ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A New Security Approach through Key Strokes Recognition in Personal Computing Systems

K.Anji Reddy
Sr.Assistant Professor & HOD,
Dept of Computer Applications,
Velagapudi Ramakrishna
Siddhartha Engineering College,
A.P., India.

B.Venkata Rao
Assistant Professor,
Dept of Computer Applications,
Velagapudi Ramakrishna
Siddhartha Engineering College,
A.P., India.

Kalisetti Durga Prasad
Pursuing MCA,
Velagapudi Ramakrishna
Siddhartha Engineering College,
A.P., India.

Abstract:

As PC's connected in different networks have started being used for multiple purposes, the security of this system became an issue of concern. This led to the entry of passwords and smart cards into the market but was later attacked by hackers and these techniques unable to reveal the victim's information. Here the application is developing a windows application for pc called key strokes Recognition. It is an application used for action of tracking the keys whenever user presses keyboard, keyboard strokes are captured in hidden monitoring manner, so users are unaware that their actions are monitored. This application also contain that action of capturing the desktop if a person is using the mouse or joystick instead of keyboard that can ultimately be stored in a hidden log file that log file is being viewed by Owner of this Application only. It can be accessed by administrator only. This technology can be used for finding out all the sites and files which are being accessed by any person in the administrator's absence. The application can be used for monitoring that children cannot access certain websites or spend money online, or to ensure that employees are not wasting time online while at work.

Keywords:
Key Strokes, Mouse Clicks, tracking, monitoring, log file, Screen shots.

1. INTRODUCTION:

Key strokes recognitions have somewhat of a bad reputation in the technology world because more often it's associated with illegal spying and theft of personal and monetary information. In reality even though that's one of the main uses, it can be used for other more appropriate and legal tasks. One clear example of this would be at a company's security policy which clearly states that the workers activities can be monitored with Key strokes recognition and can be used to monitor an employee who is under suspicion of being a malicious insider. By logging his activity on his work station the company may be able to confirm their suspicions or clear his name. Sometimes a simple and inexpensive tool like Key strokes recognitions may save companies millions in damages. The same concept may be applied to a more family based used like monitor the activities of under aged children on the web which may help to the child & safety from online predators and dangers. There are different types of Key strokes recognitions divided into 2 main groups Hardware Key strokes recognitions and Software Key strokes recognitions.

What Information a Key Strokes Recognition Can Collect

The capabilities of Key Strokes Recognition vary, but when installed on a device they can generally do the following:

- capture any passwords entered by users on the device
- take screen captures of the device at periodic intervals
- record the URLs that were visited via Web browsers, and possibly also take screen captures of the Web pages viewed
- record a list of the applications run by users on the device
- capture logs of all instant messaging (IM) sessions
- capture copies of sent emails
- automatically send the reports containing stored logs and emails to a remote location (by email, FTP or HTTP).

  This key Strokes Recognition allow not only keyboard keystrokes to be captured but also are often capable of collecting screen captures from the computer. Normal key logging programs store their data on the local hard drive, but some are programmed to automatically transmit data over the network to a remote computer or Web server.

The application is developing a windows app for pc called key strokes Recognition. Key Strokes Recognition is an application used for action of tracking the keys when ever user presses keyboard, keyword strokes are captured in converted manner so users are unaware that their actions are monitored. This software also contain that action of capturing the desktop if a person is using the mouse or joystick instead of keyboard that can ultimately be stored in a hidden log file that log file is being viewed by administrator only. It can be accessed by administrator only. This technology can be used for finding out all the sites and files which are being accessed by any person in the administrator’s absence. This application can be used for monitoring that children cannot access certain websites or spend money online, or to ensure that employees are not wasting time online while at work. This app for pc and the app called key stroke analysis. Key logger is an application used for action of tracking the keys when ever user presses keyboard, keyword strokes are captured in converted manner so users are unaware that their actions are monitored. This software also contain that action of capturing the desktop if a person is using the mouse or joystick instead of keyboard that can ultimately be stored in a hidden log file that log file is being viewed by administrator only. It can be accessed by administrator only. This technology can be used for finding out all the sites and files which are being accessed by any person in the administrator’s absence. The application can be used for proper identification and authentication. The typing dynamics can be used for different user profiles. Thus this becomes a valid tool for ascertaining personal identity. The used Programming language in this application is Java in particularly the Technologies Global keyboard and mouse listeners for Java in this a JNativeHook is a library to provide global keyboard and mouse listeners for Java. This will allow you to listen for global shortcuts or mouse motion that would otherwise be impossible using pure Java. To accomplish this task, JNativeHook leverages platform-dependent native code through Java's native interface to create low-level system-wide hooks and deliver those events to your application.

The following events are available via their respective listeners.

- Key Press Events
- Key Release Events
- Key Typed Events
- Mouse Down Events
- Mouse Up Events
- Mouse Click Events
- Mouse Move Events
- Mouse Drag Events
- Mouse Wheel Events

In addition to global event listeners, this library has the ability to post native events back to the native operating system.

2. LITERATURE SURVEY:

Objective of the Key Strokes Recognition concept is developing a windows application for pc and the app called key stroke analysis. Key logger is an application used for action of tracking the keys when ever user presses keyboard, keyword strokes are captured in converted manner so users are unaware that their actions are monitored. This software also contain that action of capturing the desktop if a person is using the mouse or joystick instead of keyboard that can ultimately be stored in a hidden log file that log file is being viewed by administrator only. It can be accessed by administrator only. This technology can be used for finding out all the sites and files which are being accessed by any person in the administrator's absence. The application can be used for proper identification and authentication. The typing dynamics can be used for different user profiles. Thus this becomes a valid tool for ascertaining personal identity.

Key Strokes Recognition

A key Strokes Recognition program can be software-based, and this is typically part of an extensive computer security system or part of a piece of malicious software (malware). Some people use security software on their computers to ensure that children cannot access certain websites or spend money online, or to ensure that employees are not wasting time online while at work. Some of these programs can include Keystroke Recognition as a feature, typically intended to track the activities of unsupervised minors and employees using the computer. (Schilperoord 1996) Certain hardware devices can be used as keystroke loggers. These devices are plugged in between the cord of a keyboard and the input on a computer tower and are similar in size and appearance to a keyboard adapter plug. Keystroke Recognition hardware can be especially troublesome because the information is logged by the device before it ever actually reaches the computer, so computer security software is useless against these types of devices. Fortunately, these devices can typically be seen by casual inspection of a computer and should be watched for whenever a person is using a public computer. (Torrance, Waes & Galbraith 2007) Some Keystroke Recognition, however, is performed by malicious programs such as Trojan horses or other types of malware. These programs are typically intended to log the keystrokes of a computer user as he or she enters account numbers, passwords, and other sensitive information. The data can then be remote accessed or sent to a specific email address or Internet protocol (IP) address that is owned by the malware designer. (Sullivan & Lindgren 2006) This data can then be used to access the accounts and can even be used to change passwords and keep the legitimate user from accessing his or her information.Though some computer security programs can detect these types of malicious keystroke loggers, no single program is always a perfect defense against such practices. Much like avoiding any other piece of malware, caution should be taken by computer users whenever opening mail from someone they do not know, or following suspicious links in email and on Internet websites.

Using antivirus and antimalware programs, and keeping them constantly updated, is also a great way to better detect programs such as Keystroke Recognition malware and remove them before private information is compromised. (Cheng & Barone 2007) A brief inspection of any text on Cognitive Science reveals that the perception, storage, retrieval and transformation of information by the cognitive architecture have been extensively studied but the transmission of information has been rather neglected. Much less is known about how chunks of information in the mind are processed for external production than is known about the other fundamental types of cognitive processes. For example, write "All for one, one for all" in capital letters. What processes are occurring during the ˜10 seconds during which the sentence is being transmitted from your mind to the paper? Do the processes occur in a largely serial fashion or do they partly overlap and even run ..

3. PROPOSED METHODOLOGY:

Existing System:

Here the windows app which already exists captures just the key strokes. Since the application is hidden user is unaware that his actions are monitored.

Proposed System:

So here in this application we want to develop the windows app by using the language java and this application would like to include certain extra features to the key logger such as recording desktop activity taking the screen shorts at regular intervals , logs are encrypted. The application is very easy to use so that customers feel happy while using this.

4. RELATRED WORK

How Key Strokes Recognition Capture Data When looking at Key Strokes Recognition s, we can typically distinguish three basic types: User- mode Key Strokes Recognitions, kernel mode Key Strokes Recognition s and hardware-based Key Strokes Recognition s. In this post, we will focus on the first two types – software-based Key Strokes Recognitions. Hardware-based Key Strokes Recognition s work by intercepting data sent from external devices (such as keyboard or mouse) to the computer hardware, and are thus outside the reach of most remote attackers.

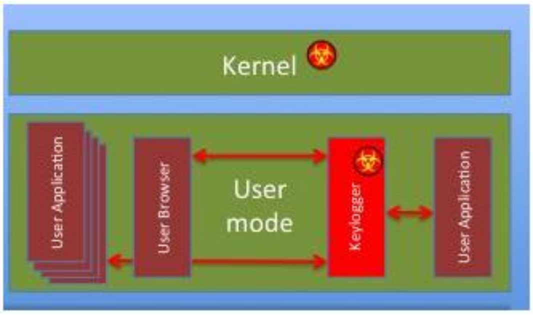


Fig : Overview of Key Strokes Recognition methods

In user-mode Key Strokes Recognitions, a very common approach used to steal information typed by the user is through the use of the windows API Set WindowsHook. This API can be used to intercept events from the system, such as keyboard and mouse activity. When the to-be-intercepted action is triggered, a function of the attacker's choosing is executed. Another user-mode method for capturing keystrokes that we found in many malware variants consists of continuously checking the system's keyboard state using the GetAsyncKeyState or GetKeyState API functions. Different from the first method, which notifies you at every keyboard event, the attacker here needs to actively monitor which keys are pressed. Kernel-mode Key Strokes Recognition s are more powerful than their user-mode counterparts, as they work with higher privileges, but are inherently more complex to implement. This type of Key Strokes Recognition uses filter drivers to intercept keystrokes received from the keyboard or modify internal Windows kernel structures in order to capture input data. The complexity and mostly-undocumented nature of kernel code can lead to malfunction of the system if a sample is executed on an unsupported system, making user-mode Key Strokes Recognition s a more prominent approach.

5. IMPLEMENTATION:

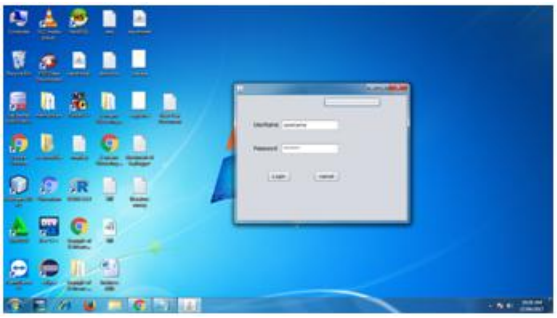


Fig 5.1: Login page

As shown in the above figure owner of the application can login to application with his provided username and password.

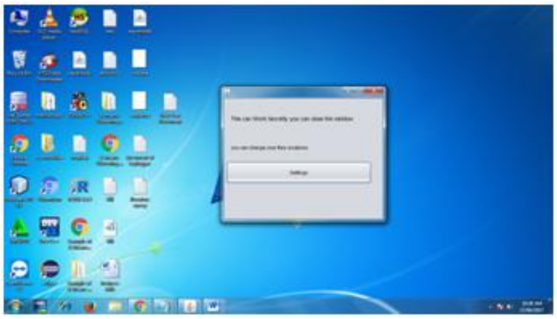


Fig 5.2: Starting Screen

After login the owner can see the starting as above and he can make some setting if he wants.

Fig 5.3: Running in the Background

In the above screen the application is still running even though we closed the application window.

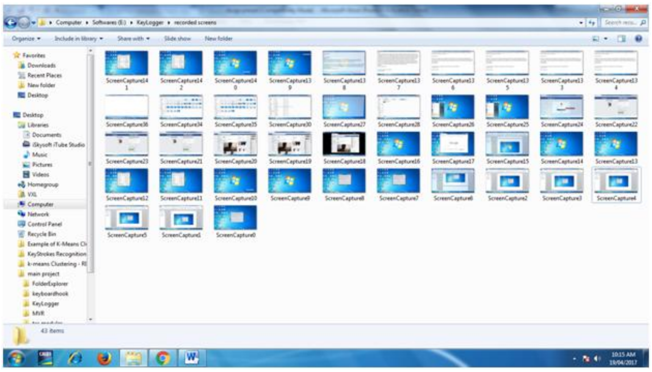


Fig 5.4: The Screen Shots stored Folder

Above shows that the recorded screens can be stored in a directory which was only known by the owner of the Key Strokes Recognition application

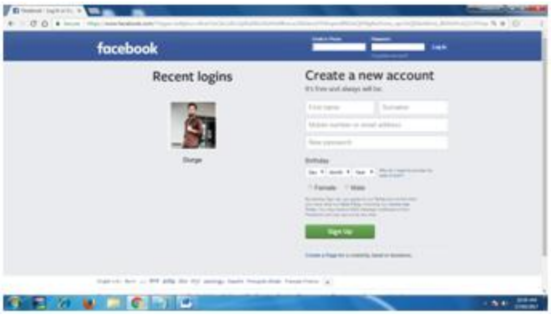


Fig 5.5: Trying to login in the facebook

Here the user is trying to login in the facebook these screen and user typed key strokes will be stored in a private place due to background run of Key Strokes Recognition Application.

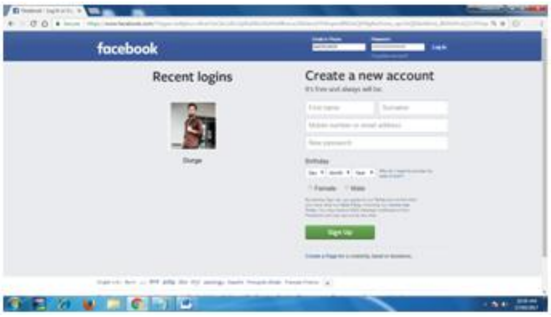


Fig 5.6: Login with dummy password screen

In above screen the user is going to type the password of course, it was a testing password. it will be stored in flat file.

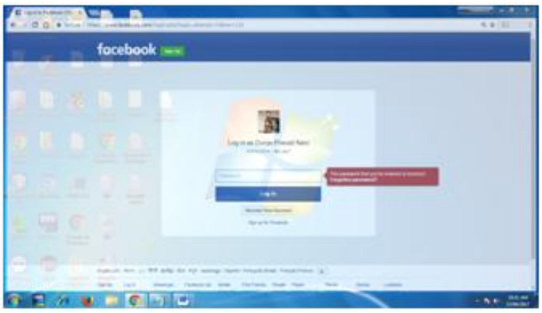
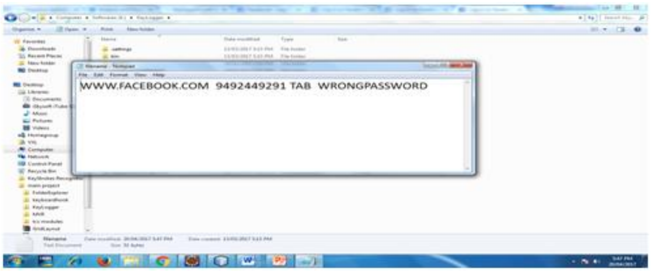


Fig 5.7: Screen after typing wrong password

These keystrokes of username and wrong password is already recorded will be stored in flat file.



WWW.FACEBOOK.COM 9492449291 TAB WRONGPASSWORD

Fig 5.7: Flat file in which the user typed Key Strokes Stored

Finally above shown figure is the file where the Key Strokes were stored and user typed www.facebook.com and type his mobile number 9492449291 of course numpad numbers of keyboard also stored differently. He typed the password "this is wrong"

CONCLUSION:

This application went over most issues regarding Keystroke logging. Although Key strokes recognitions have a bad reputation in society, the research done to elaborate this shows how these applications can be used not always in a malicious way of action such as illegal spying and theft of personal information. At a company level, Key strokes recognitions can be used to monitor any suspicious activity that may cause a serious liability to the company's benefit. Workers who are under doubt can be explicitly be discover or clear their names. This helps the company ensure their interests before any bigger security issue happens, making them save larger quantities of money. Another legal way of using a Key strokes recognition is in a closer and more personal level, home. Any head of household wants their children going on the internet without any consent of what they are watching, what websites are they surfing in, and most important who they are in contact with. Nowadays, there are a lot of people looking for victims online. Child's predator, kidnappers, and so all are always seeking innocent children, and Key strokes recognitions can be very helpful in order to minimize those kinds of attacks from occurring. In this it is also discussed the different kinds of Key strokes recognitions and their advantages compared to one another. The Keystroke Recognitions can be divided into 2 main groups Hardware Key strokes recognitions and Software Key strokes recognitions. The main advantage of Software Key strokes recognitions is that they are invisible to anyone except Owner of the application.

REFERENCES

[1] S. Sagiroglu and G. Canbek, "Keyloggers," IEEE Technology and Society Magazine, vol. 28, no. 3, pp. 10 –17, fall 2009.

[2]ThinkGeek.com,"Spykeylogger,"2010(accessedMay8,2010),http://www.thinkgeek.com/gadgets/security/c49f/.

[3] G. Hoglund and J. Butler, Rootkits: Subverting the Windows Kernel. Addison-Wesley Professional, 2005.

[4] C.Wood and R. K. Raj, "Sample keylogging programming projects," 2010 (accessed May 8, 2010), http://www.cs.rit.edu/~rkr/ keylogger2010.

[5] Bauer, Michael D., Chapter 10 (System Log Management and Monitoring) of Building Secure Servers with LINUX, O'Reilly, 2002.

[6] Babbin, Jacob et al, Security Log Management: Identifying Patterns in the Chaos, Syngress, 2006

[7] Stout, Kent," Central Logging with a Twist of COTS in a Solaris Environment.", SANS Institute, March 2002, URL: http://www.sans.org/rr/papers/52/540.pdf

[8] Stout, Kent," Central Logging with a Twist of COTS in a Solaris Environment.", SANS Institute, March2002,URL: http://www.sans.org/rr/papers/52/540.pdf

[9] Mendez, William, "Windows NT/2000 Event Logs.", SANS Institute, April 2002, URL: http://www.sans.org/rr/papers/67/290.pdf

[10] T.Olzak, “Keystroke logging (keylogging),” Adventures in Security, April 2008 (accessed May 8, 2010),http://adventuresinsecurity.com/ images/Keystroke_Logging.pdf.

[11] S.Shah, “Browser exploits-attacks and defense,” London, 2008(accessed May 8, 2010), http://eusecwest.com/esw08/esw08-shah.pdf.

[12] P. Mell, K. Kent, and J. Nusbaum, “Guide to malware incident prevention and handling,” National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. 800-83, November 2005.

[13] B. Whitty, “The ethics of key loggers,” Article on Technibble.com, June 2007 (accessed May 8, 2010), http://www.technibble.com/the-ethics-of-key-loggers/.

[14] Stout, Kent, ”Central Logging with a Twist of COTS in a Solaris Environment.”, SANS Institute, March 2002, URL: http://www.sans.org/rr/papers/52/540.pdf

[15]“Intrusion Detection planning guide.”, Cisco Systems, Inc, 1999, URL: http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_maintenance_guide_chapter09186a008007d254.htm l, page 2-3

[16] Stansbury, Jim, “Archiving Event Logs.”, SANS Institute, August 2002, URL: http://www.sans.org/rr/papers/30/1002.pdf

[17] Glenn, Michael, “A Summary of DOS/DDOS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment.”, SANS Institute, August 2003.

[18] “Snort The Open Source Network Intrusion Detection System.”, URL: http://www.snort.org,1 December 2003.

[19] Mendez, William, “Windows NT/2000 Event Logs.”, SANS Institute, April 2002, URL: http://www.sans.org/rr/papers/67/290.pdf

[20] J. Butler, B. Arbaugh, and N. Petroni, “Rˆ2: The exponential growth of rootkit techniques,” in BlackHat USA 2006, 2006 (accessed May 8, 2010), http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Butler.pdf.

[21] Symantec Corporation, “Viruses and risks,” April 2010, http://www.symantec.com/norton/security_response/index.jsp.

[22] M. Baig and W. Mahmood, “A robust technique of anti key-logging using key-logging mechanism,” in IEEE-IES Digital EcoSystems and Technologies Conference, 2007, February 2007, pp. 314 –318.

[23] M. Aslam, R. N. Idrees, M. M. Baig, and M. A. Arshad, “Antihook shield against the software key loggers,” in Proceedings of the National Conference of Emerging Technologies, 2004.

[24] L. Martignoni, E. Stinson, M. Fredrikson, S. Jha, and J. C. Mitchell, “A layered architecture for detecting malicious behaviors,” in RAID ’08: Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer-Verlag, 2008.

[25] D. Le, C. Yue, T. Smart, and H. Wang, “Detecting kernel level keyloggers through dynamic taint analysis,” College of William & Mary, Department of Computer Science, Williamsburg, VA, Tech. Rep. WM-CS-2008-05, May 2008.

[26] B. Cogswell and M. Russinovich, “Rootkitrevealer v1.71,” 2006 (accessed May 8, 2010), http://technet.microsoft.com/en-us/sysinternals/ bb897445.aspx.

[27] C. Wood and R. K. Raj, "Sample keylogging programming projects," 2010 (accessed May 8, 2010), http://www.cs.rit.edu/~rkr/ keylogger2010. [28] B. Whitty, "The ethics of key loggers," Article on Technibble.com, June 2007 (accessed May 8, 2010),
http://www.technibble.com/ the-ethics-of-key-loggers/.

AUTHORS' BIOGRAPHY:

Mr. K.Anji Reddy

Received the M.Tech degree from JNTUA, Ananthapuram in 2010 and received the M.C.A degree from Osmania University, in September 1988. He is currently working as Head of the Department, Department of computer applications, Velagapudi Rama Krishna Siddhartha Engineering College (Autonomous), Vijayawada, Andhra Pradesh. He has 17 years of teaching experience and pursuing Ph.D at Rayalaseema University, Kurnool. His research areas are Data mining and Data warehousing.

Mr.Venkata Rao Barige

He is an Assistant Professor in Department of Computer Applications, V.R.Siddhartha Engineering College,Vijayawada. And He is also a Research Scholar of Computer Science & Engineering in Rayalaseema University, Kurnool. He has attended various National and International Conferences within the State.And also published his research papers in Reputed National and International Indexed Journals. He received the best mentor award by Unisys Info systems, Bangaluru for making students projects national wide success. He implemented various online automated systems in his Institution.

Mr. K.Durga Prasad

He is persuing his MCA degree in Department of Computer Applications, V.R.Siddhartha Engineering College, Vijayawada. His areas of intrest includes advance java technologies and web designing tools.