ISSN 2320-9984

Volume 6 Issue 1| March 2018

ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A Review on Key Logger Malware Detection Concerning Password Opacity

Somya Shrivastava
M.Tech. Research Scholar
Oriental Institute of Science & Technology
Bhopal, (M.P.) [INDIA]
Email: somyashrivastava@gmail.com

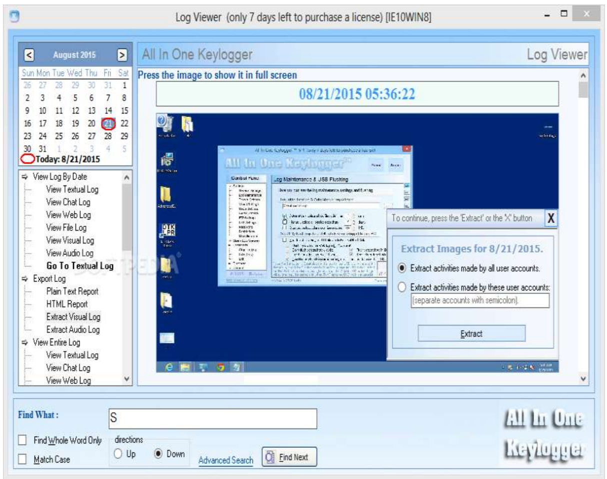
Bhupendra Panchal
Assistant Professor
Department of Computer Science & Engineering
Oriental Institute of Science & Technology
Bhopal (M.P.) [INDIA]
Email: bhupendrapanchal30@gmail.com

Abstract—*To access any crucial application related to online banking, emails etc, users need to get registered and generate unique login ID and password to access their account. Those credentials are required to handle securely. But nowadays there are various malicious spyware in the form of key loggers are available. Key logger recorder is a malicious spyware that can record key enrollments and mouse pointers that can transparent the password even if it is concealed. Key logger can expose all enrolled keys and makes password visible to illegitimate user who can access users account. Spywares operates in stealthy way and monitors every keystroke on a computer. Key logger can expose what was typed, when it was typed, in what program it was typed, and on what website it was typed. Certain researches have been done in the field of spyware detection that only detect key logger by considering it as malicious program. Paper revealed certain researches that confront secured system for password concealment or detecting key loggers. The proposed system is able to encrypt password at the time of key enrollments. When an illegitimate user trying to record key strokes using key loggers then bots enroll some random keys while enrolling password. Password will be encrypted among various strings that cannot be apprehensible. Proposed system is able to differentiate physical as well as bots keystrokes. Here it is a situation where password cannot be visible in actual form and it is impossible to find correct credentials.*

Keywords:— *Key logger, Authentication System, Malicious Program, Password Transparency, Input Credentials, Security.*

1. INTRODUCTION

Due to the constant rise of malicious software like key loggers spyware, risk of securing input credentials used for the process of authentication enhances. These kinds of malicious program cautiously monitor the overall activity of system including mouse pointer and keystrokes. Virtual keyboard has also been employed on some online services for authentication process to prevent its system from attacking but it did not work. As key logger monitors the mouse pointer too and records the activity done in a system. This malicious program creates a log file which is actually the data captured by key logger. Software mailed that log file directly to the hacker or designer who creates the software. Hacker can easily decrypt the log file and acquired the credentials used by the user during authentication process. There are numbers of software available which can easily enter in the system using any application. These malicious programs are so hazardous that they can easily filch the vital information and credentials of a user. Many times, it has been examined that key loggers are installed in mobile phones in the form of genuine application and intercept all the communication and accessing details. Generally users are not aware of these kinds of attack as they use to operate in hidden form. There are various prevention techniques like Honey ID, Spyware detection, Anti-Hook techniques, and so on. Most of the technique is employed to detect the presence of key logger program in the system which is certainly not possible every time. Variety of malicious key logger spyware is present in the environment and their severity varies which even breaches the security of antivirus. So, to detect every malicious program of key logger is practically not possible. Depends on the available technique, two kinds of key logger exists; Hardware Based Key Logger and Software Based Key Logger. Various techniques has been developed in order to detect the existence of key logger in the system or to prevent the system from key logger but somehow, they failed to ideally prevent the system from the attacks of key logger. A brief review of systems which has been proposed by various researchers previously in their paper is further concluded in the section of literature survey.


Log Viewer (only 7 days left to purchase a license) [IE10WIN8]

Press the image to show it in full screen

08/21/2015 05:36:22

To continue, press the 'Extract' or the 'X' button

Extract Images for 8/21/2015.

● Extract activities made by all user accounts.

○ Extract activities made by these user accounts:

(separate accounts with semicolon).

Find What : S

□ Find Whole Word Only

□ Match Case

directions ○ Up ● Down

Figure 1. Key logger Software [9]

2. LITERATURE SURVEY

2.1 Reviews on Existing Systems –

Mohammad Wazid, Robin Sharma et al. [1] developed a framework in order to provide detection and prevention system against key logger attacks. The technique used in this paper initially designed a scenario based on attacks through key logger spyware. As shown below in Figure 2, a scenario was taken in which three different users used various internet services like emails, internet banking etc. Key logger spyware entered in the form of application software into the computer system, where the user is not aware. After getting successfully installed, that spyware will capture keystrokes easily and create log files in reference of those keystrokes. Captured keystrokes can be those credentials which user used to access their internet banking account, emails and so on. Key logger spyware entered in the user's system and the created log file is transfer through emails to the designer shown by red arrow in the below mentioned figure.

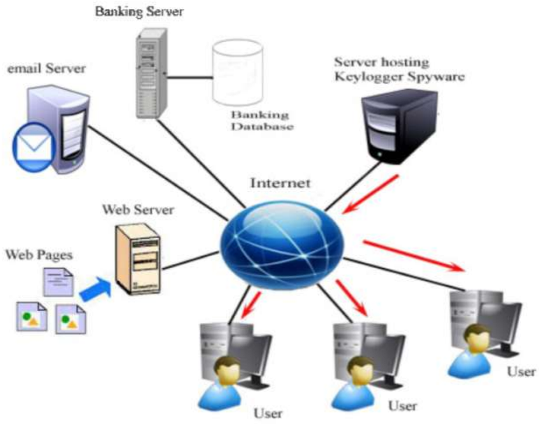
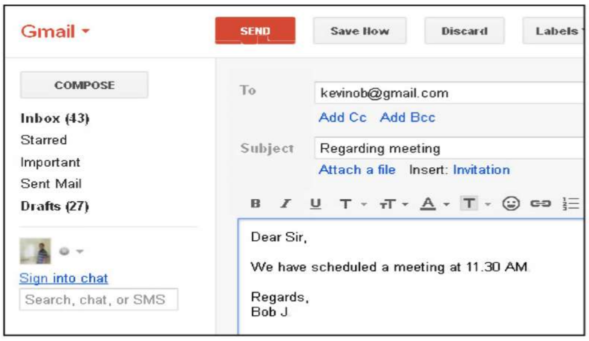


Figure 2. Key Logger Spyware Attack on Users [1]

In figure 3 shows the snapshot of the email which has been sent in the presence of key logger and in figure 4 shows the created log files in reference to the captured keystroke and mentioned every keywords used in the mail.


To kevinob@gmail.com

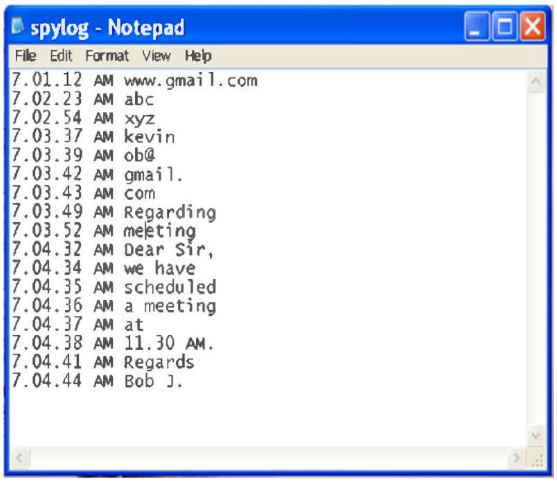
Subject Regarding meeting

Dear Sir,

We have scheduled a meeting at 11.30 AM

Regards,
Bob J

Figure 3. Email sent in Presence of Key Logger [1]



```
7.01.12 AM www.gmail.com
7.02.23 AM abc
7.02.54 AM xyz
7.03.37 AM kevin
7.03.39 AM ob@
7.03.42 AM gmail.
7.03.43 AM com
7.03.49 AM Regarding
7.03.52 AM meeting
7.04.32 AM Dear Sir,
7.04.34 AM we have
7.04.35 AM scheduled
7.04.36 AM a meeting
7.04.37 AM at
7.04.38 AM 11.30 AM.
7.04.41 AM Regards
7.04.44 AM Bob J.
```

Figure 4. Generated Log File BY Key Logger [1]

To observe those attacks, the technique which has been proposed in the paper employed honey pot system into the network of user. It enabled the entrance of key logger spyware into honey pot system to observe the activity of spyware and generates the log file which is forwarded to the server for the prevention of the system. In figure 5, observation through honey pot in the system is demonstrated. Since, the system developed an algorithm by using honey pot to detect the presence of key logger, but it is known that there are numbers of malicious program of key logger is available and to detect every program though the algorithm which has been proposed in the paper is not possible. A system is needed to save the input credentials even in the presence of key logger.

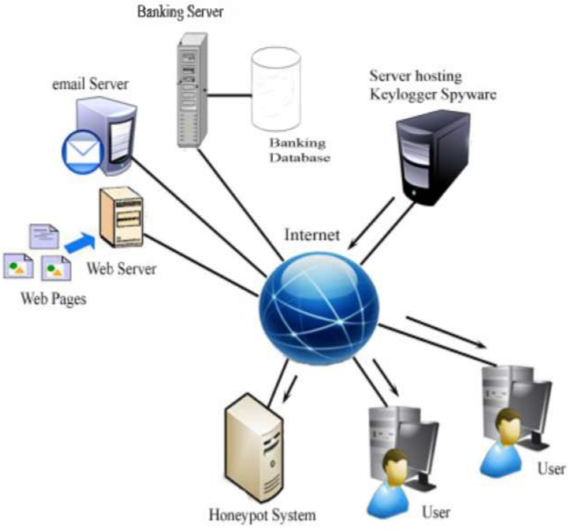


Figure 5. Honey pot Based Monitoring [1]

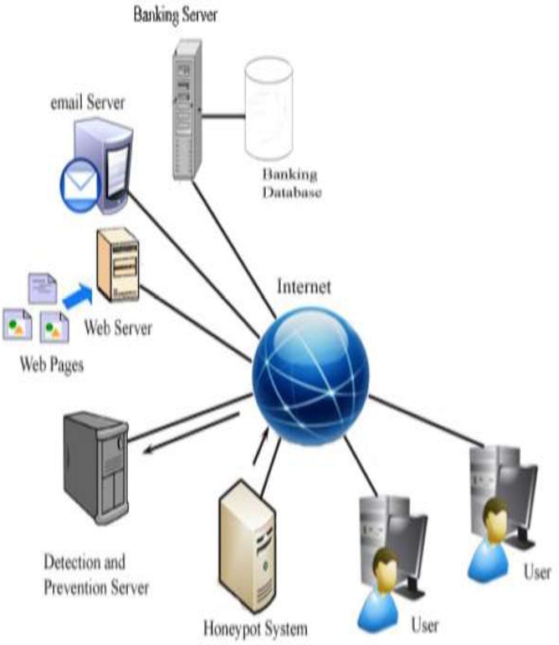


Figure 6. Transfer of Generated Log File from Honey pot to Detection Prevention Server [1]

S.Gunalakshmii et al. [2] proposed a system to detect the presence of key logger spyware program into the system and aimed to prevent the system from data leakage. The technique which has been proposed in the paper tried to recognize all the permissions and space of storage required by every application in the system. Then segregate those applications with sufficient permission from those key logger programs which can violate the permissions. Black- box technique is exploited in the system which has been proposed in the paper to identify the existence of key logger. Since, this approach is relied on the behavioral characteristic not on the structural characteristics of the key logger. This system developed a mobile based application which exploited the algorithm relied on machine learning to recognize the key logger based applications. To recognize the key logger applications present on mobiles, Support Vector Machine (SVM) algorithm is used. The overall functionality of the system relied on three different sections i.e. to collect required permissions for mobile application, analyze those permissions and identify the existence of key logger application. The architecture of system which has been proposed in this paper is shown below:

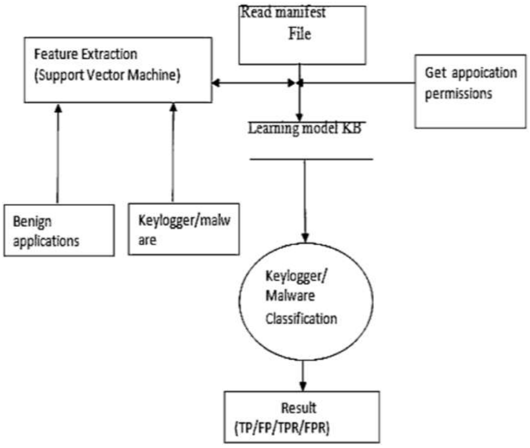

Read manifest File
Feature Extraction (Support Vector Machine)
Get appoication permissions
Learning model KB
Benign applications
Keylogger/malw are
Keylogger/ Malware Classification
Result (TP/FP/TPR/FPR)

Figure 7. System Architecture [2]

To gather the information regarding permission of application is achieved by Package Manager API which is a type of class to recover that information related to the application package. These packages are accessed under C programming library. To analyze the acquired information of permission of various applications, SVM machine learning approach is used. Using this learning approach, detection of key logger application is also achieved. Due to big set of data and high computational control is required to analyze an application; exploitation of SVM reduces the overall performance of system.

M Hossein Ahmadzadegan et al. [3] introduced a technique which can prevent the unwanted access of applications through key logger spyware. System utilized the function of logistic Map Chaos to create one time password for the authentication of user. Those generated password is for one time use only. An android application is being exploited to create the one time password. To establish a password, user needs to determine the parameters in the canal by using Logistic Map Chaos Function. That canal should be secure enough where no any key logger can capture the keystrokes; it can be a computer or any network. Those parameters included username, Xparameter, Xstart and Range as shown in below mentioned figure. System required a matchless username and other parameters and user also required to remember those credentials every time when one time password is needed.

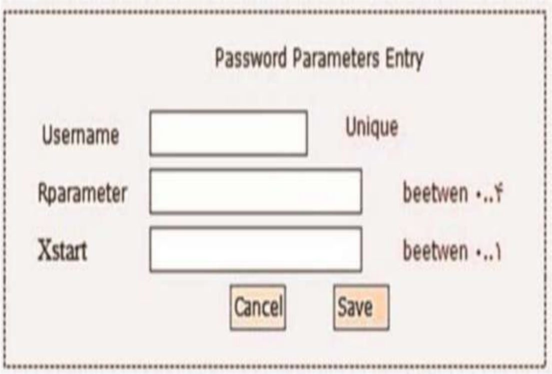


Figure 8. Determining Parameters of Password in a Secure Canal [3]

User required installing that application to generate password by using those parameters. That password is for one time use only to access any application either in the computer or mobile. The figure which is mentioned below shows the application which has been developed in the system.

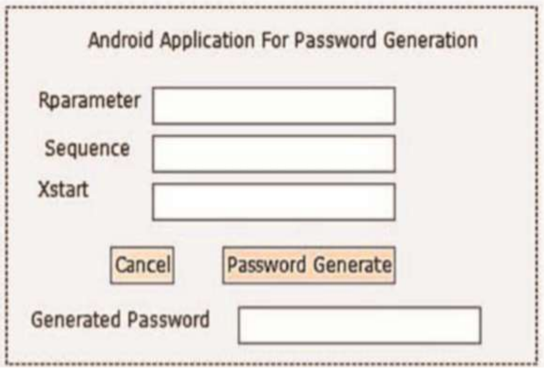


Figure 9. Android Application for Password Generation [3]

Since, the application which has been designed to generate one time password required a secure canal to execute which in itself not possible because there is no prevention technique has been developed to secure mobile systems from key logger. If mobile is already affected by key logger whose file is generally very small and hidden, then the parameters generated in the application will be captured by the key logger and the created log file is mailed to the designer, which can intellectually crack the credentials.

Junsung Cho et al. [4]discussed various prevention mechanisms against key logger attacks. It has been stated that, using third party keyboard applications on mobile contains malicious key loggers whichcan capture the keystrokes. It has been demonstrated in the system that among 100 websites which have been tested, 81 are affected with spyware program of key logger. Around 139 various keyboard applications available in Google Play examined in the paper which has been proposed, among which 84 applications are not secure as key logger might alter the functionality of the system. Customized keyboard offered by third party was taken into consideration to examine the safety issue. It has been observed that, permission taken from internet only could install the malicious spyware programs of key logger. Since, the study which has been concluded in the paper was unsuccessful to find out the real key loggers, which are potentially accessible on android platform. It has been examined that, mere permission of internet to any third party keyboard application might easily converts into malicious key logger spyware. It is required to develop a technique which can effectively prevent the system from any unusual attacks of key logger spyware programs.

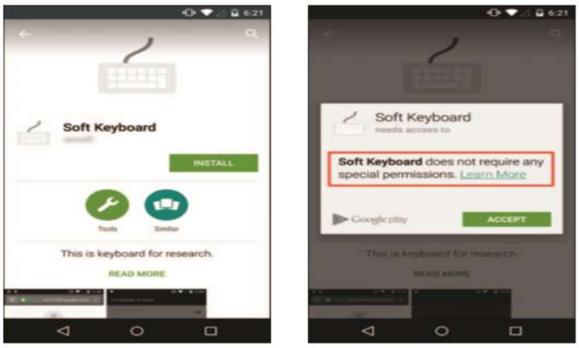
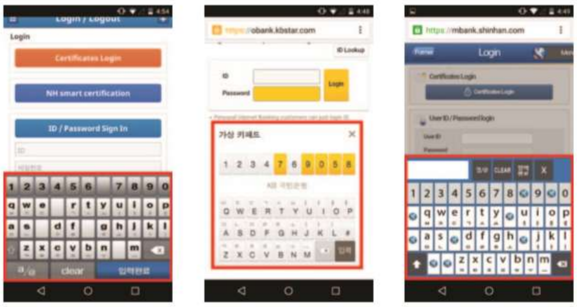

Soft Keyboard
INSTALL
Tools
Similar
This is keyboard for research.
READ MORE
Soft Keyboard
needs access to
Soft Keyboard does not require any special permissions. Learn More
Google play
ACCEPT

Figure 10. App Information and Installation Warning in Google Play [4]



(a) Nonghyup Bank (b) KBstar Bank (c) Shinhan Bank

Figure 11. Trustworthy Keyboards in Bank Websites [4]

Neenu N A [5] developed a visual authentication protocol which is based on password. The system which has been proposed exploited a protocol which deploys a blank keyboard consists several special signs linked with every character. By employing this keyboard, user can fill their credentials to access any application. The technique which has been developed in the system enhanced the short term memory generally required in an attack. As shown in figure 12, in blank screen keyboard, every character is linked with special character. The method which has been proposed, consider numeric keyboard in horizontal form having blank spaces and consist of an array of ten various signs. To enter a password of 4 digits took four different rounds to get completed. System which has been developed required a user to identify the position of the number in the keyboard which is hidden behind the symbols. Session key decision and pin entry are the two rounds required to input a pin. Method which has been proposed is too complicated and when it is implemented for alphanumeric characters, it becomes very difficult for the users to use it. So the method developed in this paper is not user friendly technique to hide their credential from key logger.

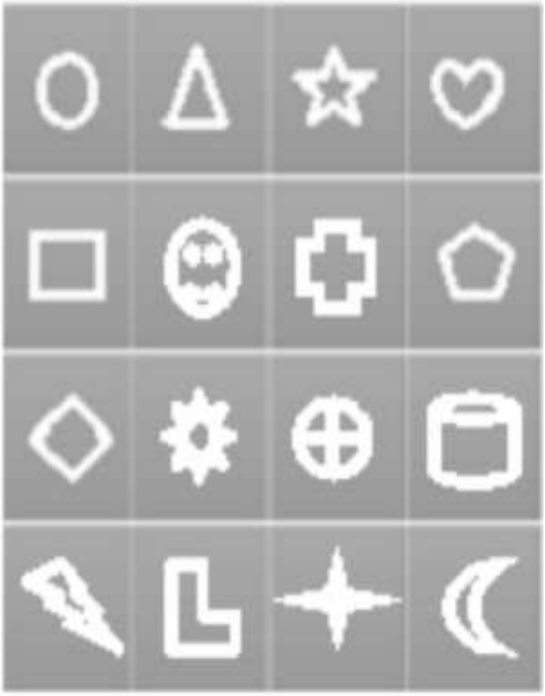


Figure 12. Blank Keyboard with Special Symbols [5]

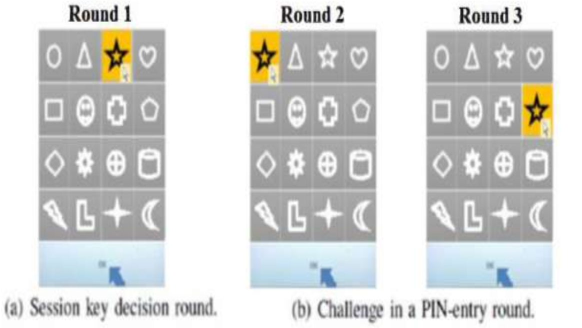

Round 1
Round 2
Round 3
(a) Session key decision round.
(b) Challenge in a PIN-entry round.

Figure 13. Example of Session Key Decision Procedure and PIN-Entry Procedure [5]

Tasabeeh O. M. Ali et al. [6] developed a prevention technique against spyware attacks. To confuse the key logger, system exploited multiple layers of keyboard. The layout of keyboard gets changed at every key press by randomly available predesigned layouts which mislead the key logger. Since the keyboard layout for key logger spyware is inconstant. The interception of keystrokes through key logger took different ways which are; the driver used by inbuilt keyboard is replaced by the malicious one, filter can be deployed between keyboard driver and message queue of system, callback function can be involved through key logger. The tool which has been exploited in the system is Microsoft Keyboard Layout Creator (MSKLC) responsible to design various layouts of keyboard in those languages which Microsoft doesn't support. Utilization of MSKLC limits the accessibility of the system as it is incapable to map more than two keystrokes to a solitary Unicode and having deficient alternatives to provide relevant input

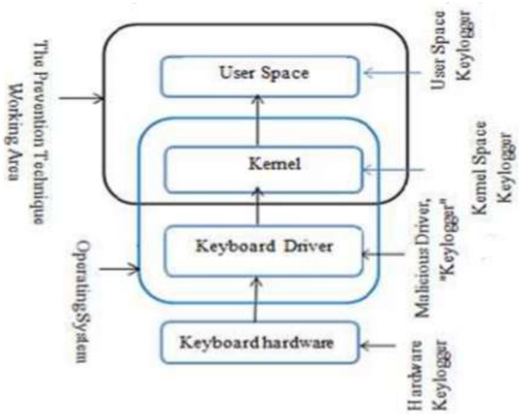


Figure. 14 Random Multiple Layouts Prevention Technique Working Area [6]

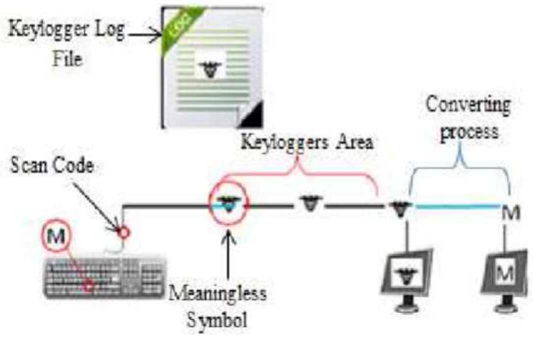


Figure 15. Random Multiple Layouts Technique Model [6]

A. Solairaj et al. [7]proposed a paper which concluded the techniques available to detect Key logger Software. Since, the spyware program of key logger is used to intercept the keystrokes to unofficially access the vital applications of the system. Relied on the behavioral characteristics, key logger software can be detected. Key loggers have an ability to operate in stealth mode and capture the keystroke used by the user. Due to this, identification of key logger's existence in the system is quite difficult. Many techniques have been developed to detect key logger software in the system such as; Honey ID: Spyware detection, Bot detection, Anti-Hook techniques, Safe access to password protected accounts and dendritic cell algorithm. Anti-Hook technique relied on the concept of using hooks for every hidden or displayed process. Through the technique offered by hooking, behavioral feature of operating system or any application can be observed and it helps to detect the existence of any spyware program of key logger.

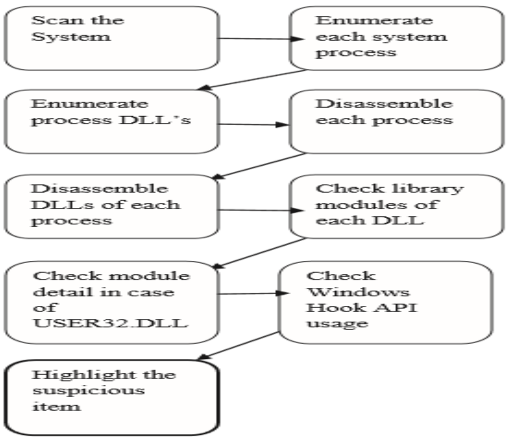

Scan the System
Enumerate each system process
Enumerate process DLL's
Disassemble each process
Disassemble DLLs of each process
Check library modules of each DLL
Check module detail in case of USER32.DLL
Check Windows Hook API usage
Highlight the suspicious item

Figure 16. Anti-Hook Approach [7]

Honey ID is a technique used to detect malicious spyware of key loggers. The method induced in Honey ID decoys the attacker. To prompt the attacks of spyware, various fake events generate by the technique due to which stealth process of spyware is identified. The study which has been projected in this paper spotted various available techniques used to detect key logger and its effect on system.

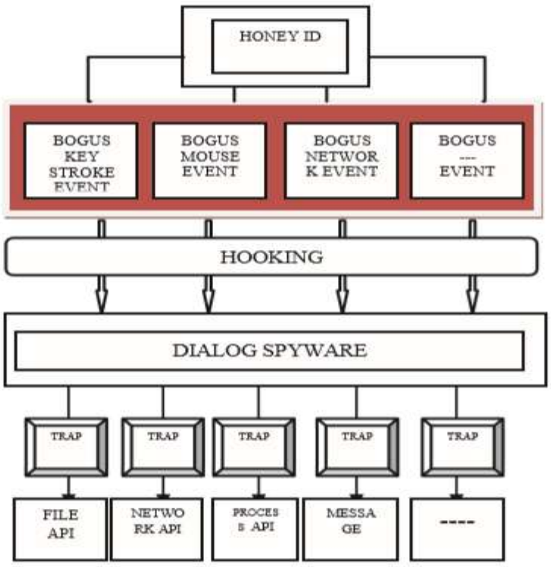


Figure 17. Basic concept of Honey ID [7]

Shaikh Saubiya Ahmed S. et al. [8] developed a prevention system against shoulder surfing attacks and key logging attack. System used an approach of graphical password based on text an exploited the technology of Persuasive Technology. The technique which has been employed in the system utilized viewport in clue point selection procedure. The protocol used in the technique created a text based graphical password to prevent their usage in session and login password. Authentication through the Cued click technique which has been proposed in the system contains two phases i.e. Registration Phase and Login Phase. Since, it has been assumed in the system that the registration process approved at secured environment which is not affected by key loggers which is practically not certain. As key logger operated in stealth mode, it may attack the registration process too without anybody's awareness. Registration phase is purely text based and if the registration environment is affected by key logger, hacker could easily crack the credentials as the generated log file is mailed to the designer. As the key logger spyware not only captured the keystrokes but also monitors the mouse pointer, cracking the system which has been proposed in this paper even after using the text based graphical password is still easier for the attacker.

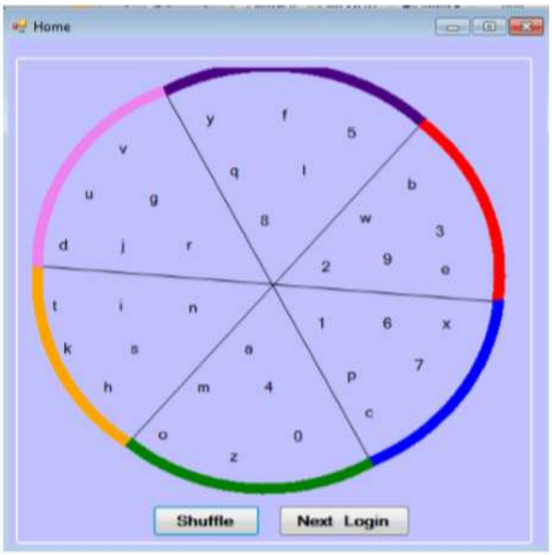


Figure 18. Password Authentication [8]

3. PROBLEM IDENTIFICATION

There are various techniques developed in the previously proposed works either to prevent the system from key logger or to detect the existence of key logger. Many techniques which have been developed in distinct papers tried to develop a secure log in environment which cannot be cracked by the key logger but failed to provide stable security. Even in mobile phones, various third party applications could easily install just by having the permission of internet contains malicious spyware. There is no any ideal system is developed which can assure the security of the system from the attacks of malicious spyware of key logger programs.

4. CONCLUSION

Most of the systems majorly relied on a technique to detect key loggers but there are varieties of malicious key logger present that can steal latent information. Certain systems are based on enrolling graphical password and some are based on temporary password token but key logger is also able to record cursor placement that transparent all the activities over the screen and if a system is able to secure password token then why not a password can be securely handle. In order to prevent the system from malicious key logger program, a system is proposed which can efficiently breach the monitoring and capturing technique of spyware programs like key logger and securely access the application by keeping the credentials secure.

REFERENCES:

[1] Mohammad Wazid, AvitaKatal, R.H. Goudar, D.P. Singh, Asit Tyagi, Robin Sharma and Priyanka Bhakuni, "A Framework for Detection and Prevention of Novel Keylogger Spyware Attacks", ISCO, IEEE Transaction, 2013.

[2] S.Gunalakshmii & P.Ezlunnalai "Mobile Key logger Detection Using Machine Learning Technique", IEEE Transaction, 2014.

[3] M Hossein Ahmadzadegan, Ali-Asghar Khorshidvand, MeherdadPezeshki, "A Method for Securing Username and Password against the Key Logger Software using the Logistic Map Chaos Method", IEEE Transaction, 2015.

[4] Junsung Cho, Geumhwan Cho and Hyoungshick Kim, "Keyboard or Key logger: a security analysis of third-party keyboards on Android", IEEE Transaction, 2015.

[5] NeenuN A, "On Screen Randomized Blank Keyboard, National Conference on Recent Advances in Electronics & Computer Engineering, RAECE -2015.

[6] Tasabeeh O. M. Ali, Omer S. A. Awadelseed, Abeer E. W. Eldewahi, "Random Multiple Layouts Keylogger Prevention Technique", Conference of Basic Sciences and Engineering Studies (SGCAC), 2016.

[7] A. Solairaj, S. C. Prabanand, J. Mathalairaj, C. Prathap and L. S. Vignesh, "Key Loggers Software Detection Techniques", Intelligent Systems and Control (ISCO), IEEE, 2016

[8] Shaikh Saubiya Ahmed S. and Narendra M. Shekokar, "Cued Click Authentication", IEEE Transaction, 2017.

[9] www.softpedia.com/get/Security/Security-Related/All-In-One-Keylogger.shtml