IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SURVEY ON KEYSTROKE LOGGING ATTACKS

Kavya .C [1], Suganya.R [2]

[1] Student, II MSc. Computer Science, Sri Krishna Arts and Science College, Coimbatore
[2] Assistant professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore

Abstract:

A Keylogger generally referred as a keystroke or system monitor. Keystroke could be a reasonably police work technology accustomed monitor and record every keystroke written on a particular data input device. Keylogging usually used as a spyware tool by cybercriminals to steal in person recognizable info, login credentials and sensitive enterprise knowledge. Keystroke is employed to visualize employer's performance to watch their laptop activities, oldsters to supervise their children's net usage, device homeowners to trace attainable unauthorized activity on their devices or enforcement agencies to analyse incidents involving laptop. The method can be thought-about moral or acceptable in variable degrees.. Some numerous keylogging techniques, extending from hardware and software based methodologies. Keyloggers are easy to detect, but once it infects our computer, it can cause unauthorized transactions. Data-stealing malware attacks are prevalent today. This paper presents an overview of different types of password attacks and analysing prevention and detection techniques of keylogger attacks and some preventive measures to reduce the malware attacks and detection of personal data.

Keywords: keylogger; keyboard; cryptography; cipher text; encryption; decryption; types of password attacks; prevention & detection of keylogger;

I. Introduction

Malware is the process of disturbing system like collect sensitive data and gain access to systems [1]. Ancient authentication systems wont to defend access to on-line services (such as passwords) square measure prone to attack by the introduction of a keystroke faller to the service user's pc [2]. Detecting and preventing malware attack is very important in cyber world as malwares can badly affect computer operation. Once an hacker got access to private user data, he/she can easily make money transfer from user account to untrusted account. The private data can have many consequences which can prove to be more hazards than particular individual's financial loss. We can summarize malware as program intentionally developed for damaging computer specifically those have internet connection [3]. Keyloggers square measure a significant threat to users and therefore the user's information, as they track the keystrokes to intercept passwords and different sensitive data typewritten in through the keyboard. this provides hackers the good thing about access the PIN codes and account numbers, passwords to on-line searching sites, email id's, email logins and different hint etc. when the hackers get access to the user's private and sensitive information, they can take advantage of the extracted data to perform online money transaction the user's account. Keyloggers will typically be used as a spying tool to compromise business and state-owned company's information. the most objective of keyloggers is to interfere within the chain of events that happen once a secret is ironed and once the information is displayed on the monitor as a results of a keystroke.

Fig shows the Image of keylogger

A keylogger can be done by introducing a wiring or a hardware bug in the keyboard, to achieve video surveillance, terminating input/output, or by also implementing the use if a filter driver in the keyboard stack. Extracting information from the user's keyboard exploitation generalized documented ways. The log file created by the keylogger may be sent to the required receiver. Some keyloggers programs will record any email addresses that you just have used and URL's of any websites that you just visit. There square measure 2 different rootkit ways employed by hackers:

masking in kernel mode and masking in user mode. during this paper we tend to specialise in the literature survey that is said to keylogger, its types, interference detection of keylogger attacks and its varied applications.

Cybersecurity & Cryptography:

Cyber security is that the follow of protective systems, networks, and programs from digital attacks [5]. These cyberattacks square measure typically aimed toward accessing, changing, or destroying sensitive information; extorting cash from users; or interrupting traditional business processes. Implementing effective cyber security measures is especially difficult these days as a result of their square measure a lot of devices than folks, and attackers are getting a lot of innovative. Cryptography is that the technique for secure communication within the presence of third parties is termed as adversaries. It deals with developing and analysing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Secure communication refers to the situation wherever the message or information shared between two parties can't be accessed by associate degree opponent. In Cryptography, associate degree opponent may be a malicious entity that aims to retrieve precious data or information thereby undermining the principles of data security. Data Confidentiality, information Integrity, Authentication and Non-repudiation square measure core principles of contemporary cryptography.

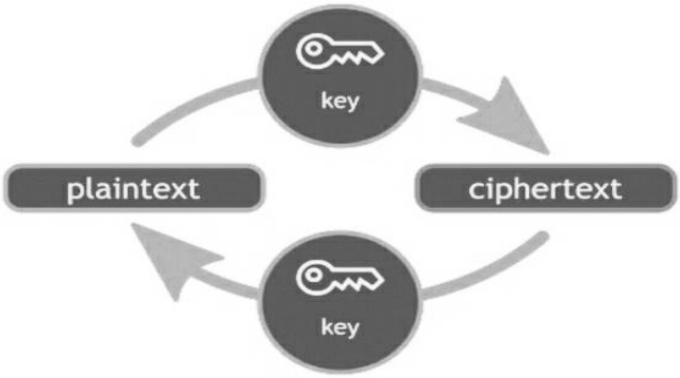

Fig shows conversion of plain text & cipher text

Consider two parties Alice and Bob. Now, Alice needs to send a message m to Bob over a secure channel. So, what happens is as follows.

The sender's message or typically known as the Plaintext, is born-again into associate degree unclear type employing a Key k. The resultant text obtained is termed the Cipher text. This method is understood as coding. At the time of receive, the Cipher text is born-again into the plaintext exploitation constant Key k, in order that it may be browse by the receiver. This method is understood as cryptography.

Alice (Sender) Bob (Receiver)

C = E (m, k) ----> m = D (C, k) (1)

Here, C refers to the Cipher text whereas E and D square measure the coding and cryptography algorithms severally [6].

II. Literature Review:

Extensive work was performed dealing with the authentication protocols. The proper information is collected by reading and analysing papers and books. For example an article about comparison, detection techniques of keyloggers was written by

final year student "KEYLOGGERS Comparison of Detection Techniques & Its Legitimate Use" the author Aaradhya Gorecha discussed that keyloggers to check the employee's web activity and also for domestic purpose parents can keep a check on their children web activities this can be helpful at company level and personal purpose for parents. Another research paper "Keylogging: A Malicious Attack" authors Sonal Shinde, Ujwala H. Wanaskar discussed that some techniques to reduce malicious attack of keyloggers. In this two research paper have some drawbacks 1) the techniques that are discussed will be useful but the user have to note each every process of the particular technique otherwise the user will forgot that what he/she done. 2) Another drawback that installation of the software, in that the user information will be stolen by some other person. It can be reduced by admin by making the user information more secure. Some other research papers will also be discussed in this paper.

Detection techniques and future scope

No	Paper name and author	Keylogger Detection Technique	Results	Future scope
1	Aslam at el. (2004) AntiHook Shield against the Software Key Loggers.	This paper describes the anti-hook technique to scan all the processes and static executable and DLLs of the system.	Since hook technique is the core of the detection of keylogger. So it can easily find all the suspicious files and processes which are present on any level [7].	This technique requires much more calculation to be doe and also the false positive rate is very high.
2	Parth Mananbhai Patel, Prof. Vivek K.ShahParth (2015) Analysis and Implementation of Decipherments of KeyLogger.	This paper describes designing a detection technique for user-space key loggers. The technique to prevent user-space key loggers from stealing confidential data originally intended for a (trusted) legitimate foreground application.	This approach is that it centred on a black-box model that completely ignores the key logger internals. Also, I/O monitoring is a non-intrusive procedure and can be performed on multiple processes simultaneously [8].	This technique has the ability to artificially inject carefully crafted keystroke patterns, and discussed the problem of choosing the best input pattern to improve our detection rate with no false positives and no false negatives reported.
3	Stefano Ortolani, Cristiano Giuffrida, Bruno Crispo (2010) Bait Your Hook: A Novel Detection Technique for Keyloggers.	This paper describes a technique to find and prevent the malicious attacks of keyloggers.	In this technique keylogger eavesdrops each keystroke issued by the user and logs the content on a file on the disk [9].	As a result of this technique, the malicious activities can be known in advance and controlled.

Another research paper "Keyloggers in Cyber security Education" authors Christopher A. wood and Rajendra K. Raj discussed that keylogging attacks and usage, overview of keylogger programs and a study of keylogging in cyber security to educate the next generation. This paper has an advantage that students can learn about the keylogging programs and keylogger attacks it may help them to avoid the detection of information without their knowledge and to secure their information from keylogger attacks [10].

III. Different types of password attacks:

Keylogger has much type of techniques to hack their victims and crack that victim's password using these techniques. The sections will give a review about some different types of password attacks. For authentication of any system password is first and foremost step so, passwords play an important role in daily life in various computing applications like ATM machines, internet services, windows login, authentication in mobiles etc. Intruders/hackers can make system vulnerable, can get access of it and can also get valuable information of ours. In this section we enlisted some of possible password attacks

A. Dictionary Attack:

The dictionary attack is used by hackers to hack user's password easily. This will check the user's password word by word like dictionary and it also find the users psychology of creation of their password. Attackers get loads dictionary files of passwords and words to run against the user. This attack is similar to brute force attack.

B. Brute force attack:

The brute force attack uses the program to crack the user's password. Multiple attempts with possible combinations of words were used to crack the account. The attacks start with commonly used, weak passwords like Password123 are considered as week passwords [9]. The programs running on attacks usually try variations on upper and lowercase characters, as well [8].

C. Phishing attack:

The most-commonly used technique in today's modern world. This technique will involves using emails, text messages sent to fool the users into providing their credentials by clicking the link or image that will install the software or it will re-direct to fake website or account that was create by the hackers.

D. Rainbow table attack:

The rainbow table attack is type of hacking that uses rainbow hash table to crack password. This uses hash table in cryptographic function to store password in database. When hackers are a pre-computed table of hash values that are pre-matched to possible plain text passwords. This allows hackers to reverse the hashing function to crack the password.

E. Shoulder surfing:

Shoulder surfing is act of obtaining the personal and private Information behind the users shoulder without their knowledge. It occurs when someone watches over users shoulder to nab the ATM pin and passwords as the user key on to electronic device. By using this technique for financial gain, the activity is considered as identify theft.

F. Credential stuffing:

This attack says that danger of using same passwords for several accounts and this will lead to hacker to steal the password easily. In this attack, hacker sets the bot that automatically log into multiple accounts in parallel using fake IP address. If the password is stolen by running on multiple websites the informative resources were stolen and hacker can store the stolen password and they can send to their circle this will lead to increase malicious activity and breach over the networks.

G. Password spraying:

Password spraying, an attack that would attempts to access the large number of accounts and databases with commonly used passwords [7].

H. Spidering:

In this attack the hackers consider that corporate passwords are related to business. The hackers look or do ground work to get information about particular corporate. By using this information they can steal that password and store them for their future usage.

I. Keylogger:

Keylogger is type of capturing or monitoring the system by installing software to record all the keystrokes. By using this software they can pass information to hackers or intruders.

IV. How keylogger & keyboard work:

Keylogger is a program that was used to secretly monitor and log all the keystrokes in a computer system. This program can be installed in a computer system or by sending the .jpg file or email to the user's system. If the user clicks this type of images or emails their system gets hacked. For example, if the keylogger sending the random image related prize, if the user clicks the image or typing their personal details they got hacked. This Section covers an overview that how the keylogger & keyboard works. Keylogger attack does that when unknown app or APK runs background of our system, when we type something in our system or if we visit any websites or if we type the bank account details that will be sent to the hacker. By using this master key the hacker can access all the information that they need. Keylogging can be two types they are hardware based keylogging and software based keylogging [10]. A hardware based keylogger, small device that serves as a connector between the computer and the keyboard. In this type, a piece of hardware that was inserted somewhere between computer and along keyboard's cables. A software keylogger is like remote access it allows to access locally recorded data from the remote location. There are some methods to be followed and used for communication: uploading the data to a website, database or FTP server, periodically emailing data to a predefined email address, wirelessly transmitting data through an attached hardware system, software enabling remote login to your local machine [11]. Some software keyloggers capture information when any of the keyboard key pressed as input. The sentence or word or anything when copied to clipboard it will be captured. Randomly timed screenshots of computer the screen of computer will be logged. The windows API allows programs to request text value of some control like password that typed for any forms it will be

captured. Keyboard plays an important role in keylogger. Keyboard is the main target for keyloggers. Keyboard has sequence of key matrix and it also called as circuit matrix. When the particular key is pressed, the keyboard controller notes that which key is pressed and ROM record the events.

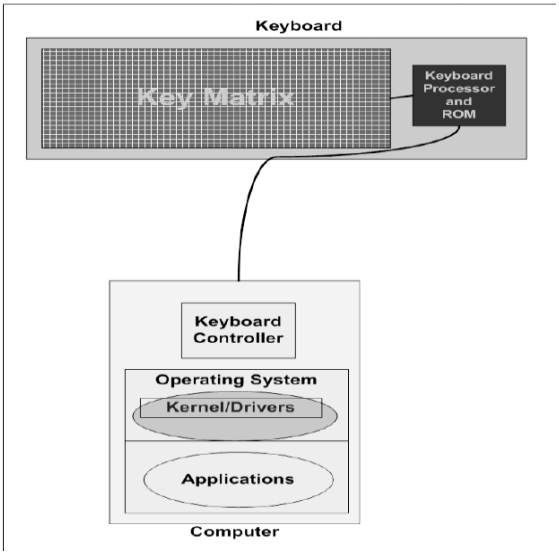

Fig shows the working of keyboard

It sends the event to operating system and it also sends the code to keyboard buffer. The data travelled between the operating system and computer keyboard is interrupted by keylogger. Whenever the key is pressed by user, every time the keylogger will be noticed. By recording the each and every key that was pressed by the user. The keylogger can hack the particular users system and so that hacker can get database and bank details of that particular user. Hacker can send stolen passwords or database to other intruder.

V. Prevention and Detection techniques of keylogger:

In today's world, everything around us is choked with digital method like internet banking, mobile recharging, searching and payments for electricity, studies, etc. These methods keep folks data regarding their general process and created easier the approach of payment. This method created advantage conjointly for hackers also as keyloggers. By exploitation this method, hackers or keyloggers will steal the knowledge and arcanum from the actual user. This cause loss of information and also the activity is taken into account as thieving. This section covers some preventive and detective measures of keylogger. Keylogger is prevented by staying aloof from untrusted apps and websites on the web. A number of interference measures are followed:

• Always use anti-virus for system, some unwanted apps are put in while not the users data. It's higher to use the antivirus for system it'll avoid the installation of unnecessary apps and virus attacks.

• fitting the firewalls security for the system to avoid the attacks from faux websites.

• Setting a selected lock arcanum or pin for the system it'll forestall the unauthorized access each on-line & offline from intruder/hackers.

• Avoid sharing of emails, confidential messages, or info publically or shared pcs.

• Always maintain the sturdy arcanum like dynamical the arcanum once at per week or month and avoid exploitation the common passwords or combination of words for many accounts.

• Always keep change the system and apps that have already put in within the system. This can management the unnecessary attacks from hackers.

Detection of keylogger is tough we will cut back and management the attacks of keylogger. In cryptography, encoding and coding methodology accustomed observe the keylogger in order that user will send the e-mail or messages firmly. During this paper, cryptography methodologies are accustomed management and observe the keylogger. Encoding is employed to convert the plain text to cipher text. Coding is employed to convert the cipher text to plain text. We will send a message or info to the person exploitation encoding and coding. By exploitation this methodology we will avoid and cut back keylogging connected attacks in order that we will forestall our files or hint from hackers. Whereas exploitation the encoding and coding methodology it's suggested to use the virtual keyboard. Usage of virtual keyboard can cut back and avoid the foremost attacks of keylogger. Virtual onscreen keyboards cut back the possibility of being keylogged as they input info during a completely different thanks to physical keyboards. This would possibly impact user productivity, isn't fool proof against all types of keystroke observance software system, and doesn't eliminate the explanation for the matter. Observant resource allocation and background method on machines, also as knowledge being transmitted from the device outside the organization will facilitate determine if a keylogger is gift. Keyloggers sometimes want root access to the machine, which may even be a tell-tale sign of a keylogger infection [4].

VI. Conclusion & Future Scope:

In this paper, the article attempts to insight the keylogger workings, different types of password attacks and prevention & detection measures to reduce and avoid the keylogging attacks. This paper had discussed a cryptography encryption decryption method to reduce the keylogging attacks. To reduce the keylogging attacks user has to keep their software up-to-date and it is advisable to maintain the strong password policy for their systems. It is advisable to disable the self-running files that are externally connected devices like USBs and restrict to copy the files to and from external computers by doing this attacks may get reduce. In literature review, this paper discussed the various measures and methods to reduce keylogging attacks and it also used for parents to monitoring the children's activity. The main point is aware of the keylogging attacks by how they are entering in to system and use suitable ways to detect them. However in future, the paper would enhance the idea which is based on the cryptography algorithm to reduce the keylogging attacks and detection. Therefore the result of the paper has achieved the main area of the paper by discussing the preventive measures to reduce the keylogging attacks from the keyloggers.

VII. References:

1. Malware Definition Available at http://en.wikipedia.org/wiki/Malware.
2. S. P. Goring, J. R. Rabaiotti and A. J. Jones, "Anti-keylogging measures for secure internet login: an example of the law of unintended consequences", Computers & Security, Page 1-9, Feb 2007.
3. Malware Definition Available at https://www.wisegeek.com/what-is-malwa.
4. https://www.csoonline.com/article/3326304/what-is-a- keylogger-how-attackers-can-monitor-everything-you-type.html/
5. https://www.ntiva.com/cyber-security-services/
6. geeksforgeeks.org/cryptography-introduction/
7. https://sec.okta.com/articles/2020/12/password-spraying-attacks-and-how-prevent-them
8. https://info-savvy.com/password-attacks/
9. https://www.linkedin.com/pulse/common-security-attacks-cyber-mobile-atms-wifi-iot-niteen-lall
10. https://searchsecurity.techtarget.com/definition/keylogger
11. https://www.veracode.com/security/keylogger
12. AntiHook Shield against the Software Keyloggers. Aslam at el. (2004)
13. Analysis and Implementation of Decipherments of Keylogger, Parth Mananbhai Patel, Prof. Vivek K.ShahParth (2015).
14. Bait Your Hook: A Novel Detection Technique for Keyloggers,Stefano Ortolani, Cristiano Giuffrida, Bruno Crispo (2010).
15. Survey of Keylogger Technologies, Yahye Abukar Ahmed, Mohd Aizaini Maarof, Fuad Mire Hassan and Mohamed Muse Abshir, International Journal of Computer Science and Telecommunications, Volume 5, Issue 2, February 2014.
16. Cyber Security – KEYLOGGERS Comparison of Detection Techniques & Its Legitimate Use Aaradhya Gorecha Information Technology Department SVKM NMIMS MPSTME, Shirpur, Maharashtra, India.