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. 6, June 2013, pg.170 – 175

RESEARCH ARTICLE

Monitoring and Its Impacts over Distributed Systems and Possible Solutions

Manjunath Kotari[1], Dr. Niranjan N. Chiplunkar[2], Dr. Nagesh H R[3]
[1]Associate Professor and PG Head, Dept of CSE, AIET, Moodbidri, India
[2]Principal, NMAMIT, Nitte, India
[3]Prof & Head, Dept of CSE, MITE, Moodbidri, India

[1] mkotari@gmail.com; [2] niranjanchiplunkar@rediffmail.com; [3] nagesh_h_r@hotmail.com

Abstract— Monitoring is the process of obtaining, collecting, and presenting the information required by a system about the observed system. Monitoring is always carried out with a purpose in mind. The general aim is to obtain information in order to construct a model of system behaviour or to modify an existing model. The general activity of monitoring a system can be specialized to a particular purpose such as accounting, debugging or testing, among others. Distributed systems (DSs) are used in an increasing number of domains, such as research, industrial and social environments. Now work environments and peoples are distributed across multiple organization and geographical boundaries. Monitoring is done to track the activities of this distributed system and that information is stored for Future use. This paper addresses the monitoring of distributed system, monitoring impacts in distributed systems and reusability of monitored information.

Key Terms: - DSs; Monitor; Activities; Reusability; RSA

I. INTRODUCTION

Monitoring is carried out in order to obtain information about a system, and in general, monitoring is part of the process of management. Among the many activities which involve monitoring are debugging, testing, accounting, performance evaluation, resource utilisation analysis, and security and fault detection. Monitoring is concerned with providing the necessary information in order to allow the construction of the required model of the observed system and its presentation. It is the purpose of monitoring which dictates what should be observed and also how the information is to be obtained. Every system is affected by being monitored. The extent of the influence may or may not be negligible from the point of view of the user(s) or the observer(s) of the system. There is a relation between the flexibility of the monitoring facilities, the cost of implementation, and the extent to which they interfere with the behaviour of the system.

Certain problems associated with monitoring in a centralized system are exacerbated when dealing with distributed systems. The following are the problems encounter during monitoring of distributed systems which includes, no central point of control, no central point of observation, incomplete observability, non-determinism, monitoring interference, replication, migration, and monitoring as a distributed activity. The monitoring of a distributed system is itself a distributed activity and it therefore requires tools which allow the management of the process of monitoring access and use to remote resources.

II. LITERATURE REVIEW

Distributed system consists of a group of computers connected together by a computer network in order to exchange information [1]. They communicate with each other using messages, pieces of information transferred

from one computer to another over a network. In Two ways we can organize computers in a distributed system. The first is the client-server architecture, and the second is the peer-to-peer architecture. In client-server architecture, single server provides service and multiple clients communicate with the server to consume its service. In peer-to-peer architecture, all computers have both sender and receiver side code and all [2].

The monitoring of distributed system involves the collection and display of information of interactions among the concurrently executing processes [3]. A company may have many number of branches located at different geographical areas and may need an interaction with all other branches for day-to-day activities. This distributed system gives sharing of the resources such as printers, web pages or database records which is located in different places. The design and implementation of such systems poses greater challenges like how monitoring should be done, what should be monitored, and the impact of monitoring may have on the security mechanism of the target system need to be carefully considered. Sule Yildirim et al. [4] present monitoring of adaptive distributed systems and security metrics for the adaptive distributed systems by using security metric function. The security threat can be minimized if monitoring is done by a trusted and authorized party as well as through secure communication channel.

Two scenarios for monitoring the target system are worth considering:

- The monitor is outside the system.
- The monitor is part of the system.

In distributed systems, some of the monitoring is usually done by a system that is external to the target system [5].

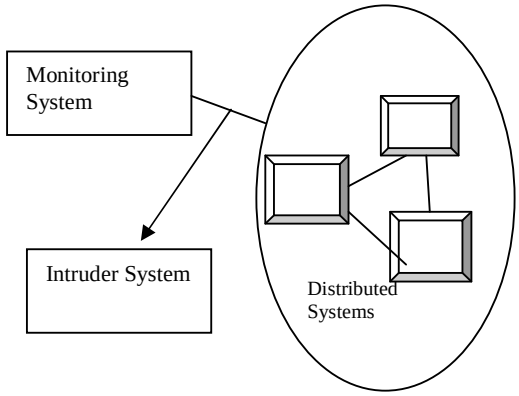

Fig. 1 External monitoring of distributed system

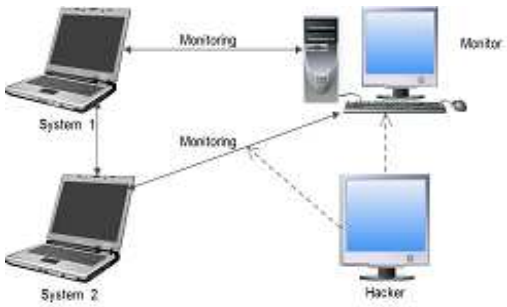

Fig. 2 Internal monitoring of distributed system

Both Fig.1 and Fig.2 shows the case where monitoring of the distributed system is going on and an intruder is trying to hack the information in two ways. One through communication channel means while transforming the information. Second one is directly hacking the monitored information which is stored in monitored system.

III. PROPOSED SYSTEM

Proposed system consists of following phases

A. Monitoring

Message which is transferring between distributed system as well as information related to that message also monitored. We can monitor the time and date of communication, source system IP address and received (destination) system IP address, Username, Exact exchanged message etc.

This monitoring is done by two ways. Viz.

1) *Using Monitoring Tool:* Wireshark is a network monitoring tool. This tool is downloaded from website www .wireshark.org and installed in monitoring system. Using this tool we can monitor even analyze the protocol as well as packets. We can make use of filter option to monitor the only required information.
2) *Using developed Monitoring application:* Application is created for monitoring system. It captures the transferring information of current running processes. Monitored information's are like the IP addresses, Time and date, message and username.

B. Reusability of Monitored information

Monitored information is stored in database. Every time we close the application that time monitored information displayed on screen will be erased but that is stored in database. Each and every time if we monitor the information, then that information may lead to security threat. Instead of disclosing monitoring activities online every time, we can use this stored information. In future whenever required this information that time we can use information in this application.

C. Implementation of security mechanism by using RSA algorithm.

The Intruder, who may present inside the network try to access the information which is transferring between two systems. Intruder will use the Wireshark tool to hack the information. If he clicks on follow TCP stream option of Wireshark tool, he will get the exact message.

Security mechanism is used to protect the information which is transforming between the distributed systems and Monitoring system. Sender nee to encrypt the information in RSA algorithm or other equivalent algorithm while sending. In receiver side it is decrypted and received. When a hacker tries to access the secure communication channels which is used for the transmission of data, an encrypted message is displayed on the screen as a result of opening packets by WireShark monitoring tool.

IV. EXPERIMENTAL RESULTS

The experimental results of the proposed systems are as follows:

1) USER1 is sending message: USER1 is sending the created message to USER2 through IP address that is mentioned in IP Add field.

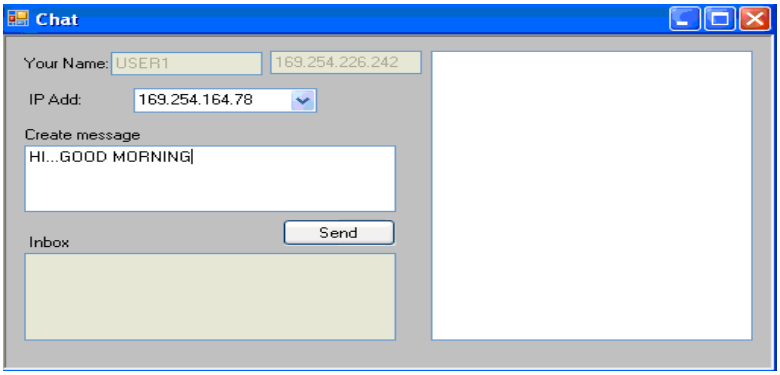

Fig. 3 USER1 is sending message

2) Sent Message is received in inbox: USER2's inbox contains the message which is sent by USER1.

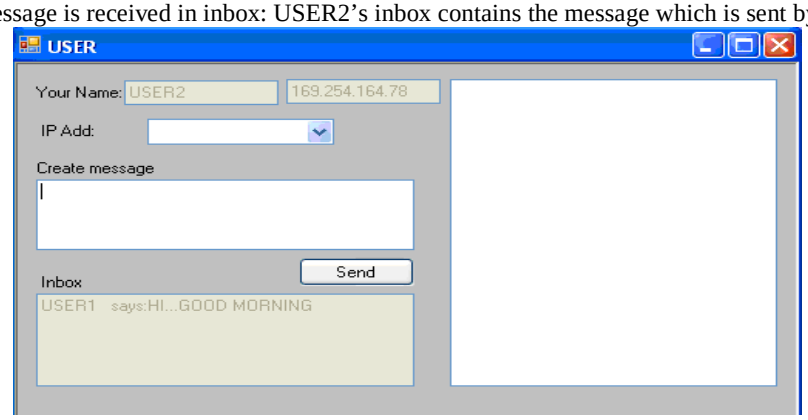

Fig. 4 USER2 is receiving message

3) Monitoring Using Wireshark: Sent message is monitored using tool and we can view the message through Follow TCP Stream screen.

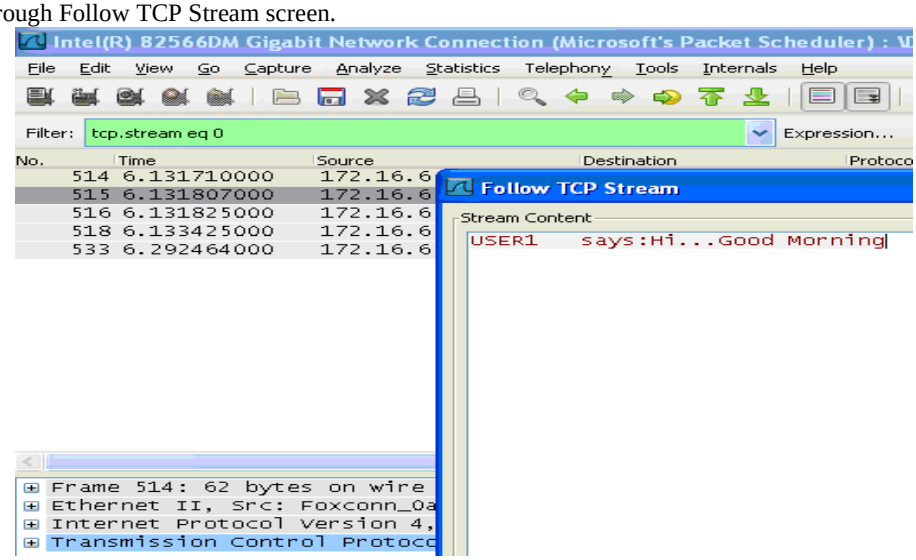

Fig. 5 Monitoring Using Wireshark

4) Monitoring Using developed application: A message which has sent from source to destination is displayed on monitor screen.

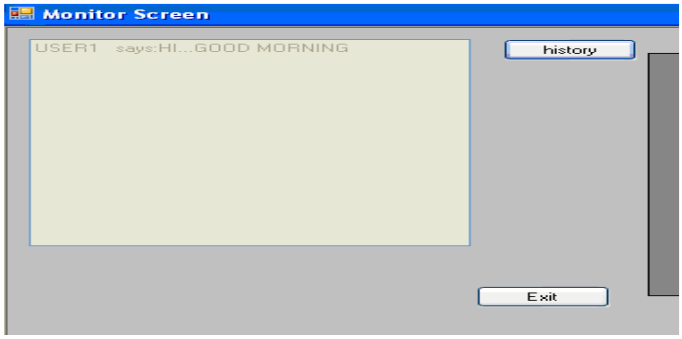

Fig. 6 Monitor screen.

5) When hacker try to hack the message, he will get the encrypted text instead of readable message.

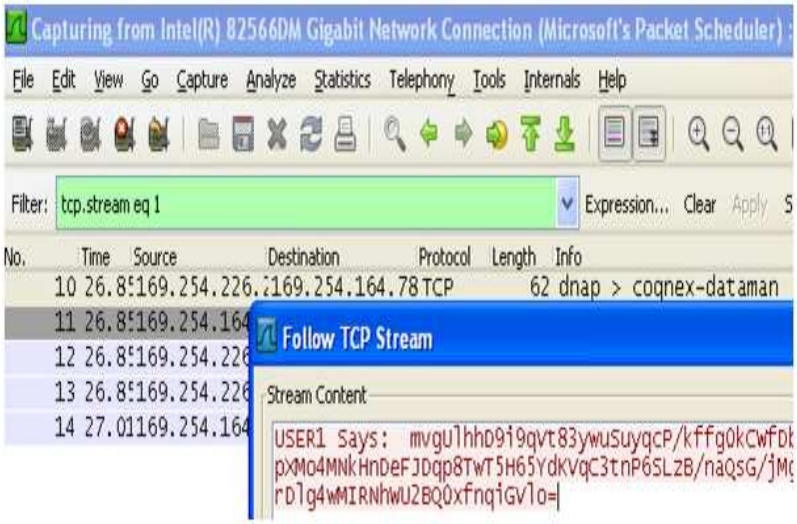

Fig. 7 Hacker gets encrypted format message

6) Reusability: All information which is exchanged between systems is stored in monitoring system. By clicking on History button we can get the monitored information at any time. History table contains information about date and time of message sent, IP_From (source system IP), IP_To (Destination system IP), USERNAME and Message which is exchanged between systems.

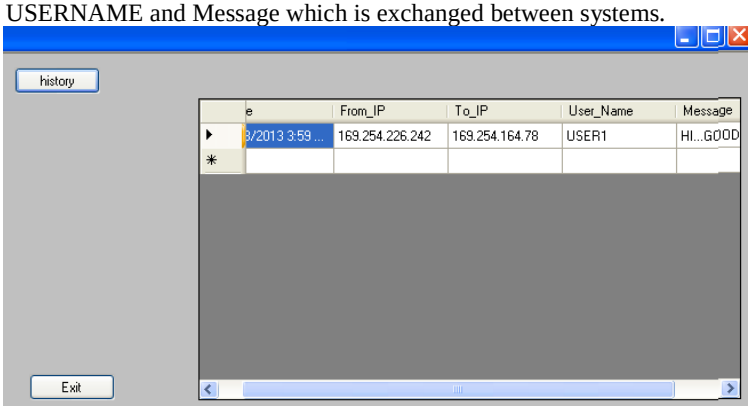

Fig. 8 Reusability of monitored information

V. CONCLUSIONS

Information about distributed system is collected and communication between distributed systems is established. Activities of distributed system are monitored by using monitoring tool and developed application. Monitored information is stored in database. For future purpose we can use this information. When we want to know the history of communication, we can get it this information from database and use it for analysis purpose. Security is provided to distributed system by using RSA algorithm. The implementation of security mechanisms for distributed system is provided using RSA. In this way we can make monitoring safe.

REFERENCES

[1] Michel Banatre, "Hiding Distribution in Distributed Systems", Proceedings of the 13th international conference on Software engineering May 1991.

[2] "Distributed and parallel computing", available at http://wla.berkeley.edu/~cs61a/fa11/lectures/communication.html.

[3] Jeffrey Joyce, Greg Lomow, Konrad Slind, and Brain Unger, "Monitoring Distributed Systems", ACM Transactions on Computer Systems, Vol. 5, No. 2, May 1987.

[4] Aredo D. and Yildirim S., "Security Issues in Adaptive Distributed Systems". Proceedings of the Fourteenth European Conference on Information Systems (ECIS 2006), Goteborg, Sweden.

[5] Manjunath Kotari , Nagesh H R , Niranjan N.Chiplunkar, "Security Aspects of Adaptive Distributed Systems and proposed solutions" ANUSANDHANA-Journal of Science, Engineering and Management, March-2012.
[6] RSA® Transaction Monitoring, White Paper , EMC Corporation, 2013

