti-virus software does not consider certain keylogger a virus, as under some circumstances, a keylogger can be considered a legitimate piece of software [4].

Keyloggers are often installed and used by people, particularly by an expartner to spy on his expartner's activities. This kind of protection is passive. The maker of the keyloggers can easily change the signature to avoid being detected by anti-spywares, thus keyloggers easily threaten the users of PC, especially the online activities are growing rapidly in these years. Since online activities rapidly grow nowadays, it is alarming that keyloggers can access data easily. Evidently, news had reported that somebody lost money in banks because the account and password were stolen by keyloggers [5].

The keylogger issue comes from the open system, both in hardware and software. It could be solved through the encryption of data packet from the strat site to destination site. It means to encrypt the data before it is outputted from keyboard, and decrypt the data at the destination application. The keylogger can only log the encrypted data of the keyboard. Hence, the problem is solved.

Anti-key logging is used to provide security on private and confidential information. Traditional authentication systems used to protect access to online services (such as passwords) are vulnerable to compromise via the introduction of a keystroke logger to the service user's computer [6]. This has become a particular problem now that many malicious programs have keystroke logging capabilities. Because the attackers are constantly refining their techniques to steal information, the needs to secure information against the malware and spyware make key logging software more significant.

This research is intended to block keystroke logs on browser and local software. This would be useful since other existing anti-keystroke logger only blocks key logger on browsers. Now that some banks and other money transactions are using internet in making transaction with the client, malwares and spyware that had have loggers are all over the web to steal information. This research helps users to secure private and confidential information.

This study aimed to develop a software which can block keystroke logger sofwatre that records keystroke and previously typed letters. Asymetric cyptography was used to gather the required data to encrypt the content of the information. The developed software can help individual to secure his private information such as user password and credit card numbers. This can prevent cyber bullying because some hacker uses keylogger software to steal user and password to hack private accounts.

Considering that asymmetric cryptography is slower than symmetric encryption, the software is limited to 128 bytes of keystrokes only. Also, it is only applicab;e or availbale on Windows operating system. Moreover, some companies and organizations could not use the keylogger to monitor their employees, network usage and manage accounts on the management. It could not also dtect if there is a keylogger installed on a machine. It will only bypass the keylogger, thus the keystrokes will not be recorded.

Methodology

A. Development Approach

This project used Rapid Application methology. Rapid application development is a software development methodology that uses minimal planning in favor of rapid prototyping. A

prototype is a working model that is functionally equivalent to a component of the product [7].

B. Crypto-systems Process

This involves the study of the activity procedure and method of the proposed system in order to have a full knowledge of the problems. The major activities in the crypto-systems include cryptography key, cipher, plaintext, windows library such as user32 and kernel 32.

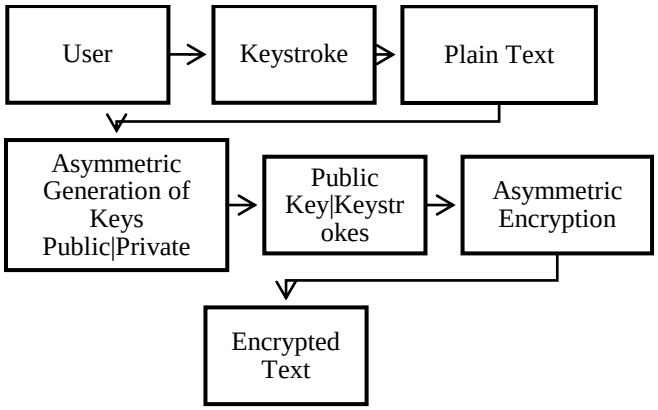

Figure 1. Data Encryption with Asymmetric Key Encryption

Figure 1 shows the process involved in the encryption process with asymmetric key encryption. The process starts when the user presses a key on the keyboard and converts it to plaintext. This plaintext contains alpha or numeric character that serves as the input of the user. The plaintext goes to the process of asymmetric encryption. It will be converted into encrypted value. This process of algorithm uses 2 different keys which are public and private keys. The public key will be used to encrypt the keystroke, and the decryption will be used to return the decrypted keystroke to where the user is inputting a data to prevent hindrance in typing, such that the key pressed is not appearing.

Application of Asymmetric Encryption and Blocking Keystrokes

As compared to other encryption processes, the application of asymmetric process made, the recorded strokes secured, resulting to a random typed characters. Asymmetric Encryption never needs to be transmitted or revealed to anyone and in secret-key system, by contrast, the secret key must be transmitted (either manually or through a communication panel) since the same key is used for encryption and decryption [8].

In terms of data protection, the proponent used real time encryption. The encryption occurs whenever the keys are pressed. Because the length of keys makes the data hard to decrypt, decryption is not considered in the process.

Another way to secure data is to remove the means of using private keys for decryption and to use the public on the process only.

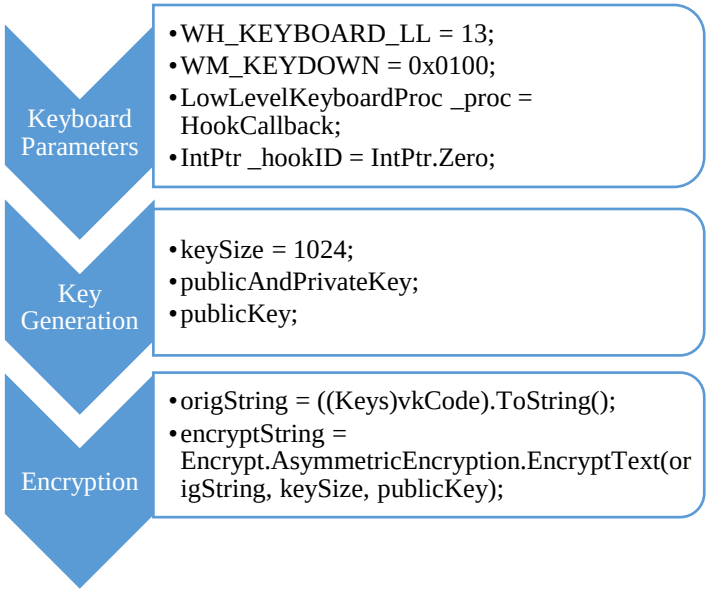

Figure 2. Application of Encryption on Keyboard Parameters

Figure 2 Shows how encryption is applied in this project. Inside the keyboard parameters are the declarations for the keyboard. Using the Windows API for keyboard the proponent used the low level keyboard hook to capture the keys pressed by the user. By doing this, the captured keys are converted into text which proceed to encryption. Inside the key generation are the variables used to store the generated keys, and size of keys to be generated. This keys are used to encrypt and decrypt the keys pressed by the user. Then, the encryption parameters are the variables used to create string of the keys pressed by the user. The "Origstring" Which contains the keystroke is encrypted by putting it on the "Encryptstring. Encrypt. Asymmetric encryption. Encrypt text" which is responsible for encrypting the origstring. Asymmetric encryption handles the class used to make the parameters of the asymmetric encryption, which is the algorithm used in this project.

Results and Discussions

This software was developed by gathering information about keyloggers. Using this data, proponent developed a software which countermeasures it. Keylogger software can record and log the user's activities and it mainly affect its user's keystroke activities.

When the user presses a key on the keyboard, the software will recognize it as the keystrokes and converts it to plain text. Plain text convert into a mathematical value, which is used to generate the asymmetrical pair of key, the public and private key. Public key is used to encrypt the plain text, the private key is used to decrypt the text, and sends back to where the users input the data or information. To avoid the instance where no character appears after pressing a letter or character on the keyboard, or a different letter shows to what is intended to appear on the application while the user is inputting the data or information, decryption is used.

When the user executes the program launcher, it will request to enable keylogger. Then, the application will enable anti-keylogger if the user chooses to use the anti-keylogger. If the user chooses not to use the anti-keylogger, it will proceed to normal keyboard input, else it will enable the anti-keylogger . If the anti-keylogger is executed then, the user will choose which security will be applied. If the security parameters are not changed, the flow goes and waits

keyboard input user's data. After inputting the data, which is encrypted, the program starts to decode the user input data from anti-keylogger keyboard. Lastly, the decrypted input will be sent application client.

Anti-keylogger Execution Flowchart Intercept Keys

Figure 3 shows the application's flowchart. This illustrates how the application really works. For further explanation, the researcher separated every function for more precise explanation and for the easy understanding of the said application.

In this case, the proponent developed a program to intercept or block the key-loggers. This anti-keystrokke logging is designed to encrypy keystrokes to ensure security on information among users. This program is intended to secure desktop from any hackers and keylogger threats. This program integrates two features, one is a anti-keylogger and the other is browser security which entraps browser on a new desktop.

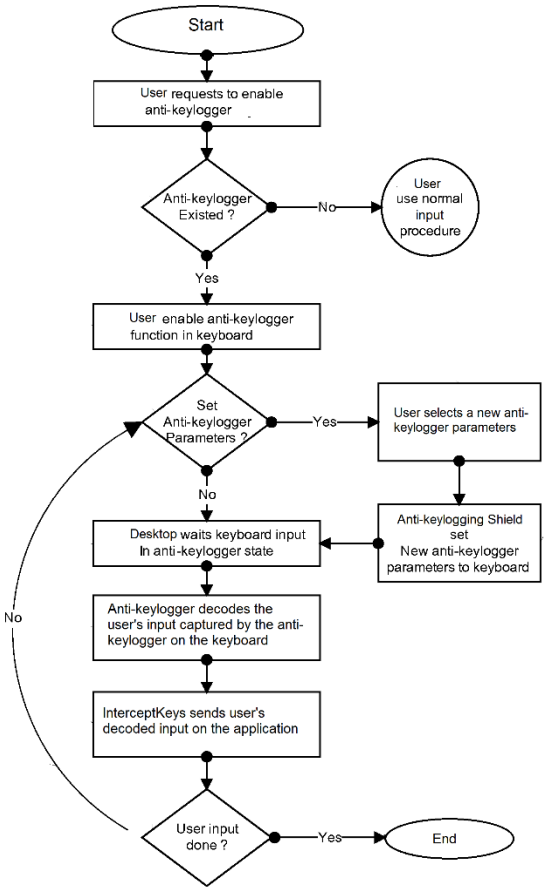

Figure 3. Anti-keylogger Execution Flowchart

Intercept Keys

This software is developed to gather information about keyloggers and how they works. Using these data, the proponent developed a software which countermeasure keyloggers. Keylogger software can record and log the user's activities and it mainly affects user's keystroke activities. When the user presses a key on the keyboard, the software will recognize it as the keystrokes and converts it to plain text. Plain text converts into a mathematical value, which is used to generate the asymmetrical pair of key, the public and private key. Public key

is used to encrypt the plain text, the private key is used to decrypt the text, and sends back to where the users input the data or information. To avoid the instance where no character appears after pressing a letter or character on the keyboard, or a different letter shows to what is intended to appear on the application while the user is inputting the data or information, decryption is used.

User Interface and Folder Paths

The proponent didn't make any interface in this project beecause some user may close the program accidentally. The proponent placed it on the background process in the task manager so that user can still be able to close the program.

Figure 4. User Interface

Fugure 4 shows the user interface of the system. (1) Anti-Keylogging Protection Switch activates and deactivates the program; (2) Browser button, is responsible for finding the executable browser's folder path; and (3) Run button will run the secured browser. The user will choose a browser, locate its folder path and choose the executable browser. Then the user will click the "Run" button to start secured browser.

Figure 5. Activated Interface

Figure 5 shows icon changes when the Anti-Keylogger software is fully activated and running on the computer. The browser icon appears after choosing it from the folder destination.

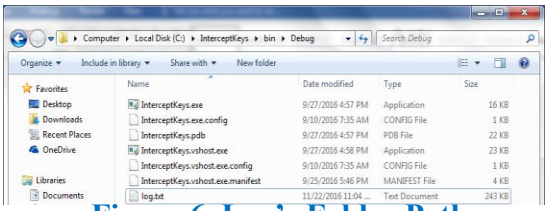

Figure 6. Log's Folder Path

Figure 6 shows that the log file made by the program is visible to ensure that none of his/her keystrokes are recorded even by the ceator of the program.

System Testing Result

In this part of the study, tests were made by experts in IT tp assess the security, effectiveness and efficiency of the program developed by the proponent.

Security

Test Sample 1

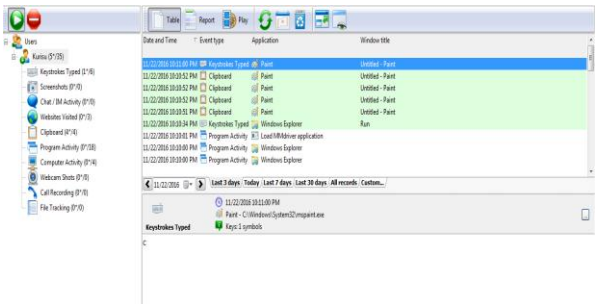

Figure 7. Refog Keylogger

Figure 7 shows the keylogger running on the computer before the execution of the program. IT experts tested the program by installing keylogger on one of the laptop. It shows that the program made by the proponent was unable to intercept the keylogging of the Refog Key-logger.

Test Sample 2

Figure 8 shows that a key has been tapped.

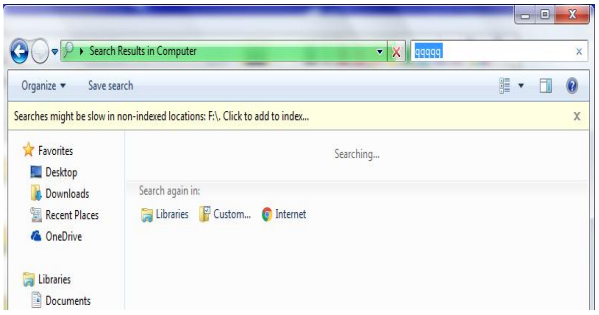

Figure 8. Keystroke Test

Figure 8 shows the key pressed to test whether the keylogger captured the keystrokes made. Every letter typed in this figure was recorded and was captured by the keylogger.

Figure 9 shows the sessions and logs of the activities made by the tester.

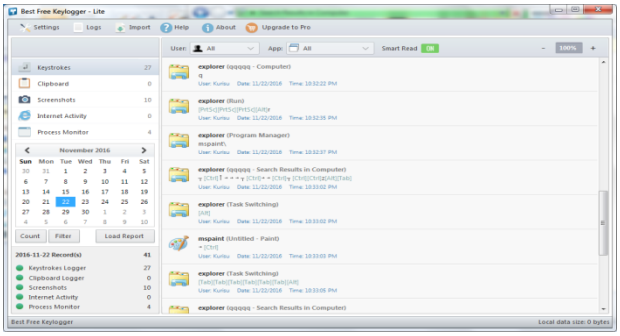

Figure 9. Best Free Keylogger Logs

Figure 9 shows that the keystrokes made by the tester were being monitored and captured by the keylogger before the execution of the program made by the proponent.

Figure 10 shows that the InterceptKeys.exe had been activated.

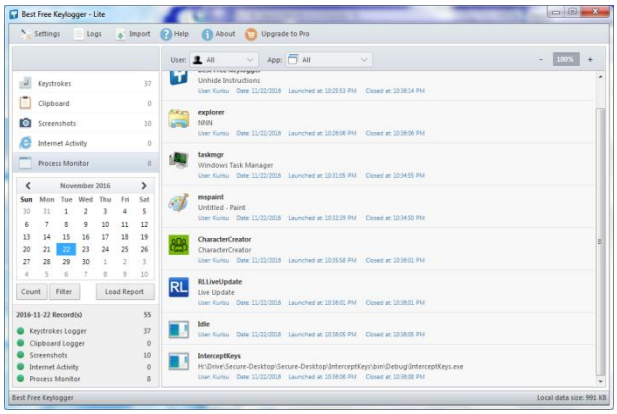

Figure 10. Program Executed

Figure 10 shows that InterceptKeys.exe was executed in the user activity logs of the keylogger. This proved that the program was run and readied in testing. In this figure, the time the program was executed is also presented.

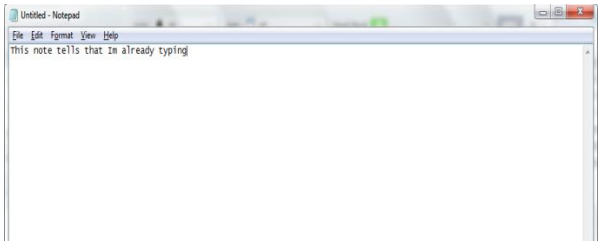

Figure 11. Testing after execution

Figure 11 shows that the tester had already pressed a key on the keyboard.

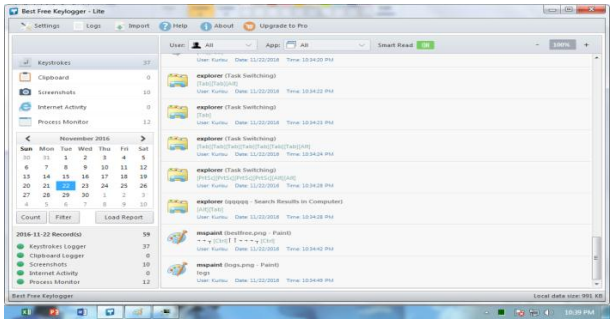

Figure 12. Logs after execution

Figure 12 shows that the keystrokes made on the notepad were not captured by the keylogger.

Effectiveness

This section presents the results of testing and evaluation of the effectiveness of the program on the security on a user's desktop. Further, results are discussed below.

Table 1. Keystrokes and Screen Capture Test

	Keylogger	Screen Capture		Keystrokes	
		Passed	Failed	Passed	Failed
Intercept Keys.exe	Refog Keylogger	✓			✓
	Best Free Keylogger		✓	✓	
	Intercept Keys (custom)	✓		✓	

Table 1 presents the test result on various known key-loggers. This shows that this system was successful in intercepting the key-loggers on recording keystrokes.

Table 2. Remote Desktop Test

	Keylogger	Screen Capture	
		Passed	Failed
InterceptKeys.exe	Local Network	✓	
	Online Network		✓

Table 2 shows the result on test in remote desktop.
As presented, the program was able to block remote access on local network because it disables the remote connection on desktop.

Efficiency

The following simulation shows the efficiency on practical use of the program made by the proponent.

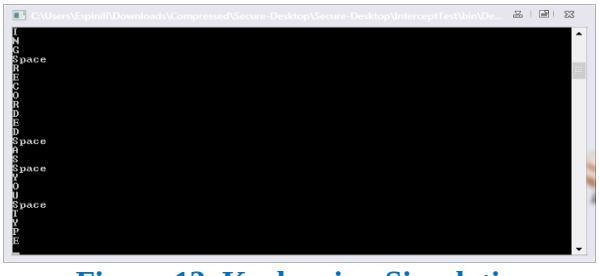

Figure 13. Keylogging Simulation

Figure 13 is a keylogger made by tester for the proponent to test the program. This keylogger captures every key pressed on the keyboard by the user. Every captured keystroke is saved on its own log file.

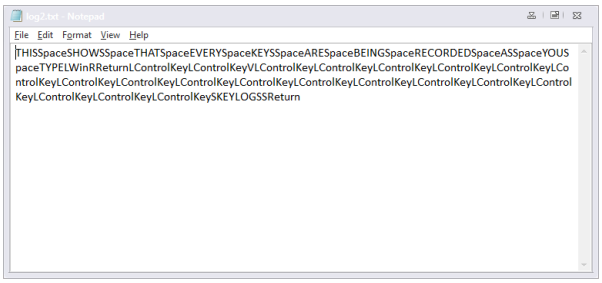

Figure 14. Recorded Keystrokes

Figure 14 show the keystrokes captured and recorded on the key loggers' log file. The recorded keystrokes on the log file are sent to the hackers. This shows the case when the computer is vulnerable to spywares. Information encoded on the device is recorded and viewed by the hacker.

Figure 15. Encrypted Keystrokes

Figure 15 shows the encrypted keystrokes of the user on the keyboard. This simulation illustrates the protected keystrokes of the user in encrypted text form and the equivalents of the plain text data of the keystrokes.

Conclusions

The researcher therefore concludes that the proposed system "Keylogging Security Using Asymmetric-Key Encryption for Non-Hybrid Keyloggers" is made to make the users input their information without any worry of being a victim of information theft. The InterceptKeys.exe is the program that uses the encryption process on keystrokes. By utilizing the system in actual situation, the proponent come up with the following conclusion:

The proposed system "Anti-Keylogging Sofware Using Asymmetric-Key Encryption" blocks almost logs and activites via keystrokes. This proposed system helps computer users in protecting their sensitive information or transaction online. Asymmetric-Key encryption is used in the proposed system. It is the best algorithm for the system since it is created for the purpose of securing data or message.

Recommendations

The following recommendations are presented to maximize the efficiency of the system. The limitation is encountered in making this study. The proponent is open that there will be further set of changes necessary for the improvement of the device.

The proponent recommends the system entitled “Keylogging Security Using Asymmetric-Key Encryption” in protecting information input in online and computer applications.

For the researchers who want to enhance this project study, it is suggested to make a program that can block all hybrid keyloggers.

References

1. "Keylogger". Oxford dictionaries.

2. Top 5 best keylogger for iOS. Available at: http://pf8fgwezdyf0uxdj.tk/INQPG11/top-5-best-keylogger-for-ios Accessed (February 2017)

3. Papagalos, Lauren, What Is Malware and How Can It Infect My Website? June 6, 2016. Available at: https://blog.sitelock.com/2016/06/what-is-malware/. Accessed (March 2017)

4. Keyloggers are Safe? Àugust 17, 2012. Available at: http://swissen.org/2012/08/17/keylogger-are-safe/. Accessed (February 2017)

5. Cyber Crime Combating Using KeyLog Detector tool. Available at: http://www.academia.edu/27876776/Cyber_Crime_Combating_Using_KeyLog_Detector_tool. Accessed (December 2016)

6. What is a Keylogger?. July 23, 2013. Available at: https://securingtomorrow.mcafee.com/consumer/family-safety/what-is-a-keylogger/. Accessed (December 2016)

7. Martin, James, 1991. Rapid Application Development. Macmillan. pp. 81–90. ISBN 0-02-376775-8