International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(03), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

CYBERCRIME SECURITY IMPLEMENTATION USING HARDWARE BASED ANTI –KEYLOGGER

Dr.D.B.V Jagannadham[1], Mr.D.Ajit Varma[2]

[1]professor, [2]research Scholar

Department Of Electronics And Communication Engineering,

Gayatri Vidya Parishad College Of Engineering, Kommadhi, Visakhapatna(India)

ABSTRACT

cyber crime has became a major threat to prudity of data owned and maintained by an organization or a company etc., one of the easiest way to collect the information is using key-loggers. The key-logger recognizes the key-strokes either by means of software key-logger or a hardware key-logger. Software key loggers can be detected using some anti key-logger software. But in some cases hardware key-loggers can not be detected using a software program, as it is connected externally to the cpu and does not involve in cpu activities. These key-loggers may cause great threat if not detected timely.

This paper presents how to detect an key-logger using an external anti key-logging device. It detects the hardware key-logger and alerts the user about the threat.

I. INTRODUCTION

cyber crime has made a tremendous rise in the past two decades. The internet is one of the fastest growing area in the technical interface. Today information and communication and trend towards digitalization is being grown widely[1][3]. The demand for internet and computers has led to integration of computer technology into products that have usually worked without it. Such as cars, buildings etc.,

In such circumstances, cyber crime has been growing faster and faster such as threat of stealing information and intruding data etc.,

Some of the common methods of intrusion of data are:Traffic flooding Asymmetric Routing Buffer overflow Attacks Key logging Trojans etc;

1.1 Traffic Flooding:-[4 A Novel method of network intrusion targeted simple network intrusion detection systems by creating heavy traffic loads created for the system. resulting environment, of chaotic and congested network. For a Fail open condition attackers may sometimes get an undetected trigger or undetected intrusion.

1.2 Asymmetry Routing:- [4]In this approach the attacker tries to create more then one route to targeted network device The main idea is to evade network intrusion sensors and certain network segments to evade detection by

bypassing by having efficient portion of the offending packets. In this methodology the non setup networks for asymmetric routing will not be effected which is the main disadvantage.

1.3 Buffer overflow attacks:-[4]In this method of attacking, the specific sections of computer's memory's normal data will be replaced with a special set of commands which will be used as a part of attacking later. In almost all the cases the motto is to intimate a Denial of Service situation (DOS situation) or channel to be setup by the attacker to gain remote access on network. Creating Like this type of attacks is very difficult as buffer sizes designed by the attacker is relatively small, or to identify executable code or lengthy URL strings before it can be written on buffer by installing boundary checking logic program.

1.4Trojans:-[4] These programs present themselves as trusted and do not replicate like a virus or a worm. Instead, they instigate Denial of service attacks, erase stored data, or open channels to permit system control by outside attackers. Trojans can be introduced into a network from unsuspected online archives and file repositories, most particularly including peer-to-peer file exchanges.

1.5 packet analyzer:-

[4]Packet analyzer is a computer software or a piece of hardware which intercepts or logs network traffic by sniffing the data.These were captured by a sniffer leading to intrusion of data. This may effect the user in loss of information.One of the easiest way of intruding data is identifying key presses. These key presses can be easily recorded using a small device or software called key-logger. As it has became a boon to many it companies to identify their employees work, but many of them are at risk of information threat as their movements are being noted and observed by a malicious hacker.

The risk of information can be ended using a counter module called 'Anti-keylogger'.

II.KEY –

logging (or) keystroke capturing: key logging (or) keystroke capturing is the action of recording the key struck on the keyboard, which makes the user using the keyboard unaware of another person who is observing (or) monitoring user's actions. Through keylogging process a person can get complete account of another person's activity.

These key loggers may affect many areas like public computers, financial institutions, IT companies etc., These may even steal information from the computers of IT companies providing confidential information and details.

III.KEY-LOGGER

A program or software which enables a person to initiate the process of recording keyboard or key strokes of a user is a keylogger. It generally is installed on a system without the knowledgeof the user.

For example, REFOG, DanuSoft keyloggers are easily available for free online and are very commonly used.

3.1SuspectedProcesses:

The processes which run in the background or the

foreground and are detected by an Anti-Keylogger to be of potential threat to a system are referred to as spected process.

They may or may not be actually harmful but are recognized by the anti-malware softwares as dangerous. For example, any keylogger which runs in the background without the knowledge of the user would be able to extract all confidential information and thus, is bound to be listed in the category of suspected process.

Key loggers are of two types:

1. Hardware -Based
2. Software - Based

For example Danu soft, Spyrix, REFOG are some of the commonly used software keyloggers.

3.1 Hardware based key logger: Hardware based key logger do not depend on any program or software as they are connected in the components section of a computer system.

3.1.1 Firmware based key logger:

The Keyboard events and the processed modified records can be handled at BIOS level firmware. for this machine requires a root level and physical access and the BIOS needs a software to be created to run the specific hardware.

3.1.2 Key board Hardware:-

The most commonly used input device is a keyboard. Signal is generated for each specific key that have been pressed by the user. This signal is understandable by the computer. Key boards can be wired or can be operated in wireless manner by means of Bluetooth. An encoder is present in every key board which generates a code for every key pressed this code is uniquely defined only for that key. The alphanumeric standard keys beside additions keys such as navigation, function keys and cursor key are included.

This Encoder is a special type of micro processor fixed in the keyboard which detects pressed and released keys. This Micro processor uniquely generates a signal to identify each key that is pressed or released. Type writer keys were arranged in a alphabetical order until the late 19th century. For reducing speed or rapid key pressing raised due to alphabetical order Christopher lotham Sholes invented a new type of type writing machine in 1872. which was named as qwerty key board featuring the first six alphabets in the top left of the keyboard. this invention made the fast typists slow down rapidly resulting in the increase of lifetime of the keyboard and increases less jam mage of the machine processor. this keyboard was later on adapted by almost all the computers. To increase the speed of typing rather than qwerty key board professor dvorak has introduced a new type of keyboard to improve the speed of typing by 35%, but in real it has increased the speed of typing by 70%.
As it is not installed on the target computer, normally the program may not interfere with the hardware key logger. Hence it
cannot be detected by any program
installed by any operating system on the computer. By using the wireless communication standards these devices have ability to control and monitor by means of wireless manner.
Somewhere in between computer keyboard and computer hardware key logger circuit is attached typically in between the connector and cable keyboard connector. In the case of laptops plugging PCI card is done into expansion slot. More minure instruments can be installed in the laptop which cannot be able to identify by the users.
3.3.2Software based key-logger:-
[1]Some specific computer programs are used to work on targeted computers. Most of the IT organizations use key loggers to troubleshoot the technical problems raised in the computer. In public domain places malicious individuals use key loggers to steal passwords and confidential information such as credit card information etc., However, malicious individuals can use key loggers in public computers to steal passwords and credit card information.
Classification of types of software key loggers:

1) Kernel Based

2) APT Based

3) Form grabbing Based

4) Memory injection Based

5) Packet Analyzing Based

3.2.1Kernel-based:This type of program is difficult

to write and combat as it has to obtain root access to hide itself in the operating system. This method intercepts the keystrokes passing through the kernel. Most of the key loggers resides at the kernel level. It is difficult to identify by the system As they are implanted as the root kits which gain unauthorized access to the hardware. so that this software gain access as a hardware driver such as keyboard, mouse etc., which make them most powerful.

3.2.2 API-based: hooking API's inside a running application is the main job of this type of key logger. This key logger acts as a normal application rather than a malware and registers all the keystroke events. While An User press or release the key the key logger receives information in every moment and indicates it. This make the key logger record the key stroke. To poll the state of keyboard events and subscribe to keyboard events Windows API's are used. A recent example was polls the Bios for pre boot authentication PINs that have not removed from memory.

3.2.3 Form grabbing based: In a web browsing centres the grabbing based key loggers are used to steal the web logging data and forms submitted through web. The grabbing of data occurs whenever the user fills the form and submitted just before into the internet.

3.2.4 Memory injection based:Memory injection table based key loggers are mainly used in injecting their logging function by changing their memory tables that were associated with the logging function. This can be done by injecting or patching the memory tables directly into memory. This
method is mainly used by intrudes to bypass
Windows UAC .Other operating systems have protection mechanisms that a key logger has developed.

3.2.5 Packet analyzers: In HTTP packet events the traffic associated with the HTTP can capture the network traffic to retrieve the non- encrypted data such as passwords by collecting thousands of packets associated with HTTP and they are analyzed. TO gain more security from thes packet capturing method later HTTPS was invented.

3.2.6 Remote access software keyloggers: Key loggers normally located in some distance and acess locally recorded data remotely with out in touch with thecomputer.

3.3Features:-

Not only capturing keystroke presses, Some of the key loggers may gain access of capturing memory other than key presses and etc., Few key loggers include following features:-

3.3.1 Clipboard logging: In this method the information copied on the clipboard is captured by the key logger Program.

Screen logging:- By using the graphic based approach screen shots are taken by the key loggers and the

information is grabbed from it. The software key loggers having screen logging abilities ,may capture screenshot either of the whole screen or only around the mouse cursor based on user activities.These type of key loggers are in such a situation where web based keyboards are used such as software used in banks army forces etc.,

3.3.2 Programmatically capturing the text in a control:- Text value in some controls are requested by the windows API's which are used to store behind the masks usually 'ASTERISKS'. These API's record every program opened including capturing the screenshot of every website visited including search engine queries, instant messenger conversations etc.,

IV.ANTI-KEY LOGGERS

In comparison to the Antivirus and Anti malware, an anti key logger can be introduced which is specifically used to detect the key logger. This software detects key stroke logging program.

4.1Typesof anti-key logger:- There are many types of anti key logger only to detect software based key loggers. Some of them are

4.1.1Signature based analysis:-

[2]This type of software consists of list of all known keyloggers. Each time you scan system it looks for any file existing in hard disk drive and alerts user. The main drawback is it can only detect the key loggers that are present in it's own data.

4.1.2Heuristic analysis:-[2] This type of software doesn't depend on signature basis. It analyzes the methods of work of all programs in pc and blocks work of all key loggers. This is better than the signature based analysis.

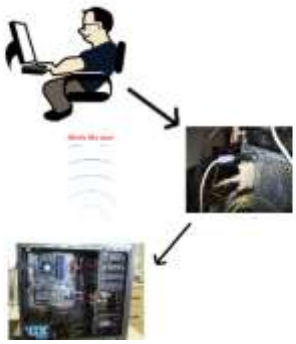
One of the drawbacks is, It may block other processes also

V. HARDWARE BASED ANTI- KEY LOGGER

In our work we design a device which is used to detect if a potential key logger (or) any malicious device is present in the computer which would be unknown to the user.

The device is set inside the cpu and keyboard and warns the user if any malicious activity is observed.

Our work 'HARDWARE BASED ANTI -KEYLOGGER' detects the suspicious potential threat to the system which may have led to identity thefts (or) thefts of crucial information data and keyloggers. This may be useful to eradicate (or) to decrease crimes related to cyber security.



By default this hardware is set up in the cpu and let it run. This is placed in between keyboard and processer when ever key logger is inserted the delay in receiving the information from keyboard may be increased. The hardware device detects the delay and signals the user that some suspected activity is being processed and alerts him so that threat related to information theft can be decreased.

VI.CONCLUSION

This paper mainly emphasize on the network security and some major issues that can affect network. Through this paper, we present our work where we create an hardware based anti keylogger specifically designed for the detection of any keystroke capturing device, if so to alert the user about the intrusion/threat involved.

Acknowledgements:- Authors are very thankful to the secretary of gvp college of engineering(A), Madhurawada, Visakhapatnam, for giving the opportunity to utilize the sources available to get related information and to publish in a reputed journal.

REFERENCES

[1] Siddhartha Ghansela, -Network Security: Attacks, Tools and Techniques. International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, page no.48-56. June 2013.

[2] Preeti Tuli, -System Monitoring and Security Using Keylogger‖ International Journal Of ComputerScience and Mobile Computing, Volume 2, Issue. 3, pg.106 – 111. March 2013,

[3]Mahak Arora- cyber crime combating using anti keylogger. Et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3, Issue 2, pp. 1-5 June 2016,

[4]Robertmoskovitz RSA Conferencee network Intrusion: Methods of Attack

Ajit varma.Dantuluri is an UG student of Electronics and Communication Engineering Dept. Gayatri Vidya Parishad College of Engineering(Autonomous), Kommadhi, Visakhapatnam- 530048.
His areas of research interest are cryptography and cyber security

Dr.D.B.V.Jagannadham is a professor in Dept. of Electronics and Communication Engineering Gayatri Vidya Parishad College of Engineering (Autonomous), Kommadhi, Visakhapatnam. He has 20 years of teaching experience and presented and published various papers in various journals(IEEE Transactions) and international conferences. His areas of research interest are non-linear and non-stationary signal processing and cyber security.