ISSN 2047-3338

Survey of Keylogger Technologies

Yahye Abukar Ahmed[1], Mohd Aizaini Maarof[2], Fuad Mire Hassan[3] and Mohamed Muse Abshir[4]

[1-4]Department of Computer Science, Faculty of Computer Science & Information Systems, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia

[1]yahy@simad.edu.so, [2]aizaini@utm.my, [3]fuaadmire@gmail.com, [4]inaboqormuse@gmail.com

***Abstract*– Keyloggers are type of a rootkit malware that capture typed keystroke events of the keyboard and save into log file, therefore, it is able to intercept sensitive information such as usernames, PINs, and passwords, thus transmits into malicious attacker without attracting the attention of users. Keyloggers presents a major threat to business transactions and personal activities such E-commerce, online banking, email chatting, and system database. Antivirus software I commonly used to detect and remove known keyloggers. However, it cannot detect unknown keyloggers. This paper presents an overview of keylogger programs, types, characteristics of keyloggers and methodology they use. A case study on Blackbery is used as a real time example in this paper. Finally we will analyze the current detection techniques, and explore several proactive techniques.**

***Index Terms*– Keylogger, Hooking, Signature-Based, Malware Rootkits, Anomaly Based, OS and API**

I. INTRODUCTION

MALWARE is termed by numerous names, Such as malicious code (MC), malicious software and malcode. Numerous [20], McGraw and Morrisett [21] define malicious code as "any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system", Meanwhile, keyloggers are becoming more diverse, evasive, sophisticated, and increasingly difficult to detect by anti-virus software and anti-keyloggers based on signature analysis [28].

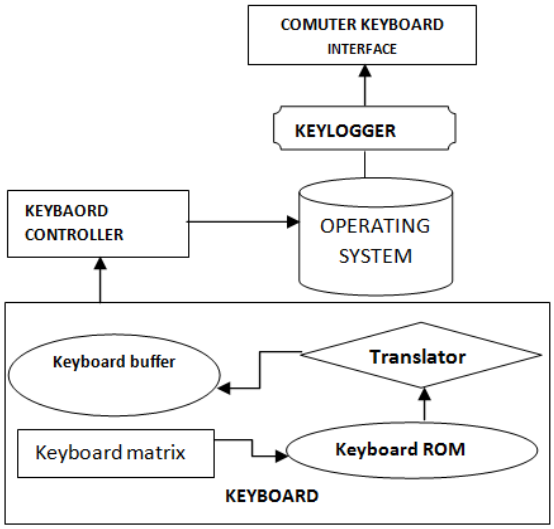
Keylogger is one of malware rootkits that intercepts the user's typed keystroke on the keyboard. The first primary target of the keylogger is to secretly record confidential information of user's input through keystroke monitoring and then relaying this valuable information to others [8]. The keyboard is the focal method of inputting textual and numerical information on the computer through typing. Therefore, an attacker can simply retrieve and access important information with the help of logging keystrokes. Generally, there is no intelligence built-in keylogger, but logs offer information about every single keyboard event and applications that users clicked or typed. Despite the lack of information on what of application is used, logs provide enough evidence that allow one to know what users are doing [1]. Data captured include passwords, user ID's, document contents and other critical information; therefore, an attacker can obtain sensitive data without cracking database or file server.

Nowadays, Keylogging acts a critical threat to the security and privacy of our systems [24], [15]. These causes because of the keylogger program can retrieve and collect the user's personal information, credit cards, passwords, performed by hackers; keylogging is undetectable as it runs in secreted mode. The stealthy keylogger cannot be detected by many Anti-viruses software as running on the victim's machine. The user has no way to determine the presence of keylogger on his machine, therefore, he turn into a victim of the identity theft [39]. In this work we observe various types of keyloggers, how they are injected into the system and analyzing current detection technique.

The remainder of this paper is structured as follows. Section II discusses how keyloggers work. Section III outlines related work of keylogger. Section IV details out the categories of software keylogger. Section V, we evaluate the methodology of developing the keylogger software system. Section VI, we analyze the current software keyloggers detection techniques, and propose some proactive steps.

II. HOW KEYBOARD WORKS

Keyboard is primary target of most common keyloggers; it consists of matrix of circuit with keys also known as key matrix, there are many different types of key matrix depending on keyboard manufactures [26]. However, the circuit closes key matrix when the user presses key, then keyboard processor and ROM detect this events. The processor translates the circuit location to a character or control code and sends to keyboard buffer.



F
ig. 1. Shows how Keyboard works

The computer's keyboard controller receives the incoming keyboard data and forwards it to the windows operating system. Data travelling between operating system and computer keyboard interface is, intercepted by keylogger. Thus the message flow is not transferred into next hook procedure [32].

A. *Types of Keyloggers*

Keyloggers fall into four main categories: Hardware, acoustic, wireless intercept and software [9]. Although they have different implications and different information capturing process, these keylogger share one thing in common; they save captured sensitive data and information in a log file.

Hardware keylogger

Hardware keylogger is physical device located between the keyboard and the computer. There are two connection methods; keyloggers can be connected between the keyboard and computer directly. Examples of this method are PS/2 and the USP keylogger [9].

Fig. 2: Shows keylogger of PS/2 [9]

The second method does not require physical connection to the PC, but installation of keylogger circuit into the keyboard standard. This method has advantages that users cannot monitor keyloggers physically.

Acoustic keylogger

Unlike hardware keylogger, Acoustic keylogger on analysis and captures the sound of individual keystrokes. Special equipment is required to listen to the sound of the user's typing. Parabolic microphones are utilized to record a long distance, so this microphone is used to pick up the keyboard sound from hundred feet away of targeted area or work [9], [31].

Wireless keylogger

Wireless keylogger exploits Bluetooth interfaces to transfer captured data to a log file up to the distance of 100M [7]. The primary target of this wireless keylogger is to intercept transmitted packet from wireless keyboard that uses 27 MHz RF connection of encrypted RF transported keystroke character. However, the bad news of this wireless keylogger needs receiver/antenna relatively closed to the target area work [9]. Fig. 3 shows Bluetooth-accessible keylogger.

Fig. 3. Bluetooth-accessible keylogger (wirelesskeylogger.com)

Software keylogger

Software keylogger intercept data travelling along the keyboard and the operating system. It collects keystroke events, stores them in a remote location, and then transmits to the attacker who installed the keylogger [10]. Research about removal of spyware parasite reported a total of 540 keyloggers and they were mostly software-based [11]. Window operating system has many event mechanisms, for examples, when a character is pressed on the keyboard or mouse clicked; the keyboard driver on the operating system translates this event into window message called WM_KEYDOAWN. This message is pushed into system message queue. Window operating system in turn places this message into message queue of the application thread with associated active window in the screen. This queue is polled by the thread and then sends message to the window procedure of the active window [10].

III. Related Works

Malware detection is often analyzed as being static or dynamic; static is based on signature detection that requires malicious signature present in the repository. The biggest disadvantage of this technique is that it has nothing to do against novel keyloggers. Dynamic detection must be used to

detect keylogging malware; behavioral based detection was implemented. As keyloggers always use Windows hooks, Aslam et al.[3] discussed ant-hooked shield that employs by flagging program that hooked system routines that always targeted by keyloggers; However, it is easy for keylogger developers to evade this detection technique by using different methods to log the user activities other than using SetWindowsHookExhowever.

Dynamic based detection techniques or behavioral based was proposed by Martignoni et al. [4] showed the semantic gap between high-level behavior and their low-level representative computer, and achieved largely for the unique layered architecture. This approach is used to modeling semantic gap through structural hierarchic. Their model detector use suspicious behavior mechanism as input with system broad process execution for monitoring, so flagging suspicious activity is recognized if a process's activity closely matches the behavior specifications. Meanwhile Ortoline et al [6] implemented Black-box approach to detect the most common keyloggers. Their model was based on behavior of the keylogger by means of keystroke to the I/O pattern formed by keyloggers.

Many of the dynamic detection mechanism being implemented and researched, but it is hard to detect keyloggers accurately. Sreenivas et al. [7] detected keylogger by using TAKD algorithms that can easily integrated into routine devices such as router, gateway, firewall, IDS and so on to improve its keylogging detection. TAKD algorithm incorporated anomaly-based detection mechanism and log based technique to overcome the problem of signature based detection.

Another useful detection mechanism is Taint data analysis framework uses a host-based Intrusion Detection System (IDS) to taint, monitor, and examine the keyboard data at the keyboard device driver level. This framework aims to detect kernel-level keyloggers that modifies the normal flow of control data in the keyboard drive to extract keystroke data events and then transmit back to the attacker. Thus extraction occurs while data travels along the chain of keyboard device driver in the kernel. This detection model was proposed by Le et al. [5].

A. Impact of Keyloggers

A keylogger captures all keystrokes that the user types on the computer keyboard, including passwords, personal information entered into an online registration form (e.g., a mailing address or telephone number), and financial information submitted as part of an online transaction [30]. Unlike other types of malicious program such as viruses and worms, keyloggers associate with or share the system resources such as CPU and memory with legitimate programs that running on the system undetected for as long as they require without attracting the attention of users. There are many types of keyloggers, having different forms and behaviors, but pose a great threat to user privacy and security. First, it is hard to distinguish from operating system files even when doing a directory listing of hidden files. Second, they have the ability to decrypt information passing through internet and transmit to the attacker. Therefore, security experts are now focusing on kernel keylogger which is the most difficult keylogger whose target on the kernel operating system, with the help of hooking mechanism. Thus, the following section will focus on the software keylogger.

IV. SOFTWARE KEYLOGGER CATEGORIES

Software keyloggers fall into four main categories, which are interrogation cycle, traps keylogger, rootkits keylogger and keylogger kernel mood [12].these categories are based on how keylogger operate.

A. Interrogation cycle Software keylogger

This type of keylogger is simplest and can easily been detected. It uses of a number of API functions that return information to int variables, and custom function to return char during function call process [23]. These functions interrogate keys on the keyboard, for instance if a key is pressed or released, the GetAsyncKeyState function determines whether a key is up or down at the time the function is called. Usually, GetKeyboardState Copies the status of the 256 virtual keys to the specified buffer then returns the state of each key on the keyboard that compatible with GUI applications. To avoid data missing, it is required to use high speed interrogation with 10-20 polls per second [12].

B. Traps Software keylogger

Generating of keyboard spyware that based on trap of hook mechanism is considered to be classical method. This mechanism works only for GUI applications to trap not only the keystrokes themselves but, message that are processed in window of other GUI application as well. For purpose of installation hook mechanism, the hook handling code has to be put in a DLL, with the help of API functions. For example, SetWindowHookEx performs installation of an application-defined hook procedure into a hook chain, and unhooksWindowHookEx helps for removal of the hook. When SetWindowHookEx function is called, the keylogger determines which type of message called the hook handler. The registration of the hook in the first time, the GUI application receives the first message that satisfies the activation of the hook registration, and then DLL including hook code is loaded into process's address space. This determines the amount of memory allocated for all likely addresses for a computational entity, such as a device or a file [12].

C. Rootkits Software Keylogger

Unlike trap software keylogger, the rootkit software keylogger are the most dangerous type of keylogger, but it is a relatively rare. It captures set of function responsible for

processing of messages or the inputted text processing. It has methods called GetMessage, TranslateMessage library, and PeekMessage user32.dll function to capture messages and to monitor the messages obtained by GUI application. Therefore, it easily intercepts the messages and data with the help of many methods and set of function [12].

D. Kernel-Mode Software Keylogger

Generally, most of the keyloggers use kernel mode techniques that based on tow standard principles: first, installing a driver-filter for the keyboard driver. This provide spyware to connect keyboard drive stack with the help IOAttachDevice and IOCreateDevice function automatically after loading the operating system.

The bad news is that the driver-filter does not register or record I/O Request Packets (IRPs) including data about keystrokes, but instead targets IRPs with requests for data from the KBdclass driver. Keystrokes Information will be available after KBdclass driver finish the IRP and transfer the requested data to the IRP buffer. Therefore the keylogger filter with the help of the API function IOSetCompletionRoutine has a chance to install its own termination procedure for every IRP of the IRP_MJ_READ.

Second, the use of rootkit technologies with the help of a user mode rootkit keylogger can intercept PeekMessage in win32k.sys functions by searching for and modifying their addresses in the system table KeServiceDescriptorTableShadow [12].

V. METHODOLOGY: KEYLOGGER SYSTEM

There are three main methods to develop keylogger systems [10]: the Windows Keyboard Hook method, the Keyboard State Table method, and the Kernel-Based Keyboard Filter Driver method. First, Windows Keyboard Hook method based on operating system provides some functions to Hook-based keyloggers for monitoring the keyboard. When a key is pressed the OS records the action and registers the application itself. Later any message running in this mechanism is approved by the application before going to the original target that receives the message. Today, most keyloggers utilize this technique to capture keystrokes.

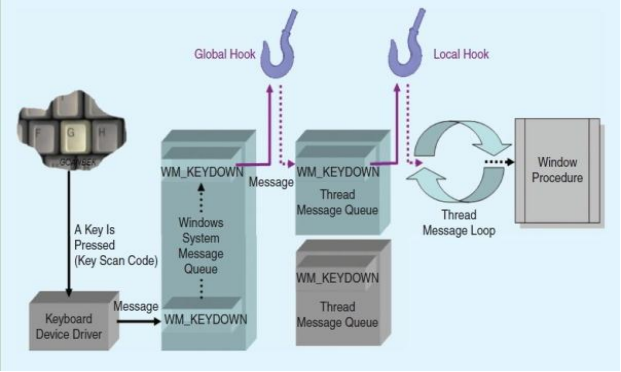


Fig. 4. Shows Block diagram hook mechanism [10], [35]

There are two distinct types of hooks related to windows message: Global hook checks system wide message and Local hook monitors application specific message. Keyboard hook is:

1) Capable of reading all keyboard messages and transfer them to the next hook procedure in a chain.
2) Able to modify the original message and pass it to the next hook procedure.
3) Talented to interrupt the flow of the message by not passing it to the next hook procedure

Second method is Keyboard State Table method which has table consists of the status of 256 virtual keys. Therefore, application that uses a window interface refers to this table. Applications normally use this table to determine the states of the key whether it is up or down. For example, when key is pressed with Ctrl or Shift key, keylogger can utilize the GetKeyboardState API functions to disclose or reveal the keystroke information, by adding its thread to the top-level of thread message loop of window using Attach- ThreadInput API.

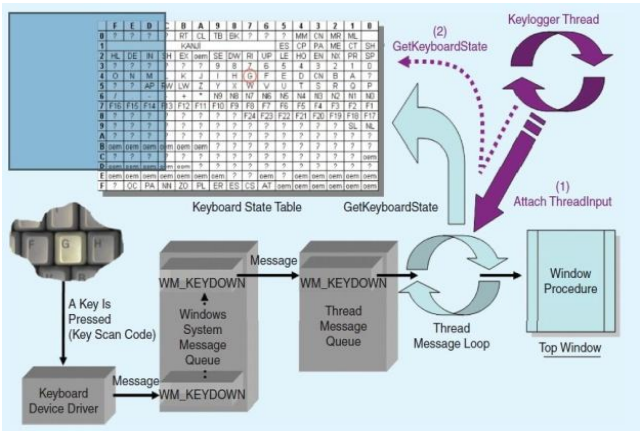


Fig. 5. Shows keyboard stat table method [10], [27].

Unlike other methods, the Kernel-Based Keyboard Filter Driver method located in the kernel level and hard to detect, but to install them on a target machine, administrator privileges are required. In this method, keylogger that has been installed keyboard filter driver before install the system's keyboard device driver can capture the keystrokes and data even before reach the operating system [34].

A. Keylogger Characteristics

Although the main purpose of keyloggers is to keep on a user's keyboard actions, they now have advanced capabilities that widen beyond that function. For example, they can track virtually application running on a computer. The informations keyloggers record, sense, and transmit are the following [13]:

Keystrokes on the keyboard :

1) Site Monitoring
2) Chatting Monitoring
3) Program / Tracking Application

4) Recording Printing Activity
5) Clipboard recording and Monitoring
6) Recording File/folder and Monitoring Screenshots
7) E-mail Reporting
8) Password Protection and Hot Key

B. How keyloggers spread

Keyloggers spread in same way as the malicious programs do. Except some cases where software companies define a keylogger as a software program designed to secretly monitor and log all keystrokes. For example, jealous spouse or partner purchases keyloggers software and installs target machine to monitor the activities performing the victim. Keyloggers are mostly spread using the following methods [14], [37]:

1) Opening file attached and emails cause installation of keylogger.
2) When a file is launched from an open-access directory on a P2P network; a keylogger can be installed.
3) A keylogger can be installed via a web page script which exploits browser vulnerability. The keylogger program will automatically be launched when a user visits a infected site,
4) Another malicious program that present on victim machine can install a keylogger, if the program is able to downloading and installing other malware to the system.

C. Case Study: BlackBerry's eBlaster Mobile software

Computer monitoring spy or keylogger records user' activity on the mobile, website visiting or typing keystrokes on the computer. Therefore, the integration of mobile applications and spy keylogger gave chance to software companies to develop profitable application. For example, SpectorSoft Company is a software manufacturer that sells legal stealth software. The company is launching eBlaster Mobile which is cell phone software for BlackBerry that provides parents chance to monitor their children activity performed on their Smartphone. It also offers a sufficient set of logging features such as text messages, chat conversations in BlackBerry Messenger, call history, video logs and photo. Recently it offered a few advanced stealth features such as GPS monitoring. Many customers declared this spy software has saved their children from Internet dangers.

VI. Analyzing Current Detection Techniques

Statistics show the technique of malware detection and prevention is not guarantee 100%, especially rootkits modify the operating system [2], [36]. In this section, we survey some main classes of keylogger detector techniques by mean of methods used both application-based and kernel based [5]. Then, we review some proactive technique.

First, Application keylogger detector: 93% of personal computers use the Microsoft Windows [16]; the purpose of the most application keylogger detectors is to detect spyware keyloggers in MS Windows. Installation of these keyloggers in a computer can be achieved in different ways, such as web browser email, or some remote access methods. To detect them, two different techniques are used, hook-based and signature-based [38].

Hook-based: A hook is a point in the system message-handling mechanism. So this technique utilize the advantage of the SetWindowsHookEx() function to observe the keystroke data passing between two hook procedures. Therefore, interception of a keylogger between these hook procedures can be detected. This technique is more effective widely used. For instance, in HookFinder [18], [25], and System Virginity Verifier [17] used this technique to detect hook-based malwares.

Signature-based: this technique is based on a file signature to monitor modification of files such as dynamic linked libraries and registry entries that are inserted into the system by keyloggers. Therefore, application keyloggers whose signatures are found in the database are reffered to be malicious.

Another important category of detection method is behavior based detection. In this technique instead of looking for the specific file signature, the Signature-based: this technique is based on a file signature to monitor modification of files such as dynamic linked libraries and registry entries that are inserted into the system by keyloggers. Therefore, application keyloggers whose signatures are found in the database are reffered to be malicious.

Another important category of detection method is behavior based detection. In this technique instead of looking for the specific file signature, the behavior of the application is scrutinized. However, this method inevitably has a high false positive rate because novel keyloggers have behaviors of stealthiness and form of legitimate applications so it is possible for keyloggers to evade this detection.

The anti-rootkits technique was proposed to detect kernel keyloggers. This technique usually concerns in the memory and scans the processes, modules in the kernel, and loaded drivers to get suspected activities. However, kernel keyloggers cannot be detected by anti-rootkits, because of it is successfully conceal or hide their behaviors [19].

There are view other related detection techniques such as Florencio and Herley [22] designed and proposed to use a effectively shared-secret proxy to go through passwords on computers that have suspected keyloggers installed.

A. Proactive detection techniques

Methods that can be used to protect known keyloggers are similar other malware detection particularly rootkits. To prevent potential keyloggers, it is good practice to apply the following steps [14]:

Since the main purpose of keyloggers is to retrieve confidential data, so using Two-step authentication or one-time passwords is required.

Block access suspicious sites by using Web filtering.

The main target of keylogger is the Keyboard. Thus, use a virtual keyboard instead of standard keyboard.

TABLE I
A SUMMARY OF CURRENT DETECTION TECHNIQUES

No	Paper Name and Author	Keylogger Detection Technique	Solution and Results	Remarks
1	Stefano at el. (2011). KLIMAX: Profiling Memory Write Patterns to Detect Keystroke-Harvesting Malware	Behavior based detection technique using KLIMAX: Kernel- Level Infrastructure for Memory and execution profiling.	Allow for no false negatives when the keylogging behavior is triggered within the window of observation and can also be used in large-scale malware analysis and classification.	Malware evasion techniques that conceal or delay information leakage are not concern for this detection technique.
2	Anith at el. (2011). Detecting keyloggers based on traffic analysis with periodic Behavior	• Client level detection technique. • Host and checkpoint levels techniques using signatures.	TAKD algorithm. Integration into routing devices such as a gateway, router, IDS, firewall	There is no quantitative analysis for irregular time intervals
3	J. Fu at el. (2010). Detecting Software Keyloggers with Dendritic Cell Algorithm.	Dendritic Cell Algorithm implement a hook program to monitor API calls generated by running processes In the host and five signals to define the state of the system.	This method can differentiate the running keylogger process from the normal processes with a high detection rate and a low false alarm rate.	Behaviour of keyloggers is the same as applications that hook the system message execution. All legitimate applications that hook the system would be detected as malicious.
4	Le at el. (2008). Detecting Kernel Level Keyloggers Through Dynamic Taint Analysis	• host-based intrusion detection • dynamic taint analysis to detect kernel level keyloggers	Framework can detect kernel level keylogging that intercept keyboard driver, particularly tty buffer and identify their root causes.	Integration with VMscope techniques is necessary
5	Aslam at el. (2004) Anti-Hook Shield against the Software Key Loggers.	Although, hook is the core of keyloggers. So this paper presents anti-hook technique to scan all processes and static executables and DLLs.	Can easily found all suspicious processes or files, whether it is visible or invisible at any level of the application	This technique requires a lot of computation and the false positive rate is very high

Update and maintain a regularly anti-malware solution.

Use keylogger detection software to monitor sensitive systems (e.g., SnoopFree Privacy Shield) and down systems when not in use [33].

Do not allow insider user to gain administrator access.

Install endpoint software policy controls (e.g., WebSense CPM);

Block illegal sessions between endpoints and outside sites.

The best method which provides suitable detection technique against both keylogging software and hardware is using a virtual keyboard. A virtual keyboard is a program built in Windows operating system that displays intangible keyboard on the screen. Mouse is used to press keys on the virtual screen keyboard.

Fig. 6: virtual keyboard of the Windows [14]

However, on-screen keyboards are not reliable detection technique method of outsmarting keyloggers. Typed Keystrokes and the mouse clicking through an on-screen keyboard can easily be interrupted by a malicious program. In order to prevent against smarting keyloggers, specially designed on-screen keyboards is recommended to ensure that information transmitted through the on-screen keyboard cannot be retrieved. Some virtual keyboards also have a feature that allows a user to enter a character by hovering mouse cursor over a letter for a few seconds. Thus the user can enter the password without even clicking the mouse button [29].

VII. CONCLUSION AND FUTURE RESEARCH

Keyloggers are powerful tools that cannot threat the system itself, but the user's confidential data such as user name, password, pin and card bank. Although some keylogger are applied as legitimate way, but many keyloggers are used illegally by the creator. This paper has surveyed most common keylogger types and methods used to hide themselves while subversive user's machine. We've also examined the current state of keyloggers and how they can spread. Finally, we analyzed the existing detection techniques, and outlined some prevention techniques.

Detecting keylogging technology within the organization is no different than controlling other malicious cod or threats, requiring common awareness, regularly monitoring and a layered defense. The main point is to be aware that they existing threat, recognize how they're used, and suitable ways

to detect them. Therefore, keylogger detection and countermeasure must to be part of the organization's incident response plan. In Future work might include enhancing TAKD algorithm [7], [40] which is based on traffic analysis such periodic behavior that has fixed time interval for the communication between source and destination. For example, every 15 minutes, determined by the attacker. Therefore, the result of this detection algorithm may be enhanced to achieve quantitative analysis for irregular time intervals.

REFERENCES

[1] C.-C. C. Chieh-Ning Lien, "Keylogger Defender," UCLA Computer Science Department, Los Angeles, CA 90095, USA, 2005.

[2] C. a. Solms, "Implementing Rootkits to address operating system vulnerabilities," presented at the. Academy of computer science and softwar engineering, Universtiy of Johannesburg.Johannesburg, South Africa., 2011.

[3] 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.

[4] E. S. L. Martignoni, M. Fredrikson, S. Jha, and J. C. Mitchell, "A layered architecture for detecting malicious behaviors,".Heidelberg.2008

[5] C. Y. D. Le, T. Smart, and H. Wang, , "Detecting kernel level keyloggers through dynamic taint analysis," College of William & Mary, Department of Computer Science, illiamsburg,, 2008.

[6] C. G. S.Ortani, and Crispo."Bait your Hook: A novel Detection technique for keylogger". University of Trento, Via Sommarive.Trento, Italy.2010.

[7] S. S. a. Anith."Detecting keylogger based on traffic analysis with periodic behavior"PSG College of Technology, Coimbatore, India.2011

[8] C. a. Rajendra."Keylogger in Cybersecurtiy Education". Rechester Institute of Technology,Rechester,New York,USA.

[9] T. Olzak." Keystroke Logging Keylogging" Erudio Security, LLC. 2008.

[10] S. S. A. G. CANBEK. (2009) Keylogger Increasing Threats to Computer Security and Privacy. IEEE TECHNOLOGY AND SOCIETY MAGAZINE.

[11] "List of keyloggers parasites," Dedicated 2Spyware, http://www.2- pyware.com/keyloggers- removal; accessed Sept. 2007.

[12] O. Zaitsev." Skeleton keys: the purpose and applications of keyloggers"2009

[13] A. R. P. Kalpa Vishnani, and Radhesh Mohandas, "An In-Depth Analysis of the Epitome of Online Stealth: Keyloggers; and Their Countermeasures," Dept. of Computer Science & Engg, National Institute of Technology Karnataka, Surathkal, Srinivasnagar, Mangalore - 575025, India, 2005.

[14] "How they work and how to detect them Part.", http://www.securelist.com; accessed Sept. 2009

[15] Y. A.H., U. Aickelin, "Detecting Bots Based on Keylogging Activities," Department of Computer Science and Information Technology, University of Nottingham, Nottingham, UK, 2008.

[16] S. Shetty." Operating system market share", 2007.

[17] J. Rutkowska." System virginity verifier defining the roadmap for malware detection on windows system". http://www.invisiblethings. rg/papers/hitb05_virginity_verifier.ppt.

[18] D. S. H. Yin, E.Manuel, C. Kruegel, and E. Kirda. Panorama. "Capturing system-wide information flow for malware detection and analysis". In Proceedings of the 14th ACM Conferences on Computer and Communication Security (CCS'07), 2007.

[19] Freeware antirootkits. http://wiki.castlecops. com/Lists_of_freeware_antirootkit.

[20] N. I. a. P.Mathur."A Survey of Malware Detection Techniques".Department of Computer Science Purdue University, West Lafayette, IN 47907.2007.

[21] G. McGraw and G. Morrisett. Attacking malicious code: A report to the infosec research council. IEEE Software, 17(5):33–44, 2000.

[22] D. F. a. C. H. Klassp, "Entering passwords on a spyware infected machine using a sharedsecret proxy," Washington, DC, USA, 2006.

[23] F. Hasani. 2011. The Secrets in the Keylogger. http://www.itknowledge24.com/the_secrets_in_keyloggers.pdf

[24] J. Jensen, "Detection of Hidden Software Functionality," Master of Science in Communication Technology, Norwegian University of Science and Technology Department of Telematics, 2007.

[25] P. P. Heng Yin1, 3, Steve Hanna2, and Dawn Song2, "HookScout: Proactive Binary-Centric Hook Detection," Syracuse University, Syracuse, 2010.

[26] A. Davis, "Hardware keylogger Detection," Smith Square London, 2007.

[27] T. W. JiaJing Li, Wei Zou, "A Static Method for Detection of Information Theft Malware," presented at the Second International Symposium on Electronic Commerce and Security, Peking University, Beijing 100871, China, 2009.

[28] Y. L. Jun Fu, Chengyu Tan,Xiaofei Xiong, "Detecting Software Keyloggers with Dendritic Cell Algorithm," presented at the 2010 International Conference on Communications and Mobile Computing, Wuhan University, 2010.

[29] S. Shetty. 2006," Introduction to Spyware Keyloggers". http://www.securityfocus.com/print/infocus/1829

[30] Doja, M.N.; Kumar, N.; , "Image Authentication Schemes against Key-Logger Spyware," Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD '08. Ninth ACIS International Conference on , vol., no., pp.574-579, 6-8 Aug. 2008

[31] Zhuang, L, Zhou, F. & Tygar, J.D. (2005). "Keyboard acoustic emanations Revisited". Retrieved 2011 from http://www.cs.berkeley.edu/~zf/papers/keyboard-ccs05.pdf

[32] Wilson, T. V. & Tyson, J. (2008)." How computer keyboards work". HowStuffWorks.com. Retrieved 2011 from. http://computer.howstuffworks.com/keyboard.htm.

[33] G. Canbek, "Analysis, design and implementation of keyloggers and anti-keyloggers," Gazi University, Institute of Science And Technology, M.Sc. thesis (in Turkish), Sept. 2005, pp. 103.

[34] D. Wampler, James H. Graham. "A Normality based method for detecting kernel rootkits". ACM SIGOPS Operating Systems Review, 2008, 42(3)

[35] K. Kasslin." Kernel malware: The attack From within". In The 9th Annual AVAR International Conference, 2008.

[36] A. Baliga, L. Iftode and X. Chen, "Automated containment of rootkits Attacks, " Computers & Security, vol. 27, Issues 7-8, pp. 323-334, 2008.

[37] B. Whitty, "The ethics of key loggers," Article on Technibble.com, June 2007 (accessed December 8, 2011), http://www.technibble.com/the-ethics-of-key-loggers/.

[38] ThinkGeek.com, "Spy keylogger," 2010 (accessed December 15, 2011), http://www.thinkgeek.com/gadgets/security/c49f/.

[39] Online fi nancial fraud and identity theft 2007," Cyveillance, 2007; http://www.cyveillance.com/web/news/press_rel/2007/2007- 03-27.asp, accessed October. 2011.

[40] D. Stefan, C. Wu, D. Yao, and G. Xu. " Cryptographic provenance verification For the integrity of keystrokes and Outbound network traffic". In Proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS), June 2010.