ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

Relied Security in Dynamic Routing

Suma Patra

Assistant Professor, Dept. of Information Technology, KITS, Warangal, Andhra Pradesh, India.

ABSTRACT- S**ecure transmission of data plays a crucial role in the networks. To improve the security many methodologies have been proposed till now like cryptographic designs, intrusion detection, dynamic routing etc. In this paper we consider that the data transmission is done by using the concept of dynamic routing. Sometimes the sender may be neglecting the security due to the lack of personal interest, but the receiver has to take the utmost care. In such cases the receiver may force the sender to transmit the data packets by dynamically routing them in a network and crosschecks whether they are dynamically routed or not. From the source each individual packet will be transmitted through multiple paths i.e. through different nodes. If host name or IP Address of each such node (at first hop) is printed along with the data packet delivered through it, the receiver can ensure that the received data is transmitted in a secured manner.**

Keywords: Security-enhanced data Transmission, Assurance, Host name, IP Address.

I. INTRODUCTION

Secure transmission of data plays a major role in the networks. To improve the security, many measures have been taken till now like authentication for user admission, intrusion detection, cryptographic designs, dynamic routing etc. In some cases the sender may be neglecting the secure data transmission. Whether the sender is interested to deliver the data with the security considerations or not, there is a need for the receiver to crosscheck the way of transmission.

In the cryptographic designs, the sender encrypts the original data into cipher text (encryption) and this encrypted data will be decrypted by the receiver (decryption) to get the original text. In this particular case, the receiver gets an assurance that the data received is the secured one, as he receives the cipher text which cannot be understood by the intruder. So, we can say that cryptography provides a noticeable level of security. That is the reason why cryptography based design is implemented on different platforms and systems. But overheads [3], [4] also increase i.e. the time taken to encrypt the data and decrypt the data will increase. It is undesirable. So a need for another alternative has come. A concept called dynamic routing has come into picture. This paper introduces a concept in which the receiver can confirm that the received information is the secured one. The rest of the paper includes the related work in Section 2, proposed work in the Section 3. Section 4 states the conclusion.

II.RELATED WORK

Bohacek et al. [5] proposed a random routing mechanism to provide security while routing. Lou et al. [10] proposed a secured routing protocol to transmit the data by using multiple paths to provide security. Here the multiple paths assigned for the data transmission are determined in an online fashion. But the major drawback of this is that, the number of control messages increases to a great extent as it uses message flooding. Wenjing et al. [11] proposed the delivery of secret information across insecure networks. They proposed an end to-end data delivery scheme called secure protocol for Reliable data delivery (SPREAD).The basic idea of SPREAD is to improve the confidentiality by using multipath routing. Gojmerac et al [7] proposed a simple algorithm called Adaptive Multi-Path routing (AMP) algorithm for dynamic traffic engineering within autonomous systems. In contrast to related multipath routing proposals, AMP does not employ a global perspective of the network in each node. Here available information is restricted to a local scope, through which signaling overhead and memory consumption in routers are reduced. Chin–Fu Kuo et al. [1] explored a security enhanced dynamic routing algorithm which randomizes the paths in which the data packets are sent. This algorithm is efficient and compatible with mostly used routing protocols like Routing Information Protocol (RIP) and Destination-sequenced Distance Vector (DSDV) protocol for wired and wireless networks respectively. Both the above stated protocols need to exchange extra control messages. But control messages are avoided in security enhanced dynamic routing. The main objective in it is to minimize the path similarity i.e. the path taken by the consecutive packets must not be the same.

III. PROPOSED WORK

Security enhanced dynamic routing concepts are the base for this paper. Each and every node in the network maintains a routing table which consists of the destination node, an estimated minimal cost to send a packet to the destination, the Assurance of Security for the Dynamically Routed list of next nodes that can be chosen to reach the destination and the history record for packet deliveries. History of each packet delivery is considered in each case. Suppose a packet is sent through a node N1 which is one of the next-hops of the source S, that particular node will be removed from the list of next-hops. Then the consecutive packet cannot pass through N1. Hence the path taken by any two consecutive packets will not be similar. Secure data transmission is possible if the above process is followed. The best aspect of this method is that there will no extra control messages. When compared to the different methods of improving security like cryptography and multiple path routing, this is better.

Even if the receiver requests the sender to use the concept proposed by Chin-Fu Kuo et al. [1] i.e. security enhanced dynamic routing algorithm to transmit the data, he cannot trust upon the way of transmission, as the sender may or may not be using it. And the data received will not show any evidence of security. For example, if a text "BE GOOD DO GOOD" is sent using security enhanced dynamic routing, the same text will be received at the target system without any additional specifications and there will be no confirmation of dynamic routing. So a situation arises such that the receiver has to cross-check the way of transmission i.e. whether the data packets are dynamically routed with minimum path similarity or not.

The data packets are generally transmitted through different nodes of the network to reach the destination. The destination node will be collecting all the data packets from its neighboring nodes. The message to be sent is divided into number of packets. The source node will be distributing all the packets to different neighboring nodes from the list of next hops by considering the history. In general, the minimum packet size is 64 bytes. Maximum packet size or maximum transmission unit (MTU) is about 1.5KB. An Ethernet LAN typically will have a maximum transmission unit (MTU) of 1500. However, this may be lowered by a router. The packet size has the most profound effect on the number of packets sent across the network. Here whatever the packet size and number of packets may be, no two consecutive packets will take the same path. Suppose, the complete data to be sent is divided into 10 packets and the possible next-hops are 8. 8 packets will be delivered to 8 different nodes and the remaining 2 will be sent through two different nodes among the available next hops. Care has to be taken such that the path similarity is minimal. If the receiver can get a clarification that the packets are dynamically routed, our work is done.

Each computer will have a unique address to communicate with each other. In order to enable the computers to communicate with each other on a network, the concept of the hostname is included. The hostname was just a simple string of alphanumeric characters and a hyphen can also be used.

Now it is a Fully Qualified Domain Name (FQDN) that absolutely and uniquely identifies every computer connected to the Network. Example of the hostname is: student-2883f53.An Internet Protocol

Address (IP address) is also a unique identifier for a computer or device on a TCP/IP network or a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number among the four can be zero to 255. For example, 1.180.20.120 could be an IP address.

We propose that if the Host Name or the IP Address of the node which is the first hop from the source is printed along with the data packet delivered through it, the receiver can ensure that the data packets are received in a secured way i.e. through different paths.

Since IP Address is rather difficult to remember as they are not particularly descriptive, we can specify a computer by a Host Name rather than a number string. It is preferred to print Host Name along with the data packet.

If this is implemented, the received data will be as follows,[host name 1][data in the first packet] [host name 2][data in the second packet]……………… [host name n] [data in the last packet].

By this an assurance that the data packets received are dynamically routed with minimum path similarity can be achieved.

IV. CONCLUSION

This paper has proposed a way in which confirmation of secured data transmission is done. If our proposal is implemented, a receiver can know that the data received by him has got transmitted in a secure manner. i.e. each packet is delivered to the target through multiple paths. So, no intruder can get the complete data. This can be achieved if the host name of the node which is the first hop from the source of each packet is printed along with the data packet transmitted through it. This is the Relied Security for Dynamically Routed Data.

ACKNOWLEDGEMENT

I am very much thankful to my employer institute, Kakatiya Institute of Technology and Sciences for providing me with all the facilities which helped me in publishing this paper.

REFERENCES

[1] Chin-Fu Kuo, Ai-Chun Pang, and Sheng-Kun Chan, "Dynamic routing with security considerations", IEEE, 2009.

[2] A.Tsirigos, Z.J. Haas , " Multipath routing in the presence of frequent topology changes", IEEE Communication Magazine, Nov 2001

[3] S.-H. Liu, Y.-F. Lu, C.-F. Kuo, A.-C. Pang, and T.-W. Kuo, "The Performance Evaluation of a Dynamic Configuration Method over IPSEC," Proc. 24th IEEE Real-Time Systems Symp.: Works in Progress Session (RTSS WIP), 2003.

[4] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, "Securing ElectronicCommerce: Reducing the SSL Overhead," IEEE Network, 2000

[5] S. Bohacek, J.P. Hespanha, K. Obraczka, J. Lee, and C. Lim,"Enhancing Security via Stochastic Routing," Proc. 11th Int'l Conf.Computer Comm. and Networks (ICCCN), 2002.

[6] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On PowerLawRelationships of the Internet Topology," Proc. ACM SIGCOMM'99,pp. 251-262, 1999.

[7] I. Gojmerac, T. Ziegler, F. Ricciato, and P. Reichl, "Adaptive Multipath Routing for Dynamic Traffic Engineering," Proc. IEEE Global Telecommunications Conf. (GLOBECOM), 2003.

[8] J.F. Kurose and K.W. Ross, "Computer Networking—A Top-Down Approach Featuring the Internet". Addison Wesley, 2003.

[9] V.I. Levenshtein, "Binary Codes Capable of Correcting Deletions,Insertions, and Reversals," Soviet Physics Doklady, vol. 10, no. 8,pp. 707-710, 1966.

[10] W. Lou and Y. Fang, "A Multipath Routing Approach for SecureData Delivery," Proc. IEEE Military Comm. Conf. (MilCom), 2001.

[11] W. Lou, W. Liu, and Y. Fang, "SPREAD: Improving Network Security by Multipath Routing," Proc. IEEE Military Comm. Conf.(MilCom), 2003.

[12] C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proc. ACM SIGCOMM '94, pp. 234-244, 1994.

[13] Secure Sockets Layer (SSL), http://www.openssl.org/, 2008.

[14] Cisco Systems, White Paper: EIGRP, Sept. 2002.

[15] R. Thayer, N. Doraswamy, and R. Glenn, "IP Security Document Roadmap, Nov. 1998.

[16] The Network Simulator-ns2, http://www.isi.edu/nsnam/ns/, 2008.

Biography

I am Suma Patra. I am a Master of Technology in Software Engineering. At present I am working as Assistant Professor in Kakatiya Institute of Technology & Sciences, Warangal since 1 year. I have the teaching experience of 2 years. I am very much interested in the area of network security.