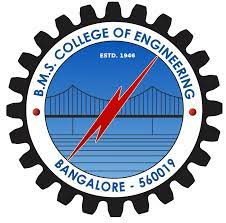
**BMS COLLEGE OF ENGINEERING**

**(Autonomous College under VTU)**

**Bull Temple Road, Basavanagudi, Bangalore – 560019**

****

A report on

***Seminar Based on Summer/Winter Internship***

***"Analysis and Implementation of  
Decipherment of Key Logger”***

Submitted in partial fulfillment of the requirements for the award of degree

**BACHELOR OF ENGINEERING**

**IN**

**INFORMATION SCIENCE AND ENGINEERING**

**Submitted by**

Hiral Honnorali (1BM20IS406)  
G Pramod Sai (1BM18IS070)

**Under the guidance of**

Nalina V  
Assistant Professor

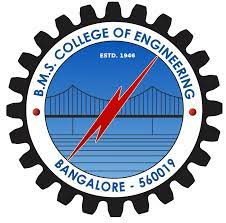
**Department of Information Science and Engineering**

**2020-21**

**BMS COLLEGE OF ENGINEERING**

**(Autonomous College under VTU)**

**Bull Temple Road, Basavanagudi, Bangalore – 560019**

****

**C E R T I F I C A T E**

Certified that the Technical Seminar has been successfully presented at **BMS College of Engineering** by bearing USN:**1BM20IS406 AND 1BM18IS070** in partial fulfillment of the requirements for the IV Semester degree in **Bachelor of Engineering in Information Science & Engineering** of **Visvesvaraya Technological University, Belgaum** as a part of for the **course Seminar Based on Summer/Winter Internship Course Code -19IS4SRSMI** during academic year 2020-2021

**Faculty Name : Nalina V**

**Designation : Assistant Professor**

**Signature :**

**Abstract**

Software keyloggers are very famous tools which are often used to harvest confidential information. One of the main reasons for this rapid growth of keyloggers is the possibility for unprivileged programs running in user space to eavesdrop and monitor all the keystrokes typed by the users of a system. A keylogger is a program that records all key sticks entered on the keyboard, in another word keyloggers are the sort of the spywares that take the information of the clients by following their keyboards. Detecting the key loggers is a troublesome undertaking to perform because generally they hide their presence using technology like rootkit so they don’t get detected from antivirus and other system protections. The primary work of this program is that they will catch the keystrokes squeezed by the client and store them in a log file.

**Introduction**

Keyloggers are implanted on a machine to intentionally monitor the user activity by logging keystrokes and eventually delivering them to a third party. While they are seldom used for legitimate purposes (e.g., surveillance/parental monitoring infrastructures), keyloggers are often maliciously exploited by attackers to steal confidential information.

Keylogging is a way to spy on a computer user. It’s generally used to gain access to passwords and other confidential information through fraud. It records every keystroke made on your computer.

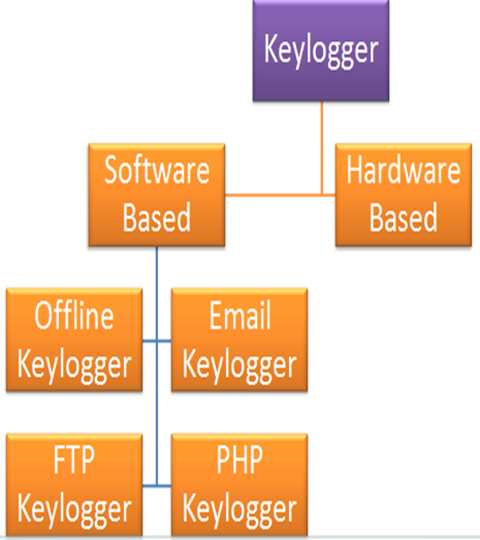


Fig-1

**Literature Survey**

Yousof Al-Hammadi et al[1] Has proposed that different works deal with the detection of key loggers. The simplest approach is to rely on signatures. Many commercial anti-malware adopt this strategy as a detection routine. One popular technique that deals with malware in general is taint analysis. The role of the injector is to inject input stream into the system, mimicking the behavior of a simulated user at the keyboard.

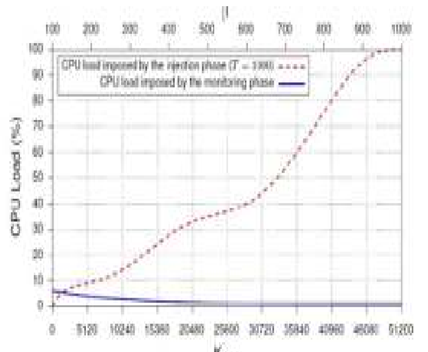
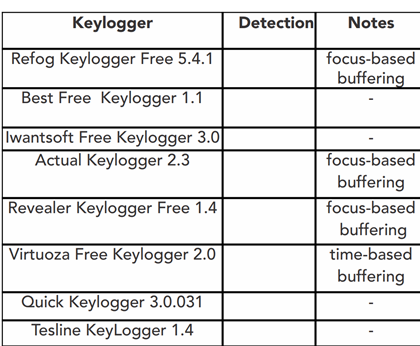
 

Fig-2

Anita at el. (2) has said that the 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 .

Jun Fu at el. (3) that This method can differentiate the running keylogger process from the normal processes with a high detection rate and a low false alarm rate. All legitimate applications that hook the system would be detected as malicious. Software keylogger intercept data travelling along the keyboard and the operating system. It collects key stroke events, stores them in a remote location, and then transmits to the attacker who installed the keylogger Research about removal of spyware parasites reported a total of 540 keyloggers and they were mostly software-based. Windows operating 3 system has many event mechanisms.

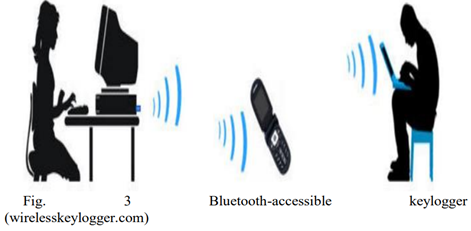


Fig-3

Aslam at el. (4) has proposed that the anti hook shield can easily find 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.

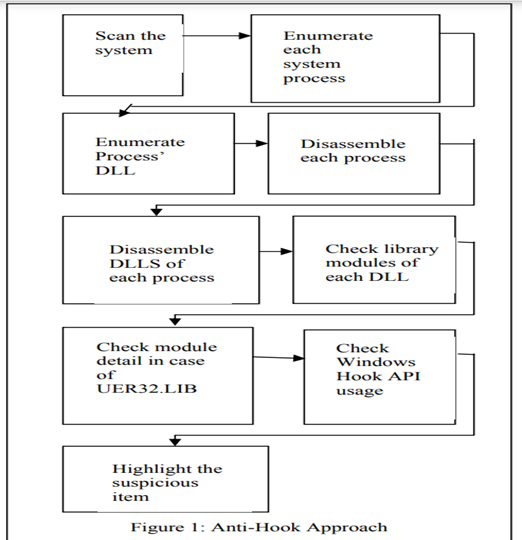


Fig-4

Le at el. (5) has said that the integration with VMscope techniques is necessary. The framework can detect kernel level keylogging that intercept keyboard drivers, particularly tty buffers and identify their root causes. Keyloggers as invisible keystroke recorders have posed a serious threat to user privacy and security. It is difficult to detect keyloggers, especially kernel keyloggers that operate at the operating system’s kernel level, because of their inconspicuous activities and flexible interception methods.

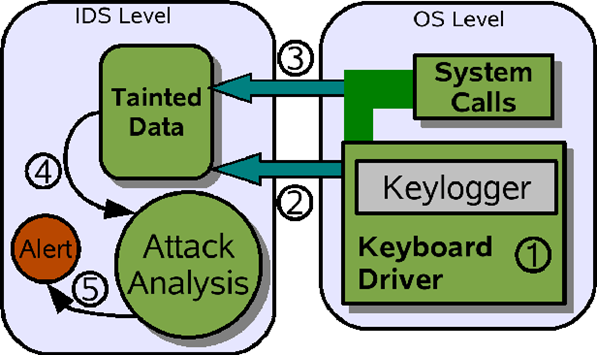


Fig-5

Stefano at el. (6) has said that the KLIMAX: Profiling Memory Write Patterns to Detect Keystroke-Harvesting Malware. Malware evasion techniques that conceal or delay information leakage are not concerned with this detection technique. 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.

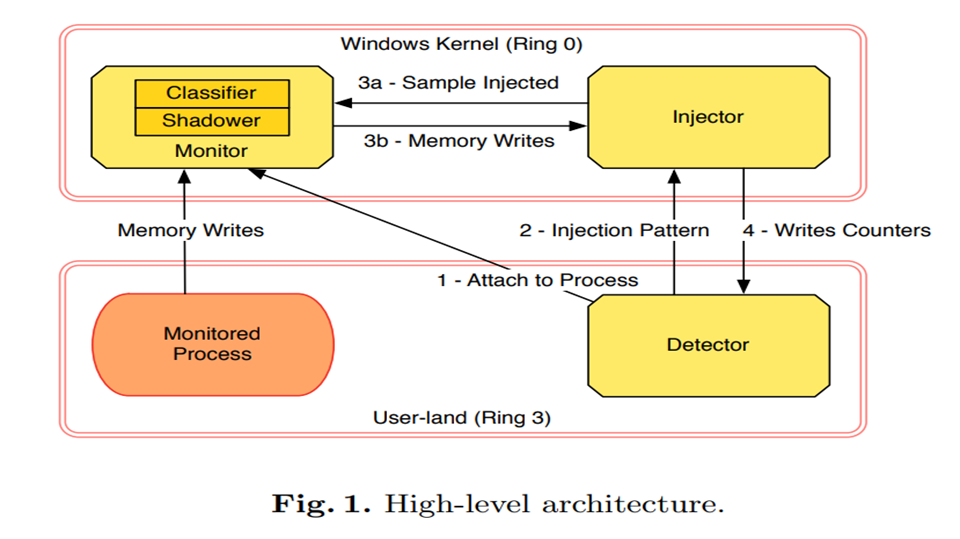


Fig-6

Manan Kalpesh Shah at el. (7). Has proposed that real time working of keylogger malware analysis. Your machine will also search for behaviors that may indicate the existence of new, unidentified malware. We concentrate on a specific form of malware, keyloggers.

Martin Vuagnoux at el. (8). Compromising electromagnetic emanations of wired and wireless keyboards. A keylogger can possibly get installed after opening a file attached to email. When a file is launched from an open-access directory on a P2P network, a keylogger can get installed.

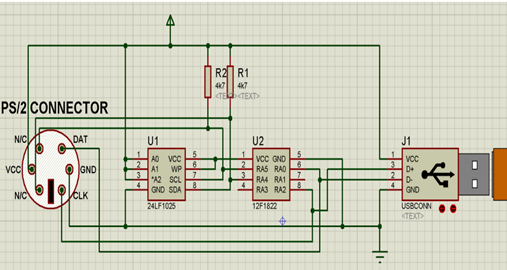
Fu, Jun, Yiwen Liang at el. (9). Has stated that Detecting software keyloggers with dendritic cell algorithm. Data captured include passwords, user ID’s, document contents and other critical information; therefore, an attacker can obtain sensitive data without cracking a database or file server.

A. Davis at el. (10) the hardware keylogger detection in Small electronic devices used to record the data between a keyboard interface and an I / O port are hardware keyloggers. After being installed on a computer system, they store the keystrokes in their built-in memory.

**Countermeasures**

Denial of physical access to sensitive computers, e.g. by locking the server room, is the most effective means of preventing hardware keylogger installation. Visual inspection is the easiest way of detecting hardware keyloggers. But there are also some techniques that can be used for most hardware keyloggers on the market, to detect them via

software.



**Conclusion**

Keyloggers are powerful tools that cannot threaten the system itself, but the user’s confidential data such as user name, password, pin and card bank. Although some keyloggers are used in a legitimate way, many keyloggers are used illegally by the creator. Detecting keylogging technology within the organization is no different than controlling other malicious code or threats, requiring common awareness, regularly

monitoring and a layered defense.

**References**

[1] Yousof Al-Hammadi and Uwe Aickelin. Detecting bots based on key logging activities. In Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, ARES ’08, pages 896–902, march 2008.

[2] M. Aslam, R.N. Idrees, M.M. Baig, and M.A. Arshad. Anti-Hook Shield against the Software Key Loggers. In Proceedings of the 2004 National Conference on Emerging Technologies, pages 189–192, 2004.

[3] Martin Vuagnoux and Sylvain Pasini. Compromising electromagnetic emanations of wired and wireless keyboards. In Proceedings of the 18th conference on USENIX security symposium, SSYM ’09, pages 1–16, Berkeley, CA, USA, 2009. USENIX Association.

[4] Mihai Christodorescu and Somesh Jha. Testing malware detectors. In Proceedings of the 2004 ACM SIGSOFT International Symposium on Software Testing and Analysis, ISSTA ’04, pages 34–44, New York, NY, USA, 2004. ACM.

[5] Manuel Egele, Theodoor Scholte, Engin Kirda, and Christopher Kruegel. A survey on automated dynamic malware-analysis techniques and tools. ACM Computing Surveys (CSUR), 44(2):6:1–6:42, March 2008. ISSN 0360-0300.

[6] Andrea Lanzi, Davide Balzarotti, Christopher Kruegel, Mihai Christodorescu, and Engin Kirda. Accessminer: using system-centric models for malware protection. In Proceedings of the 17th ACM conference on Computer and communications security, CCS ’.

[7] Kaspersky Lab. Key loggers: How they work and how to detect them.

http://www.viruslist.com/en/analysis?pubid=204791931. Last accessed: Jan 2014.

[8] Engin Kirda, Christopher Kruegel, Greg Banks, Giovanni Vigna, and Richard A. Kemmerer. Behavior-based spyware detection. In Proceedings of the 15th conference on USENIX Security Symposium, SSYM ’06, Berkeley, CA, USA, 2006. USENIX Association.

[9] Anthony Cozzie, Frank Stratton, Hui Xue, and Samuel T. King. Digging for data structures. In Proceedings of the 8th USENIX conference on Operating systems design and implementation, OSDI ’08, pages 255– 266, Berkeley, CA, USA, 2008. USENIX Association.

[10] Security Technology Ltd. testing and reviews of key loggers, monitoring products and spy software. http://www. k e y logger.org.

[11] Don ’t fall victim to Key loggers http://www.makeuseof.com/tag/dont-fall-victim-to-keyloggers-use-these-important-anti-keylogger-tools/ Last

accessed: Jan 2014.

[12] Overview of detecting key loggers: http://www.sandboxie.com/ Last accessed: Feb 2014.

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

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

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