Key Exchange Protocol and Remote System Monitoring with Extended Security Model

Manju Lakshmi[1] Bibin Varghese[2] Smita C Thomas[3]
[1,2,3]Mount Zion College of Engineering, Kadamannitta, Pathanamthitta, Kerala, India

Abstract— In this paper we propose remote monitoring, key exchange. Remote System Monitoring is a remote control program, which enables the administrator to access the resources on the remote computer from his own computer and also control the remote computer from the server. Key exchange, authenticated group key transfer protocol consists of three processes: initialization of KGC, user registration, and group key generation and distribution.
Key words: KGC, IP, TCP

I. INTRODUCTION

Remote System Monitoring is a remote control program, which enables the administrator to access the resources on the remote computer from his own computer and also control the remote computer from the server. In remote monitoring first login the client and administrator then access the system. We use the IP trace marking algorithm to trace the IP number of the client system. When IP is trace we can use client system without the permission of the client. In IP trace marking access the system in different ways, monitoring, client authentication, tracing, port scanning etc. The various information regarding the resources of a system in the network are transferred from the remote system to the administrator system in short period of time which will save the administrator time in than the administrator himself going to that system. The administrator can see the remote computer screen in a window on his desktop.

II. PROPOSED SCHEME

In this section propose six phases are there;1) registration ;2) login; 3) key generation; 4) group key generation ; 5) communication ; 6) remote system monitoring. The system architecture, client enters the details and send the request to the server. The sever check the details with a smart card number and accept the request. Sever generate a password to client login the chat. When the client or use is login the chat that time a group key is generating The main proposed method is remote system monitoring and key exchange. To monitor the client system firstly we trace the Ip address of the client system. In IP trace marking to trace all information of the user system. We provide algorithms for the IP trace marking and key exchange method. A) Sever provide a password for the client to login the chat session b) automatically key is generated for the user c) to control the user system. The main advantage of this system is highly secured and freshness of the key.

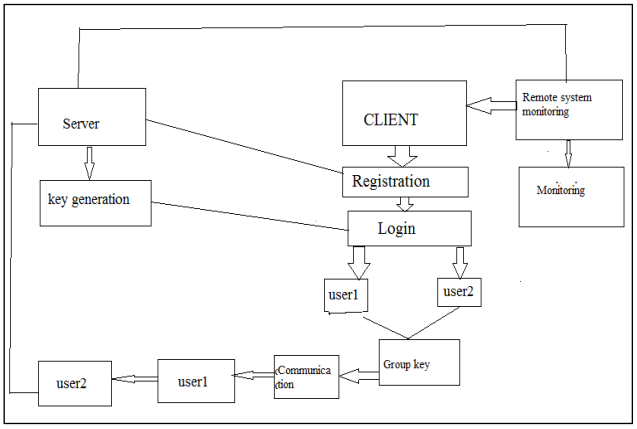

Fig. 1.1: system architecture

A. Remote system monitoring

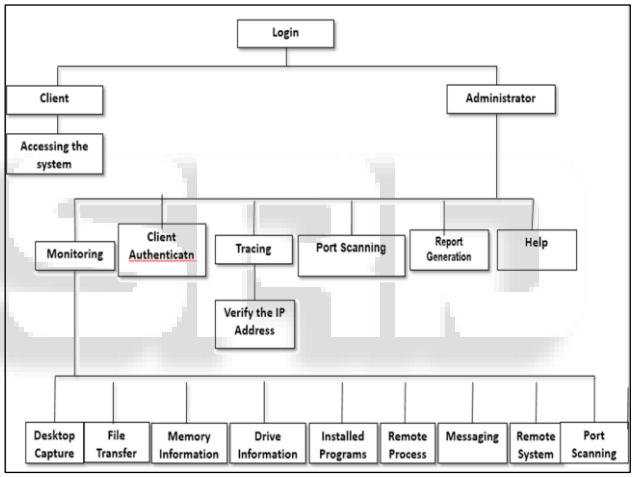

Fig. 2.2: Architecture of remote system monitoring

Remote System Monitoring is a remote control program, which enables the administrator to access the resources on the remote computer from his own computer and also control the remote computer from the server. In remote monitoring first login the client and administrator then access the system. We use the IP trace marking algorithm to trace the IP number of the client system. When IP is trace we can use client system without the permission of the client. In IP trace marking access the system in different ways, monitoring, client authentication, tracing, port scanning etc. The various information regarding the resources of a system in the network are transferred from the remote system to the administrator system in short period of time which will save the administrator time in than the administrator himself going to that system. The administrator can see the remote computer screen in a window on his desktop. The information retrieved from remote machine is displayed in server machine in a user friendly way rather than complicated output formats of certain available software. The module also keeps track of the processes that are running on each system in which the client program has been installed. The remote computer can

be anywhere in the network. Another feature of this module is that, administrator can Shutdown, Restart, or Logoff the remote PC from his computer. "Remote System Monitoring" is developed with the aim of helping the network administrator to gather information about the resources in a remote machine in the network and to keep track of the users working in the systems. The administrator can send a file from his machine to the Remote Machine in the network. The administrator can transfer the file or the information to the client machine. The administrator can transfer the information or the file based on the client request. In the client machine, the user can receive this file and he stored it in a specific location and he can view the information in the file. It prevents the illegal use of any hardware in the client machine. The user cannot able to use CD or any other hardware devices without the permission of the administrator. If the user wants to use CD or any other hardware, he wants to get the permission from the administrator and the administrator can open and view the contents in that particular hardware and if the contents are legal, then only the administrator can sent the contents in that hardware to the client machine from his machine. Then the user can receive this file and save it in a particular location and can view and use the information.

B. Key exchange

Authenticated group key transfer protocol consists of three processes: initialization of KGC, user registration, and group key generation and distribution. The detailed description is as follows:

1) Initialization of KGC:

The KGC randomly chooses two safe primes p and q (i.e., primes such that p0 ¼ p_1 2 and q0 ¼ q_1 2 are also primes) and compute n ¼ pq. n is made publicly known.

2) User Registration:

Each user is required to register at KGC for subscribing the key distribution service. The KGC keeps tracking all registered users and removing any unsubscribed users. During registration, KGC shares a secret, ðxi; yiÞ, with each user Ui, where xi; yi 2 ZZ_n.

3) Group key generation and distribution:

Upon receiving a group key generation request from any user, KGC needs to randomly selects a group key and access all shared secrets with group members. KGC needs to distribute this group key to all group members in a secure and authenticated manner. All communication between KGC and group members are in a broadcast channel. For example, we assume that a group consists of t members, fU1; U2; . . . ; Utg, and shared secrets are ðxi; yiÞ, for i ¼ 1; . . . ; t.

III. SCHEME SPECIFICATION

Key Exchange Algorithm

The key generation and distribution process contains five steps.

- Step 1) The initiator sends a key generation request to KGC with a list of group members as fU1; U2; . . . ; Utg.
- Step 2) KGC broadcasts the list of all participating members, fU1; U2; . . . ; Utg, as a response.
- Step 3) Each participating group member needs to send a random challenge, Ri 2 ZZ_n, to KGC.
- Step 4) KGC randomly selects a group key, k, and generates an interpolated polynomial fðxÞ with degree t to pass through ðt þ 1Þ points, ð0; kÞ and ðxi; yi _ RiÞ, for i ¼ 1; . . . ; t. KGC also computes t additional points, Pi, for i ¼ 1; . . . ; t, on fðxÞ and Auth ¼ hðk;U1; . . . ; Ut; R2; . . .;Rt; P1; . . . ; PtÞ, where h is a one-way hash function. All computations on fðxÞ are over ZZ_n. KGC broadcasts fAuth; Pig, for i ¼ 1; . . . ; t, to all group members. All computations are performed in ZZ_n.
- Step 5.)For each group member, Ui, knowing the shared secret, ðxi; yi _ RiÞ, and t additional public points, Pi, for i ¼ 1; . . . ; t, on fðxÞ, is able to compute the polynomial fðxÞ and recover the group key k ¼ fð0Þ. Then, Ui computes hðk; U1; . . . ; Ut;R1; . . .; Rt; P1; . . . ; PtÞ and checks whether this hash value is identical to Auth. If these two values are identical, Ui authenticates the group key is sent from KGC.

In Fig. illustrate this group key transfer protocol for a group containing three members X, Y, and Z.

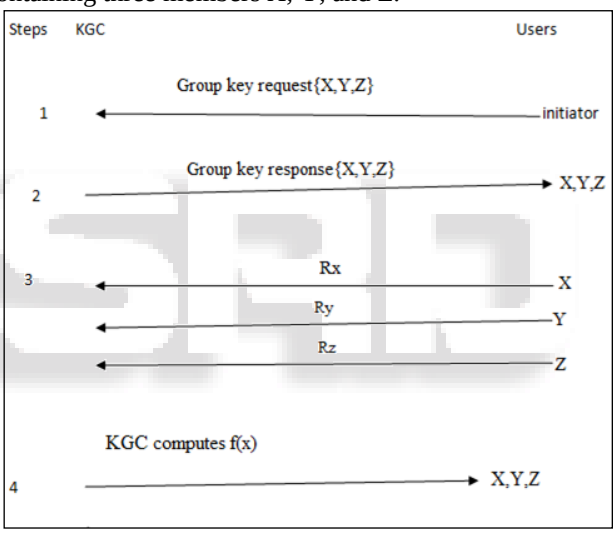

Fig. 3.1: key exchange

A. IP Traceback Marking Algorithm

1) If the traceback server infers a router logged the attack packet, examining the digest tables at that router would identify its upstream router in the attack path.
2) If the traceback server infers a router didn't log but marked the packet, querying the neighbor routers of that router in and examining the digest tables on these neighbor routers would identify the upstream router.
3) If the packet undergoes transformation at the current router, commit both marking and logging operations on the packet, and record the transformation information in the transform lookup table. Given a packet, consulting the transform lookup table can get to know whether the packet was transformed and the original packet can be reconstructed. The implementation of the transform lookup table
4) Add all information of client system to hash table
5) If the packet is a fragmented packet, compute and store the packet digest in a particular digest table which is

only for fragmented packets and is managed in the same way as the hash-based approach.

6) Based on the hashed based table data is remote system is monitored.

IV. CONCLUSION

In this paper propose the remote monitoring of the network. The main advantage of the system is we can control the user or client system. Remote System Monitoring is a remote control program, which enables the administrator to access the resources on the remote computer from his own computer and also control the remote computer from the server.

ACKNOWLEDGEMENT

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of Mount zion college of engineering, for their immense support.

REFERENCES

[1] "Provably Secure Dynamic ID-based Anonymous Two-factor Authenticated Key Exchange Protocol with Extended Security Model" Qi Xie*, Duncan S. Wong, Guilin Wang, Xiao Tan, Kefei Chen, Liming fang.

[2] "Scalable approach for content based image retrieval in peer to peer networks" lelin zhang, tao mein. Volume: 28, issue: 4 april 1 2016.

