Journal of Computer Science 4 (7): 565-570, 2008
ISSN 1549-3636

A New Enhancement for Security Mechanism in Routers

[1]Khalid Khanfar, [2]Riyad Khanfar, [3]Walid Al-Ahmad and [4]Eyas El-Qawasmeh
[1]Computer Information Systems Department, Ahlia University, Bahrain
[2]Computer Information Systems Department, Al-Quds Open University, Palestine
[3]School of Engineering and Technology, NYIT Amman, Jordan
[4]Computer Science Dept., Jordan University of Science and Technology, Jordan

Abstract: Problem statement: Routers are very important components in any network. They control and organize the in-bound traffic and the out-bound traffic. Controlling a router by an intruder leaves the entire network unsecured. In different studies, Router security was discussed from different aspects such as the routing protocol, the firewall. In this research, we present a new effective security mechanism for routers depending on the packet structure. **Approach:** Our approach in the new security mechanism is based on the utilization of the unused bits in the packet structure that have been left for future use. These unused bits will be used for security purposes to increase the protection level along the path between various routers between networks. **Results:** In the proposed approach, the router represents a manager that can take security decisions and coordinate between the operations that are related to both the packet and the routing table, both of which will assume a new structure. Achieving integration between these main routing components will make the routing of information more secure. **Conclusions/Recommendations:** From the analysis, we see that the proposed mechanism takes the communication security a step further without extra cost and effort and this is because we have used the unused bits that are already exist in the packet header.

Key words: Security, routers, routing table, packet structure.

INTRODUCTION

The network is an environment in which users exchange data through specific paths. This data can be vulnerable to many types of threats such as intruders who attempt to enter into these paths and perform illegal activities when they have the appropriate opportunity for DOIng that. In computer networks, data must be directed more carefully. Networks are actually composed of a collection of LANs that are interconnected.

Routers take network data messages from a LAN and convert them into packets suitable for transmission through a Wide Area Network (WAN). The goal is almost always to get these packets to another LAN and ultimately to the correct host on that LAN.

The role of a router becomes very important in modern networks, because routers provide services that are essential to the correct and secure operation of the networks they serve. One of the most important decisions made by a router is about where to send these packets according to the routing information that exists within the packet headers and a table of routes maintained within the router. Routers must also continuously update the changes made on these routing tables.

Securing data transfer between networks needs integrated techniques and procedures to provide the highest level of protection against many of the threats that may occur. One of the most dangerous threats is the attacks against the routing operations and routing devices. These include froged routing information, attempt to modify legitimate routing messages sent by other nodes, or attempt to exploit mechanisms in the routing algorithm. Therefore, a secure routing algorithm has become a very significant issue.

MATERIALS AND METHODS

Many studies have been done on routing security. Next is a brief description of some of these studies.

Zhang[1] show that the major concern about BGP security is that malicious BGP routers can arbitrarily falsify BGP routing messages and spread out incorrect routing information. However, one type of attack, which we term as the selective dropping attack, has

Corresponding Author: Khalid Khanfar, Computer Information Systems Department, Ahlia University, Bahrain

been largely neglected in literatures. A selective dropping attack occurs when a malicious router intentionally drops incoming and outgoing UPDATE messages, which results in data traffic being black holed or trapped in a loop.

Chen[2] proposed a mechanism to identify the characteristics in attack detection algorithms and attack responses where these responses are coming from network-based points.

Yun[3] propsed a new model based on multi-objective programming for solving multicast routing problem in computer network. A Genetic Algorithm is also proposed to solve the model.

Hu[4] presented new mechanisms as tools for securing the distance vector routing algorithm and for the path vector routing protocols.

Singh[5] suggested the integration of some useful additional information along-with intrusion detection systems and virus monitors into firewalls. They have done this to create what is called an enhanced firewall.

Seifedine[6] proposed a secure design and implementation of a network and system using windows environment.

Christian[7] developed tools focused on measuring the quality of the network by performing daily sampling of hundreds of web connections to get a real time evaluation.

Naganand[8] discussed different areas that are used in internet security. The discussed One-Way Functions and Trap Dors, One-Way Hash Functions, and different algorithms that are used in Symmetric Cipher and asymmetric Cipher.

PROPOSED ALGORITHM

We propose a security mechanism that supports the authentication and security along the communication path between the two routers (sender and receiver). Such a security mechanism can be done by an algorithm on a router. This algorithm manipulates both the packet and the routing table. The proposed algorithm is based on the following ideas:

- How to invest the padding field within the packet structure to provide more security efficiency through the router.
- Add a new field (column) to the routing table whose values are computed based on the result derived from the decryption of the packet status message field flag AN within the packet.
- How the router will manage the analysis of the packet and then build the enhanced routing table and cryptography algorithm number table. The final decision taken by the router depends on the new results.

Modified packet and routing table structures: We divided the work of the proposed mechanism into two parts. The first part works at the packet level and the second part works at the level of the routing table. We also show how the two parts are integrated together to cater for the new security mechanism.

The packet level: There are unused bits in the packet structure as shown in Fig. 1. Most of these unused bits are reserved for future use. The Unused Bits can be used and investigated to enhance the security of the routing mechanism and the level of authentication that can protect the network against attackers. This will also help to discover the attackers who attempt to enter the path between the routers to launch their attacks.

In our work, we propose that these bits within the padding field (32 bits) can be investigated as shown in Fig. 2:

- Cryptography Algorithm Number (AN) = 2 bits (represent 4 choices)
- Packet Status Message (PSM) = 14 bits (Variable, Max = 14 bits)

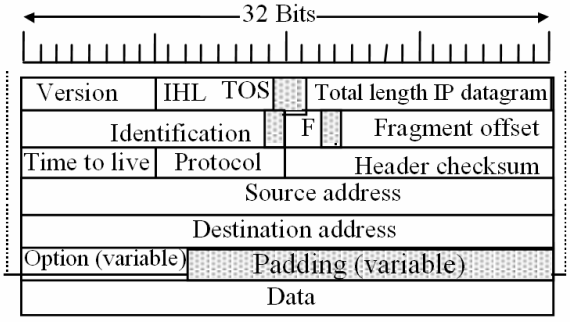

Fig. 1: Packet structure with unused bits IPV4)

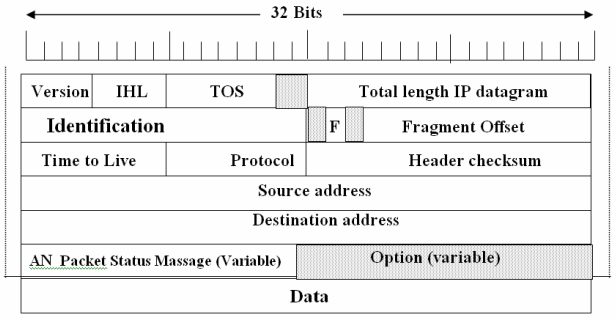

Fig. 2: The new packet structure with a packet status message field with flag (an)

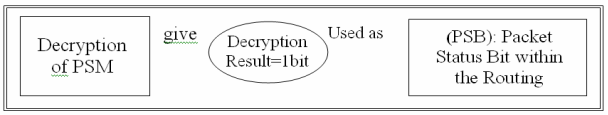

Fig. 3: Relationship between PSM in the packet and PSB in routing Table

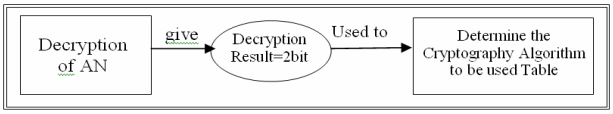

Fig. 4: Relationship between AN in the packet and the cryptography algorithm number Table

Table 1 : Cryptography algorithm number table structure

Using cryptography Algorithm No.	Algorithm Mode
1	00
2	01
3	10
4	11

Table 2: An example for our proposed routing table structure

Source address	Destination address	Next-hop	Cost	PSB
192.168.1.0	192.168.5.0	A	20	1
192.168.3.0	10.3.1.0	B	50	1
10.1.1.0	10.2.1.0	C	10	0
10.1.4.2	192.168.4.1	D	90	1
192.186.10.3	192.186.10.5	E	70	1
10.1.3.1	192.186.2.1	F	15	1

We notice that the data field of the packet header of the IPV4 protocol consists of two parts: the option part which is of variable length, and the padding part which is also of variable length. The total length of these two parts is 32 bit. These 32 bits are unused bits. Figure 1 explains the packet structure with the unused bits in the IPV4 protocol.

Decryption of PSM will be 0 or 1, and this bit (0 or 1) will be sent to and filled in the PSB (packet status bit) column within the new proposed routing table (Table 2) and then used as shown in Fig 3.

If the PSB result value is 0 by the meaning of (decryption =! Encryption), we named that negative decryption, and if the PSB result value is 1 by the meaning of (decryption=encryption), we named that positive decryption.

As shown in Fig. 4, we proposed the AN field within our new proposed packet structure consisting of encrypted message, and when this message is decrypted, the decryption result will give two bits (00, 01, 11, 10) which will be sent to and filled in the new proposed cryptography algorithm table shown in Table 1, and then choose what is the cryptography algorithm mode must be used. Later this mode will be used for choosing the decryption algorithm.

Using the new packet and routing structures: Decryption of packet status message needs the secret key for the sender and receiver using symmetric cryptography.

It must be whether or not the content of PSM field is the same that is known to the receiver. PSM field in the packet is decrypted to make authentication between the sender and receiver.

Encryption of the message gives one of 4 choices (every choice represented by 2 bits as shown in Table 1) to be used by the receiver in order to determine the encryption algorithm so it can be used to decrypt the message.

This is accomplished by adding these two bits as shown in Table 1.

We propose the AN field to provide more alternatives for routers to secure its information from hacking by using more than one algorithm to encrypt and decrypt the exchanged packets.

In other words, when the router receives a packet, it finds the corresponding cryptography algorithm from Table 1 to decrypt the Packet Status Message (PSM) within the packet based on the decryption result (2 bits) of AN, which represents the cryptography algorithm that must be used by the receiver. This allows for using many different cryptography algorithms for each packet or group of packets (Table 1).

As we see in Table 1, we have 2 bits that give us four different combinations (we call them algorithm modes). By having four different modes, we can use four different encryption algorithms at the same time. This leads to make it harder to a hacker to hack our system and also it gives us enough time to detect any abnormal behavior.

As shown in Table 1, using more than one cryptography algorithm for the packet status message between two routers in the same information path will add more complexity level by which the attacker may succeed in analyzing one of them and face problem with others.

The routing table level: We are suggesting adding a new column to the routing table and naming it Packet Status Bit (PSB) as shown in Table 2.

Table 2 is an example for our proposed routing table structure

The size of the Packet Status Bit (PSB) value is one bit only (0 or 1). By using only one bit, a small

space will be used which leads to a low processing time.

This security bit is used in the Routing Table 2 to determine which paths are secure to transfer secure packets over it and to discover the hacking attempts through the path.

Before filling out the value (0 or 1), derived from the decryption operation, into the PSB column in the routing Table (Table 2), the router checks, through its software, every PSB value in the Packet Status Bit column within the Routing Table 2 in order to check if a hacking attempt exists.

The following steps show how we use the PSB bit in Table 2 to find out about the existence of any hacking attempts

- IF (PSB) value is empty (i.e. no data founded in PSB), then no hacking attempts. This means that it is a secured path.
- IF (PSB) value is NOT-empty then the router has found data in PSB (before filling the Decryption result by the Router). This means that there is a possibility of hacking. This scenario can be determined by the following:
- Failed if value of PSB = 0, it means that a hacker attempted to decrypt the PSB but his attempt failed (Dec! = Enc), i.e., the decrypted value is different than the encrypted one
- Successful if value of PSB = 1, it means that a hacker attempted to decrypt the PSB and his attempt was successful (Dec = Enc)

Therefore, there are two cases that should be handled by the router based on the fact that whether there was a hacking attempt or not.

- If Decryption = Encryption: [give (1) = PSB]
- If Decryption! = Encryption: [give (0) = PSB]

These PSB values will be filled in Table 2.

Example: Suppose that the router has received a packet, first the router decrypts the AN which contains two bits representing the algorithm number AN. Recall, AN is used to determine which algorithm must be used by the receiver to decrypt the message (PSM). The two bits are then filled into the algorithm number Table (which is Table 1).

Hence, we can use four types of cryptography algorithms:

- If the Decryption result of AN = 00 then use Algorithm No 1
- If the Decryption result of AN = 01 then use Algorithm No 2
- If the Decryption result of AN = 10 then use Algorithm No 3
- If the Decryption result of AN = 11 then use Algorithm No 4

After the decryption of the packet status message by using one of selected cryptography algorithms, one of two values will be derived and filled into the new routing table (Table 2) column, the PSB column (Packet status bit).

The value that is generated and directly filled will be either (1) if the decryption of packet status message is positive or (0 if the decryption of packet status message is negative. We named this value (Packet status bit).

The Router will use the result bit (Packet Status Bit) that is automatically and directly generated after the decryption of the message (1 or 0). This bit value is stored in a variable and then put into the (PSB) column in the proposed routing table column (Table 2). This column is the last component of our proposed routing table, the main part of it. So, the routing operations will be incomplete and will not continue until this value is filled into Table 2 after the decryption of the message (no spaces are allowed in any part of the routing Table, especially the packet status column).

It is very important for a router to check if there is any value in the Packet Status Bit column before filling the decryption result of the (PSM). This means that if there was any value (0 or 1) previously filled, there was a hacking attempt. This attempt can be:

- Failed if the existed bit value is (0), or
- Successful if the existed bit value is (1).

The number of these values, i.e., 0s and 1s = number of unsuccessful and successful hacking attempts, respectively.

According to the packet status bit value (0 or 1), the router will make many decisions as will be illustrated next.

Case one: If there are no hacking attempts (no intruder) the following will happen:

- The PSB value derived from the decryption of the Packet Status Message within the received packet is stored in the PSB column of the Routing Table 2 by the router, as soon as the decryption operation ended and directly after checking the existence of hacking attempts.

- After checking (testing) the value of PSB and if there is no value in PSB, the next step is to decrypt the packet status message. There are two possibilities as shown in Table 3:

Positive decryption: If [Encryption = Decryption], then set the value of PSB to 1 in the Routing Table (Table 3) and notify the sender that the path is secure to continue sending data through this path.

Table 3: An Example of the Proposed Routing Table Structure

Source Address	Destination address	Next-hop	Cost	PSB
192.168.1.0	192.168.5.0	A	20	1 Enc = Dec
192.168.3.0	10.3.1.0	B	50	1
10.1.1.0	10.2.1.0	C	10	0 Enc! = Dec
10.1.4.2	192.168.4.1	D	90	1
192.186.10.3	192.186.10.5	E	70	1
10.1.3.1	192.186.2.1	F	15	1

Negative decryption: if [Encryption! = Decryption], then set the value of PSB to 0 in the Routing Table and notify the sender that there is something wrong in the path and thus retransmit packet.

Case two: If there is hacking attempts (possible intruder and path is not secure), the following will happen.

If the Router find any a value (0 or 1) stored in PSB, the router must send the sender an acknowledgment that the path is not secure and that it should select another path.

RESULTS AND DISCUSSION

There are many metrics that can be used by the routing algorithms to determine the best path that the packet must going through to arrive the desired destination. The path bandwidth between source and destination is an example about these metrics by which the routing algorithms can know the optimal path to be used.

In addition to the main components, there are other information can be added to the Routing Tables relating to determine the optimal routes by making comparison between many metrics which is differ regarding the routing algorithm design.

A router can use a set of metrics, depending on the contents of the table and its routing algorithm, to compare routes and to determine the best path to a destination by using of the routing information within the routing tables.

Router algorithms attempt to determine the best path according to many metrics and the term best is ranging among, cheapest, fastest, most reliable. This research work adds a new parameter to the routing table related to security.

In addition to all other metrics, we propose an extra metric which is the security metric. This metric is very important in the environment in which communications take place, especially the Internet.

CONCLUSIONS

Security considerations are very important and sensitive part of the routing infrastructure security in modern networks. We must create more and more innovated algorithms for securing paths through which data transferred between routers. This study presented a security mechanism that can be implemented by routing algorithms. We believe that the proposed mechanism can be implemented without undue costs and efforts. The proposed security mechanism requires modifying the packet and routing table structures along with the integrity between them.

REFERENCES

1. Ke Zhang, Xiaoliang Zhao and Wu, S.F., 2004. An analysis on selective dropping attack in BGP. The Proceedings of IEEE International Performance Computing and Communications Conference, pp: 593-599, DOI: 10.1109/PCCC.2004.1395106 http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1395106
2. Li-Chiou Chen, Thomas A. Longstaff and Kathleen M. Carley, 2004. Characterization of defense mechanisms against distributed denial of service attacks. Comput. Security, 23: 665-678. DOI:10.1016/j.cose.2004.06.008
3. Yun Pan, Zhenwei Yu, and Licheng Wang 2003. A Genetic Algorithm for the Overlay Multicast Routing Problem. Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, pp: 261, Bookmark:http://DOI.ieeecomputersociety.org/10.1109/ICCNMC.2003.1243054
4. Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003. Efficient Security Mechanisms for Routing Protocols," , The 10th Annual Network andDistributed System Security Symposium, San Diego, California 2003. URL:http://www.isoc.org/isoc/conferences/ndss/03/abstracts.shtml

5. Singh, U.K., A.K. Ramani N.S. Chaudhari, 2005. On analysis and design of the enhanced firewall for ntranet security. J. Comput. Sci., 1: 290-295, April 2005. URL:http://www.scipub.org/fulltext/jcs/jcs12290-295.pdf ISSN:15493636
6. Seifedine Kadry, Wassim Hassan, 2008. Design and implementation of system and network security for an enterprise with worldwide branches. J. Theoretical Applied Inform. Technol., 4: 111-118. http://www.jatit.org/volumes/fourth_volume_2_2008.php
7. Christian Huiteme , 1999. Routing in the Internet. 2nd Edn., Prentice-Hall, PTR, ISBN: 0130226475. http://www.amazon.com/Routing-Internet-2nd-Christian-Huitema/dp/0130226475
8. Naganand Doraswamy, and Dan Harkins, IPSec, The New Security Standard for the Internet. Itranets and Virtual Private Networks. 2nd Edn., Prentice-Hall, USA. http://www.amazon.com/gp/reader/013046189X/ref=sib_dp_pt#reader-link