International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

System Monitoring and Communication

Omkar Kolambkar[1], Namita Kolambkar[2]

[1]Tata Consultancy Services, India
om3101[at]gmail.com

[2]V.P. M's Polytechnic Thane, Maharashtra, India
namita.redkar90[at]gmail.com

Abstract: ***In this paper we have the advanced remote desktop monitoring system with communication. This application enables us to monitor n-number of clients at real time. Key-logging is also an enhanced feature in order to keep track of minute actions of clients. This application also enables the Server to initiate the chat with clients as well as it enables the Server to take actions like shut down, log-off and other actions.***

Keywords: Monitoring; SysMoCom; Key-Logging; Encryption; Steganography; Cryptography; Network Security

1. Introduction

One of the most important responsibilities a system administrator has is monitoring their systems. A system administrator should always monitor the network to keep the network secure. In today's era hackers and crackers are increasing day by day. In today's competitive era where business competition is at an apex if any intruder passes confidential information to the rival company then the company can suffer millions of losses. In order to prevent such attacks system monitoring is very essential [4].

Nowadays, Computer Security has given more importance. In today's era hackers and crackers are increasing day by day. Terrorist also communicates via internet connections. Computer systems can be exploited for both fraud and theft both by "automating" traditional methods of fraud and by using new methods. For example, individuals may use a computer to skim small amounts of money from a large number of financial accounts, assuming that small discrepancies may not be investigated. Financial systems are not the only ones at risk, systems that controls access to any resource are targets (e.g., time and attendance system, inventory systems, school grading systems, and long distance telephone systems). Computer fraud and theft can be committed by insiders or outsiders [4].

System Monitoring and Communication is abbreviated as SysMoCom. SysMoCom is used by administrator to monitor various client activities in the network at real time. Using SysMoCom we can see the live motion pictures of the client's desktops at real time. Moreover, it can also be used as a key-logger.

The additional features include chatting between server and client, key-logging, taking various actions on client's computer and retrieving all the information of the client's computer. For communication purpose chatting is enhanced in SysMoCom. The information which will be logged on the client's side will be encrypted and will be steganographed in a .jpeg (Joint Photographic Expert Group) format. This will ensure that all the operations carried out on the client side will be done without the knowledge of client. If any illicit activities are encountered at the client side the server can chat or warn the client. If client does not listen then server can take actions such as shutting down, restarting and logging off the client's machine. Additionally, server can also lock or release the mouse of the client's machine. The software which will be installed on the client's machine will be hidden and will not be accessible by the client. Moreover, it will neither be visible in the task bar nor in the control panel and neither in program files. So client will have no knowledge that somebody is monitoring him. If the server wants its desktop to be viewed on all the client machines' then it can also be done using this application.

2. SysMoCom Working

Initially SysMoCom server application will be installed on the server side. Then the client application will be installed on the client side. The architecture is shown in the Fig1. According to the fig 1, a Server is monitoring 5clients simultaneously. After both the client side and the server side installation, add the clients with their client name and their IP Address at the server SysMoCom [9].

Figure 1: Architecture of Monitoring in SysMoCom

After adding the clients start the monitoring and the key-logging process. The working of SysMoCom is based on following main features:

A. Monitoring at real time.
B. Key-Logging
C. Cryptography and Steganography
D. Communication and Taking Actions

A. Monitoring

While monitoring the client SysMoCom will capture the whole desktop image and will send at a high rate at approximately 10images/sec to the server in order to show a motion video of the client's desktop at real time. The image will be stored in the buffer while sending in .JPEG format. So the size of the image will be less.

B. Key-Logging

Key-Logging is an important feature as it tracks each and every minute action of the client. It enables us to monitor what the client is typing, which application is open and which is closed [5]. If the client travels through any path for example, Start→ Programs → Paint, the key-logger will record all the actions. Moreover, it will show us the Process list and the Service List of the client from which we can detect the status of any application or any external hardware. All this information which is logged at the client side is encrypted [1] and steganographed [iii] in an image file to keep the user unaware that some external entity is monitoring his system.

C. Cryptography and Steganography

Cryptography in SysMoCom includes encryption on the client side and decryption on the server side [3].

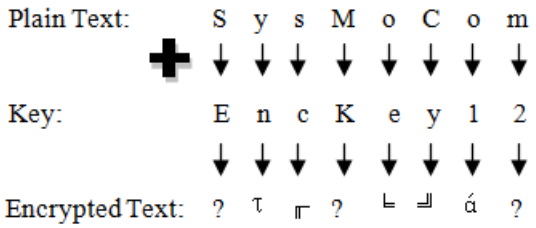

Figure 2: Encryption Process

1) Encryption:

In the process of encryption, the ASCII (American Standard Code for Information Interchange) value of the characters of the plain text and the ASCII value of the characters of the key are added. If the sum of these ASCII value is greater than 255 i.e., if the sum is exceeding the ASCII range then subtract 255 from the sum. Then convert the resulting number to character. The above Fig2 depicts the process of encryption. In SysMoCom, the password which is entered at the server side to start the application is encrypted by the above method using username as the key. Then the resulting encrypted text is used as a key to encrypt the logged information at the client side. Thus, double encryption in SysMoCom enables high security. Then this encrypted text is steganographed in .jpeg file. As the text is encrypted client cannot recognize the difference between the encrypted text and the image text [3]. So even if they open the image file in text format they cannot make out from where the actual data starts.

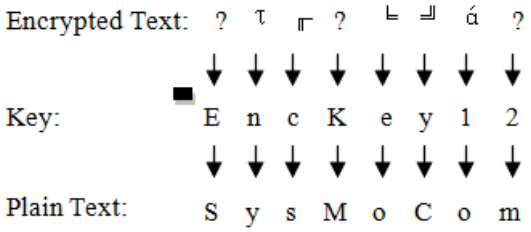

Figure 3: Decryption Process

2) Decryption:

In the process of decryption, the ASCII value of the characters of the key are subtracted from the ASCII value of the characters of the encrypted text [3]. If the difference of these ASCII values is less than 0, i.e., if the difference is negative, then add 255 to the difference. Then convert the resulting number to character. Fig3 depicts the decryption process. In SysMoCom, the decryption takes place in the reverse manner of the encryption [3].

3) Steganography:

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity [1]. In SysMoCom application, the client SysMoCom will write the encrypted logged data in an image file. After the encryption is complete, the client SysMoCom will seek the pointer to the end of an image file stored at the client side. Then, it will append all the encrypted log data to that image file. While, retrieving the data the server SysMoCom should know the seek point in the image file so that it can retrieve the data after the end of the actual image data [3]. After encrypting the data, the encrypted data looks similar to the data in the image. Thus, client cannot recognize that data is hidden in the image.

D. Communication and Taking Action

SysMoCom has a feature of communication. Communication between server and client is enabled using the logic of chatting. Server can communicate with one client or with the whole network simultaneously. This feature of communication can be initiated only by the server. The other mode of communication is specifically a visual element. In this visual element the server can broadcast his desktop on all the client's machines. This visual element communication can be very useful during conferences [10].

SysMoCom has enabled a feature of taking some actions on the client. The actions to be taken on the clients are totally depended on the server.

Server can take actions such as shut down, log-off, restart, mouse lock and mouse release on the client's machine. In this operation, server SysMoCom will inform the client SysMoCom which action should be taken. After the information of the action has received, client SysMoCom will execute commands relevant to the action on the client's machine [5]. Server can take actions on as many client machines as his requirement [10].

3. Features of SysMoCom

Usually monitoring softwares comes isolated in parts comprising of only remote desktop monitoring or only key-logger [1]. SysMoCom is the combination of both viz, remote desktop monitoring and key-logging. Moreover, it provides us with initiating any new process or application on the client side. It also enables server to kill any process on the client side as well as check status of any service on the client side. SysMoCom enables the server to get the whole information including the configuration of the client's machine. SysMoCom has high security features which include cryptography and Steganography. Cryptography comprises of double encryption which makes the client unaware of monitoring. Moreover, the client SysMoCom which is installed on the client side is invisible in the task bar or in the task tray and all the logged information is stored in encrypted form and steganographed [3] in an image file which cannot be recognized by the client. This makes the application highly secure and concealed. One more interesting feature SysMoCom provides is communication. Server can communicate with one client or with the whole network simultaneously. This feature of communication can be initiated only by the server. The other mode of communication is specifically a visual element. In this visual element the server can broadcast his desktop on all the client's machines. This visual element communication can be very useful during conferences. SysMoCom also enables server to take some actions on the client's machine such as shut down, restart, log-off, mouse lock and mouse release.

4. Existing Systems

There are many types of software available in the market consisting of remote desktop monitoring. Internet is flooded with freeware consisting of key-loggers [7]. TeamViewer is an application which enables a client to become the master of any other machine in the network via internet [2]. LANvisor is another application which consists of remote desktop monitoring concept [6]. The drawbacks of the existing applications are that they are isolated. Some applications have high security features but they do not have efficient transmission. Some software lag behind due to slow buffering. If they have good data rates they lack in security. VNC remote desktop software has remote desktop monitoring features but it does not comprise of key-logging feature [7]. In order to overcome the drawbacks of the existing systems SysMoCom is developed.

5. Scope

As the human life is very busy and fast and use of computers is growing very rapidly and the computers handles much of the human work, due to this we need to be advanced and have technology, which reduces our complications [1].

SysMoCom can be used in various areas. Scope of SysMoCom is vast. As every organization, industry, educational institute and various other sectors are totally computer equipped security is a major issue [3].

SysMoCom can be used in companies by the supervisors to supervise their employees. It can be used in Cyber Café to prevent cybercrime. It can be used in educational institutes to prevent cheating done by students during practical examinations. It can be used by users as honey-pot to spy on hackers and seek their techniques. It can be used on a large scale as a part of national security. SysMoCom can be used as essential software in any company to hide confidential information from the rivals.

6. Trends and Risks

The challenge in SysMoCom is to breach all the firewalls and anti-virus specifications so that the monitoring could be done clearly without any interruption. The network speed should not degrade due to transfer of data continuously. For this purpose, the monitoring is done using compressed version of .jpeg format files.

Image compression at the client side should take place in order to decrease the transmission time and increase the speed of simultaneous transmission.

Another risk is that the connection should be duplex. This risk occurs when along with remote desktop monitoring and key-logging, conference desktop is also held simultaneously. This will have performance degradation.

7. Conclusion

Remote Desktop Monitoring is very popular software but not up to consumers demands. System Monitoring and Communication is an application which comprises of all aspects of monitoring such as visual, data monitoring as well as communicating with the clients. Moreover, interrupting and modifying the clients machine is also enable by SysMoCom. SysMoCom satisfies all the aspects of high security features which make the client's unaware that they are being monitored.

8. Summary

SysMoCom application comprises of following process:

1. Connection of one computer with n – number of computers.
2. Image Capture at a very fast speed in milliseconds as to show the working of client's machine in real time.
3. Encryption: Double Encryption used.
4. Decryption: Double Decryption used.
5. Steganography: Append the encrypted data to the end of the image file.
6. Database Connectivity on the server side.
7. Key Logging at the client side.
8. Transfer of data from client side to server side.
9. Hiding the Client-SysMoCom on the client's machine i.e., the software at the client side should not be visible to the client.
10. Retrieving service and process list as well as the client's machine information.

11. Automatic activation of Client-SysMoCom at the start-up of client's machine.
12. Chatting between server and client machines.
13. Designing an interface such that n - number of clients can be monitored simultaneously.
14. Giving certain privileges to Server to shut down, log-off, restart, mouse-lock.
15. Conference Desktop: Server's desktop is visible on the entire client's screen.

Acknowledgment

A project is a creative work of many minds. A proper synchronization between individuals is a must for any project to be completed successfully.

We owe deep gratitude to our Prof. Suhasini Shukla (HoD, Computer Engineering Department). She rendered her availability and guidance with a touch of inspiration and motivation. She guided us through quite substantial hurdles by giving plenty of early ideas and which finally resulted into fine work.

We would also like to thank our Principal Mr. D. K. Nayak(V.P.M's Polytechnic) who has been a constant support.

Finally, we also would like to express our thanks to all those who helped us directly or indirectly in successful completion of this paper.

References

[1] www.wikipedia.org
[2] www.teamviewer.com
[3] Behrouz A. Forouzan, Cryptography & Network Security, 3rd ed, Tata McGraw-Hill Publication.
[4] William Stallings, Cryptography & Network Security, 3rd ed, Textbook and Academic Authors Association, 1999.
[5] Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, Gray Hat Hacking The Ethical Hacker's Handbook, 2nd ed, TMH Publication.
[6] www.lanvisor.com
[7] www.softpedia.com
[8] Wang and Jie, Computer Network Security Theory and Practice, 4ed, Higher Education Press, 2009.
[9] Behrouz A. Forouzan, Computer Networks- A Top Down Approach, TMH Publication, 2011
[10] www.msdn.microsoft.com