Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 3, March 2013, pg.106 – 111

RESEARCH ARTICLE

System Monitoring and Security Using Keylogger

Preeti Tuli [1], Priyanka Sahu[2]
[1]Reader, Department Of Computer Science Dimat, CSVTU, Raipur, Chhattisgarh, India
preetituli@gmail.com
[2]M tech scholar, Department Of Computer Science Dimat, CSVTU, Raipur, Chhattisgarh, India
pri.sahu18@yahoo.com

Abstract— It is likely that about one out of many large companies systematically monitors the computer, internet, or email use of its users employees. There are over hundred's different products available today that will let organizations see what their users do at work on their "personal" computers, in their email, and on the internet. But what do such numbers really mean? What does company monitoring of user/employee email, internet, and computer usage actually look like? What sorts of things can an organization/company see users do at their computers, and what sorts of computer activities are currently invisible to workplace monitoring? This admittedly document attempts to propose, as concretely as possible what "Informational Flow" on internet and computer usage looks like: its extent, the key concepts involved, and the forces driving its adoption. The keylogging program logs all keystrokes (aka Keystroke Logging) along with the name of the application in which the keystrokes were entered. Using keylogger we prevent the miscellaneous use of system. Using this we capture all information in text and image form.

Key Terms: - Email monitoring, Internet monitoring, Computer monitoring, Chats/IM is monitoring, Network monitoring, Document monitoring, Web site monitoring, Productivity monitoring, keylogging.

I. Introduction

A study found that 20 million users in the US, or about 1/3 of the online workforce (that is, those users with regular internet access at work), have their web surfing or e-mail monitored. Globally, the figure is about 28 million, or about 1/4 of the global online workforce [1].

Why capture?

- Monitor work flow: 29.2%
- Investigate theft: 29.2%
- Investigate espionage: 21.5%
- Review performance: 9.2%
- Prevent harassment: 6.2%
- Seek missing data: 3.1%
- Seek illegal software: 3.1%
- Prevent personal use: 3.1%

This monitored include unneeded services, unnecessary open ports, multiple system/security events, drivers, shared folders, programs that load during startup and network configurations . Monitoring is an important factor to maintain stability for the network. Information security focuses on ensuring, confidentiality, integrity and availability.

The goal of this paper is to give an idea about some of the benefits that anyone can get from the complete monitoring of the system network. Keylogging programs, commonly known as keyloggers, are a type of malware that maliciously track user input from the keyboard in an attempt to retrieve personal and private information. Keystroke logging, also known as key logging, is the capture of typed characters/number [2]. The data captured can include document content, passwords, user ID's, and other potentially sensitive bits of information. The program logs all keystrokes (aka Keystroke Logging) along with the name of the application in which the keystrokes were entered**.** It also notes the window captions and all URLs visited with a web browser. This allows you to review all the text written by your employ/user, whether it was created with a text editor, e-mail client or an on-line text control on a web page. You can view all the pages visited by your employ/user and the passwords for all their on-line accounts. For easier monitoring, you can also turn on automatic screenshot capture.

The rest of the paper is organized as follows. Overview of keylogging and how keylogging work is explain in section II. Logging and monitoring and computer security explain in section III. Design and implementation of keylogging explain in section IV. Proposed algorithms are presented in section V. Benefit and list of accountability and where it is need are explained in section VI. Concluding remarks are given in section VII.

II. Overview of Key Logging

The keyboard is the primary aim for key loggers to retrieve user input from because it is the most common user interface with a computer. Although both hardware and software key loggers exist, software key loggers are the dominant form and thus are main point in this paper. Software keylogger are most inexpensive easily used program. This keyloggers need to be adapted to each target operating system to ensure I/O is handled appropriately. System differences thus unavoidably lead to operating system specific mechanisms implemented in software keyloggers: use of the keyboard state table, system routine hooks, and kernel-mode layered drivers [3]. Additional detail about techniques used in the development, distribution, execution and detection of user- and kernel-mode keyloggers, particularly on Microsoft Windows operating system. A basic concept behind keyloggers and similar malware is their pattern of attack. Most of malware infections follow a fairly standard attack pattern that involves the sequential order of development, distribution and infection, and execution stages. Distribution and execution can both be implemented as a component of the malware and therefore are a contributing factor in its design and development. The keylogging malware to begin executing and can occur in several different ways depending on the implementation and context of the keylogger. However, most realistic keyloggers share two operations: (a) hooking into user input flow to receive keystrokes and (b) transporting the data to a remote location.

HOW KEY LOGGERS WORK

Keyloggers are hardware or software tools that capture characters/number sent from the keyboard to an attached computer.

- Quality assurance testers analysing sources of system errors;
- Developers and analysts studying user interaction with systems[4];
- Employee monitoring; and
- Law enforcement or private investigators looking for evidence of an on-going crime or Inappropriate behavior.

Other detection methods include:

- Scan local drives for log.txt or other log file names associated with known keyloggers;
- Implement solutions that detect unauthorized file transfers via FTP or other protocols;
- Scan content sent via email or other authorized means looking for sensitive information;
- Detect encrypted files transmitted to questionable destinations.

III. LOGGING AND MONITORING

From monitoring you can detect hacking attempts, tracking, virus or worm infections and propagation, configuration problems, hardware problems and many others. Monitoring is most important factor to maintain stability for the network. Information security focuses on ensuring confidentiality, integrity and availability, accountability. From network monitoring you can detect attempts to access to exclude information or resources such as unauthorized access, which in turn ensure confidentiality [5]. You can detect attempts to change or alter information such as file modification, which ensure integrity. And you can detect any kind of problems that can affect the availability of the information such as DOS or DDOS attack [6]. The main goal of this paper is to give an idea about some of the benefits that anyone can get from the complete monitoring of the network. Logging can give detailed information about any access or change for any of the network resources.

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network [7]. Logs were used primarily for troubleshooting problems, but logs now serve many functions within most organizations, such as optimizing system and network performance, recording the actions of users, and providing data useful for investigating malicious activity. The widespread deployment of networked servers, workstations, and other computing devices, and the ever-increasing number of threats against networks and systems, the number, volume, and variety of computer security logs has increased greatly. This has created the need for computer security log management, which is the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Logging can be a security administrator's best friend. It's like an administrative partner that is always at work, never complains, never gets tired, and is always on top of things. If properly instructed, this partner can provide the time and place every event that has occurred in your network or system [8].

The major log management operational processes typically include configuring log sources, performing, log analysis, initiating responses to identified events, and managing long-term storage. Administrators have other responsibilities as well, such as the following:

- Monitoring the logging status of all log sources.
- Monitoring log rotation and archival processes.
- Checking for upgrades and patches to logging software, and acquiring, testing, and deploying them.
- Ensuring that each logging host's clock is synched to a common time source.
- Reconfiguring logging as needed based on policy changes, technology changes, and other factors.
- Documenting and reporting anomalies in log settings, configurations, and processes.

THE BASICS OF COMPUTER SECURITY LOGS

Logs can contain a wide variety of information on the events occurring within systems and networks [9]. This section describes the following categories of logs of particular interest:

- Security software logs primarily contain computer security-related information.
- Operating system logs and application logs typically contain a variety of information, including computer security-related data.

This paper focuses on the types of logs that are most often deemed to be important by organizations/company in terms of computer security. Organizations should consider the value of each potential source of computer security log data when designing and implementing a log management infrastructure.

IV. DESIGN AND IMPLEMENTATION

Key logger design and implementation strategies are based upon several factors: the infecting medium, the type of target machine, the lifetime of the key logger, and the level of stealth and footprint left on the machine while active. Infection mechanisms depend on the form of the key logger.

A software keylogger target the user-mode of an operating system is injected remotely and a hardware keylogger via physical device placement. Software keyloggers require a well-crafted infection mechanism to ensure proper installation, for example, a web browser exploit. Most keyloggers share a common execution technique known as hooking, though each keylogger will implement it in a different way depending on the context for which the keylogger is needed [10]. The basic goal of hooking is to intercept the normal control flow and alter information returned by a target system routine. Hooks can be implemented in any level of the operating system for most functions, which makes them a general technique to be utilized by keylogger developers. High-level key loggers executing in the user-mode of an operating system are implemented using a variation of user mode hooks [11]. Low-level kernel-mode key loggers are typically implemented as root ware, a combination of both root kits and spyware that employ another variation of hooking.

ENHANCEMENT OF KEYLOGGING: CLIENT-SERVER-BASED INTERCEPTION

All available user-monitoring products are essentially programs that report on (and in some cases constrain) how you use other programs. Having installed an user-monitoring program, an organization can -- depending on the type of program -- see how much time users (individually and/or in aggregate) spend playing Solitaire, or what web sites they visit, or even read email messages that they typed but then deleted and didn't send. The organization may also be able to prevent users from visiting certain web sites, or from sending or receiving certain emails [12]. One way to understand these products is to consider where they are installed. There are basically two types: server-based monitors, designed to be installed on the organization's network; and client-based monitors, designed to be installed right on the personal computer (PC) used by the user[13]. First, we'll look at the network (server), then at the PC (client). To see the difference, let's imagine a typical user, whiling away the time playing Solitaire. Wes Cherry, the Microsoft programmer who wrote the Solitaire game included with Windows, has noted that he has single-handedly "wasted more corporate time than any other developer" (though organizations might recall that many users first learned to use a mouse by playing Solitaire). The question is, Can the corporation tell (short of looking over his or her shoulder) whether an user is playing Solitaire? The answer is yes, they can see everything.

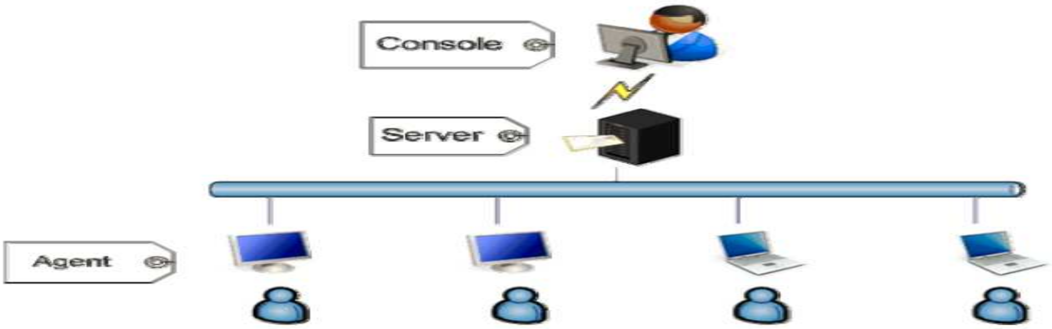

Fig.1 Client -Server

V. Proposed Algorithm

- **Signature based keylogger.** These are applications that typically identify a keylogger based on the files or DLLs that it installs, and the registry entries that it makes. Although it successfully identifies known keyloggers, it fails to identify a keylogger whose signature is not stored in its database. Some anti-spyware applications use this approach, with varying degrees of success. Most of the anti-virus software's detect Keylogger application based on this approach.

- **Hook based keyloggers.** A hook process in Windows uses the function SetWindowsHookEx (), the same functions that hook based keyloggers use. This is used to monitor the system for certain types of events, for instance a keypress/mouse-click — however, hook based anti-keyloggers block this passing of control from one hook procedure to another. This results in the keylogging software generating no logs at all of the keystroke capture. Although hook based anti-keyloggers are better than signature based anti-keyloggers, note that they still are incapable of stopping kernel-based keyloggers.

The mechanism used to intercept events using specific functions (e.g. sending Windows messages, data input via the mouse or keyboard) in Microsoft Windows is called 'hooking'. This function can react to an event and, in certain cases, modify or delete events. Functions which receive notification of events are called filter functions; they differ from each other by which events they can intercept. In order for Windows to call a filter function, the function must be bound to a hook (for instance, to a keyboard hook). Binding one or more filter functions to a hook is called "setting a hook". The system also supports separate chains for each type of hook. A hook chain is a list of pointers to filter functions (specific callback functions determined by the application.). When an event linked to a particular type of hook takes place, the system consecutively sends the message for each type of filter function to the hook chain. The actions which filter functions may perform depend on the type of hook: some function can only track the appearance of an event, while others may modify message parameters or initiate message processing, by preventing the next filter function in the hook chain from being called, or the message processing function for the relevant window from being called.

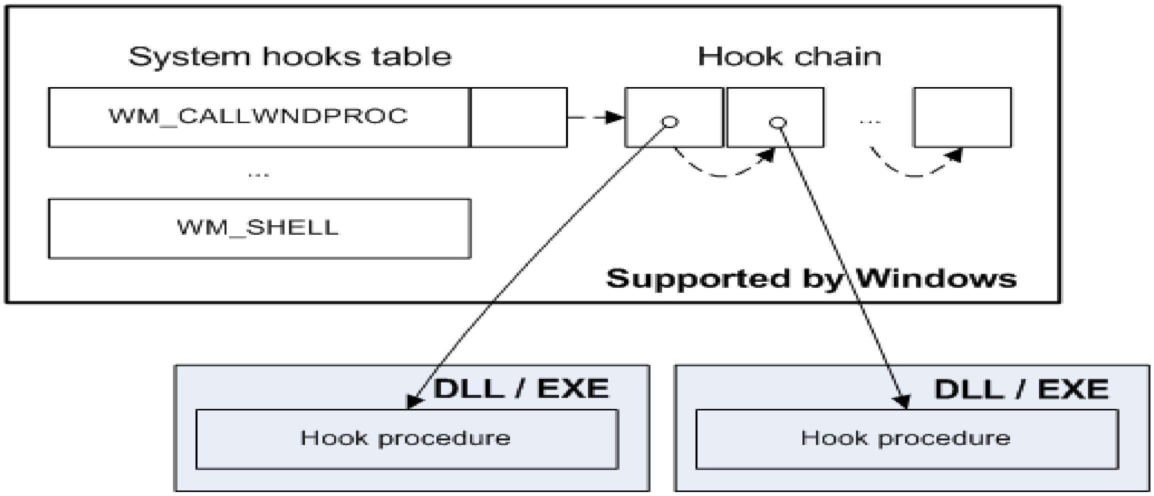

Fig.2 Filter function chain in Windows

VI. BENEFITS AND FEATURES OF OUR APPROACH

- As storage is now cheaper and processors faster, "recording everything" becomes a realistic possibility, which we will try to accomplish.
- A "universal inbox" (all company documents are delivered as email or email attachments) would make it possible to record all company workflow.
- "Convergence" of all office devices may provide a single "integrated" site for monitoring.

A LIST OF ACCOUNTABILITY FEATURES:

- Key Strokes Typed at any place
- Programs opened
- Title of documents, videos, music, etc opened
- Websites visited
- Online duration & uptime
- PC-wise and user wise analysis
- Notification of harmful PCs on the network
- Control of Network Usage
- Prevention of Information Leak From Organization

WHO MAY NEED THIS?

- Hospitals
- Banks
- IT Organizations
- Institutions & Universities
- Call Centers
- Internet Business Organizations
- Government Bodies

VII. CONCLUSION

Software that can not only monitor every keystroke and action performed at a PC but also be used as legally binding evidence of wrong-doing has been unveiled. Worries about cyber-crime and sabotage have prompted many employers to consider monitoring employees. They have joined forces to create a system which can monitor computer activity, store it and retrieve disputed files within minutes… "People need to recognize that you are using a PC as a representative of a company and that employers have a legal requirement to store data.

Website monitoring service can check HTTP pages, HTTPS, SNMP, FTP, SMTP, POP3, IMAP, DNS, SSH, TELNET, SSL, TCP, ping and a range of other ports with great variety of check intervals from every 4 hours to every one minute.

Typically, most network monitoring services test your server anywhere between once-per hour to once-per-minute. Features:

- Protect intellectual property and business secrets
- Prevent and stop sabotage and data theft
- Prevent Internet/email abuse
- Reduce workplace slackers
- Improve efficiency and productivity

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(accessedMay 8, 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, March 2002, 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/.