Implementation of Network Monitoring As a G-Host

[1] Mr. Anand Tembhurne, [2]Mr. Pratik Kaste, [3]Mr.Vighnesh Chavhan,
[4]Asst. Professor Mr.Pradip O. Balbudhe

[1,2,3,4] Computer Engineering Department, Suryodaya College of Engineering & Technology, Nagpur, India

Abstract: **Spyware – malicious software that passively collects users' information without their knowledge is a prevalent threat. Spy Monitoring Server is used to monitor and control the client machines in the network. It allows the administrator to view the systems connected to the LAN. The system information contains OS name and version, Processor details. It is capable of storing login details of the user. It can also monitor the data send by the user. It can share the desktop screen of the users also. The project Spy Monitoring Server‖ is an application which needs to be installed in the server. The computers are connected by a LAN. The computers are recognized either by their computer names or by their IP address.**

Keywords: **Log Monitoring, Live Monitoring, Desktop Sharing, Online/Offline Communication, Monitoring And Reporting.**

1. INTRODUCTION

This network monitoring software gives a supervisor or administrator the tools they need to monitor and filter employee or student PC activity. SNM also boasts unique remote control tools including the ability to FULLY control and use any PC all from the comfort of the admin's own workstation.

SNM runs in total stealth and is hidden within the Application Task List in Task Manager. No icons or other traces of the software will be displayed on the desktop or start menu. The network administrator can connect and monitor any machine in total stealth.

2. LITERATURE SURVEY

Spyware is one type of malicious software (malware) that collects information from a computing system without your consent. 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. 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.

3. EXISTING SYSTEM

Monitoring is done using only Hidden Camera. We only watch how many users are available in the office or organization, but we don't know what they are doing.

Limitations of Existing system:

- Single user access within network
- Less efficient

- Absence of real-time environment
- Can’t take Screenshot
- Does not allow Multiuser monitoring

4. PROPOSED SYSTEM

The Network Monitoring section has two different types of features. The first type is that of ***Live Monitoring***. Certain functions can be performed live to instantly "check-up" on a user. The second type of monitoring is ***Logged Monitoring*** which captures specific activity and stores it for later viewing.

4.1 LIVE MONITORING:

Spy Network Monitoring allows you to check-in one, some or all users at once. This shows you whether they are doing what they are *supposed* to be doing. You can also watch keystrokes as they happen! These features allow you to effectively watch all users' actions in real time.

4.1.1 View Real Time Screens, Events and Keystrokes!:

Spy Network Monitoring allows the administrator to view an actual screenshot of one, some or all workstations instantly! You can even watch keystrokes and events as they happen! This is used for live surveillance to see if your network users are *working* or playing.

4.1.2 View Active Processes, Services and System Info:\

Spy Network Monitoring will show the administrator a full list of processes and services running on the remote machine. A full list is shown along with the ability to kill any process. Real time general system information can also be viewed.

4.1.3 View Recent Documents:

Spy Network Monitoring will show the administrator a list of recent documents opened by a user. This and other functions can be performed instantly at any time. Shows all types of files such as Excel, word.

4.2 LOGGED MONITORING:

Log monitoring is just like software. It does maintain that monitors log files. Application, network and Security devices Servers generate log files. Errors and problems is constantly logged and saved for analysis. In order to detect problems

After installing Spy Network Monitoring onto a network, it immediately begins to record all activity on the client PCs. Logs can be exported for storage and are standard JPG images and text files. Logs can easily be printed from within the interface.

4.2.1 Window Opened:

Spy Network Monitoring creates a list of windows that were opened on the monitored computer. This feature stores the title of the window along with the username and timestamp. Also includes the ability to display records from a specific date all at once.

4.2.2 Screenshots Capturing:

Spy Network Monitoring captures full-size screenshots of the entire screen at any interval you set. That's right; you will have a picture of the entire screen however often you choose. This captures a picture of absolutely ANY activity displayed on the screen.

5. ONLINE/OFFLINE COMMUNICATION

Spy Network Monitoring is used for online/offline communication. The terms "online" and "offline” have specific meanings in regard to computer technology and telecommunications. In general, "online" indicates a state of connectivity, while "offline" indicates a disconnected state. In common usage, "online" often refers to the Internet or the World-Wide Web. The concepts have however been extended from their computing and telecommunication meanings into the area of human interaction and conversation, such that even *offline* can be used in contrast to the common usage of *online*. For example, discussions taking place during a business meeting are "online", while issues that do not concern all participants of the meeting should be "Taken offline" — continued outside of the meeting.

6. SPY MONITORING

Spy monitoring is a ¯Network monitoring". It refers to the practice of overseeing the operation of a computer network using specialized management software tools. Network monitoring systems are used to ensure availability and overall performance of computers (hosts) and network services. These systems are typically employed on larger scale corporate and university IT networks.

PLAN OF ACTION

Month	**Plan Of Action**
Dec. 2014	Study Of Literature Survey.
Jan. 2015	**Module1** Creating a client program
Feb. 2015	**Module 2** creating a server program
Mar. 2015	**Module 3** connectivity with database for storing images
April.2015	Deployment of all modules and Final testing.

7. METHODOLOGY

7.1 Java Remote Method Invocation:

The **Java Remote Method Invocation** Application Programming Interface (API), or **Java RMI**, is a Java application programming interface that performs the object-oriented equivalent of remote procedure calls (RPC).

1. The original implementation depends on Java Virtual Machine (JVM) class representation mechanisms and it thus only supports making calls from one JVM to another. The protocol underlying this Java-only implementation is known as Java Remote Method Protocol (JRMP).

2. In order to support code running in a non-JVM context, a CORBA version was later developed

7.2 The RMI Architecture:

The server must first bind its name to the registry. The client lookup the server name in the registry to establish remote references. The Stub serializing the parameters to skeleton, the skeleton invoking the remote method and serializing the result back to the stub.

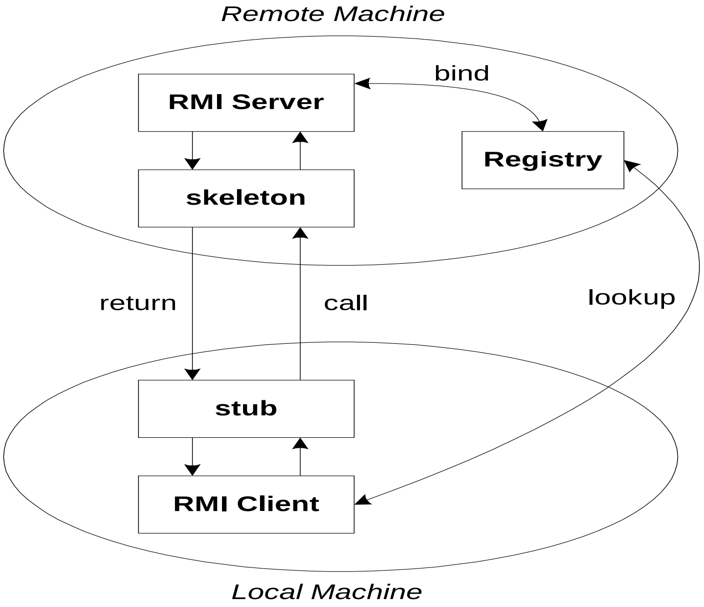
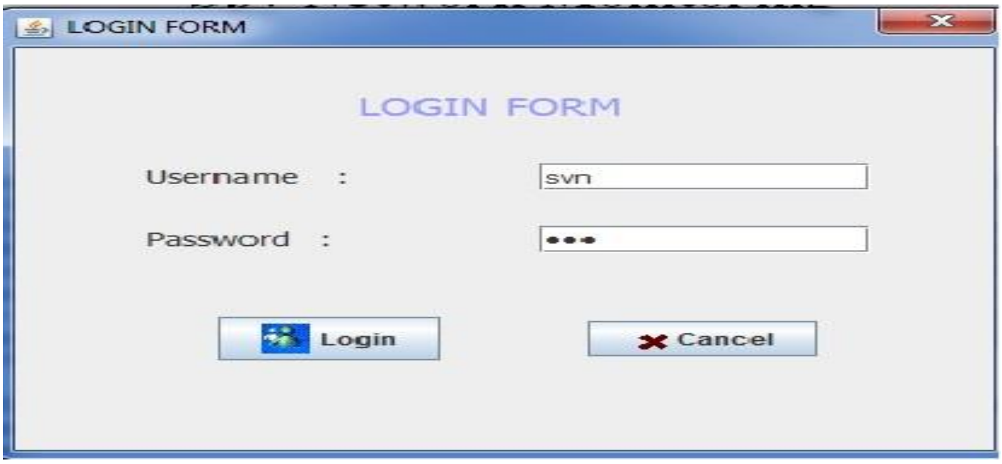


Fig.1 RMI Architecture

8. BASIC FEATURES

1. Full Remote Control
2. View Events LIVE
3. View Remote Desktop
4. Documents Recorder
5. Keystroke Recorder
6. Snapshot Recorder
7. Shut Down Remote PC
8. Restart Remote PC
9. Lock Remote PC
10. Content Filtering
11. Application Blocker

SCREEN SHOT:



Username : svn

Password : •••

Fig.3 login administrator

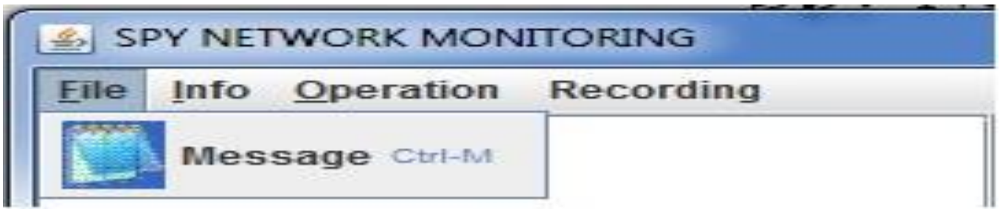


Fig.4 sending a message to client

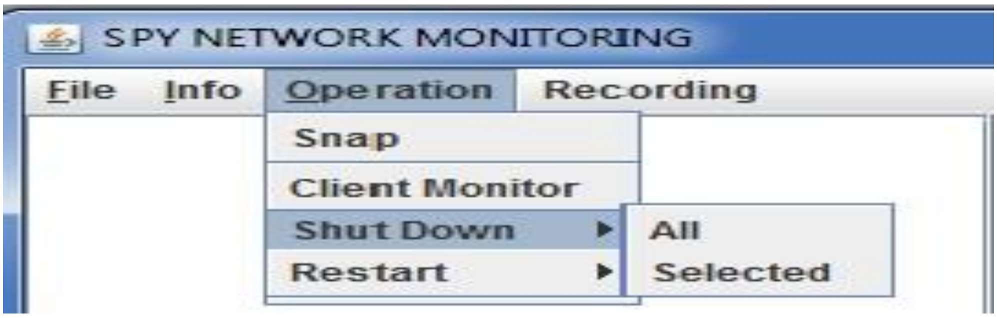


Fig.5 Administrator performing some operation

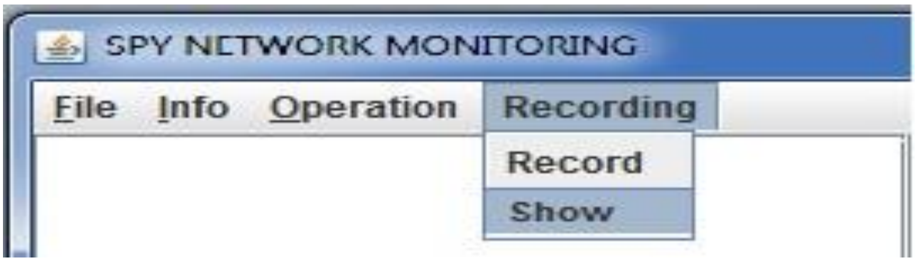


Fig.6 recording the client activity

9. 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 we are conclude that some future scope can be added & implement the source code later. This project can be easily helpful that to monitor all the remote pc & also to protect some important database related with us. Improves the speed of work in transfer Data. 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.

REFERENCES

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

[2] Ethereal - A Network Protocol Analyzer,‖ 2009

[3] Net Spy: Automatic Generation of Spyware Signatures for NIDS by Hao Wang, Somesh Jha, Vinod Ganapathy, 2006.

[4] Behavior-based Spyware Detection: Kirda and Kruegel, 2006

[5] Federal Trade Commission Staff report, March 2005.

[6] En.wikipedia.org topic ―Log Monitor‖.

[7] Packet Sniffing: Robert Graham.

[8] Exploring Spyware Effects: Martin Bold, Bengt Carlsson & Andreas Jacobson, 2004.

[9] A Crawler-based Study of Spyware on the Web: Alexander Moshchuk, Tanya Bragin, Steven D. Gribble, and Henry M. Levy, 2006.

[10] Spyware: Aaron Hackworth, 2005.