A New Way Towards Security in TCP/IP Protocol Suite

M.ANAND KUMAR, M.HEMALATHA, P.NAGARAJ AND S.KARTHIKEYAN

Karpagam University
Pollachi Main road
Eachanari Post, Coimbatore
Tamil Nadu, INDIA

Department of Electronics and Computer Engineering
Caledonian College of Engineering
(University College)
(Affiliated with Glascow University, Scotland, UK)
CPO Seeb - 111

Abstract-**Internet Control Message Protocol is a protocol which is mainly used to provide information relating to errors on networked machines. Considering the few controls that IP protocol carries out, it not only allows errors to be corrected but also informs the protocols of neighboring layers of these errors. So, ICMP protocol is used by all routers, who use it to indicate an error (called a Delivery Problem). ICMP error messages are sent over the network in a datagram form, like any other data. So, the error messages themselves can be subject to errors. ICMP messages are used by the network administrators for troubleshooting the networks. Even though this protocol has many advantages, there are some of the flaws such as security,which is a major concern to be considered and to be eliminated. In this paper, we present an existing scenario and provide the authentication mechanism for ICMP messages. We also propose enhanced Packet format for ICMP message in such a way that authentication can be done. Kerberos algorithm is used for authentication mechanism which uses private key encryption method.**

***Keywords*— Network Security, ICMP, Router Security, Source Quench, TCP/IP, Troubleshooting.**

I. INTRODUCTION

The Internet Control Message Protocol is a typical instance of a client server application. Internet Protocol is the base of the TCP/IP protocol suite, since it is the mechanism responsible for delivering datagram. Three major characteristics that describe IP's datagram delivery method are connectionless, unreliable and unacknowledged. IP is a connectionless which means that the datagram's are just over the internetwork without any initial connection establishment. Because of this no assurance will be given to datagram delivery and no acknowledgement is sent back to the sender indicating the arrival of the datagram in the destination.. So It seems like it would result in a protocol that is difficult to use and impossible to rely on, and therefore a poor choice for designing a protocol suite. However, even though IP makes no guarantees, it works very well in most of the time, IP internet works are sufficiently robust that messages get delivered at the right place.

The two Scarcity of IP Protocol are namely lack of error control and lack of assistance mechanisms. The IP Protocol has no error reporting or error correcting mechanisms. Then, what happens if some thing goes wrong? And what happens if a router must discard a datagram since it cannot find a router to a final destination or time to live field has a zero value?What happens if the final destination host discards all fragments of a datagram because it has not received all the fragments in within a predetermined time limit? These are examples of situations where an error has occurred and the IP Protocol has no built in mechanism to notify the original host.[1]

The IP Protocol also lacks a mechanism for host and management queries. A host sometime needs to determine if a router or another host is alive and some times network manager needs information from another host or router. Even the best-designed system still encounters problems, of course. Incorrect packets are occasionally sent, hardware devices have problems, routes are found to be invalid, and so forth. IP devices also often need to share specific information to guide them in their operation, and to perform tests and diagnostics. However, IP itself includes no provision to allow devices to exchange low-level control messages. Instead, these features are provided in the form of a "companion" protocol to IP called the Internet Control Message Protocol (ICMP).

II INTERNET CONTROL MESSAGE PROTOCOL

ICMP is a very important part of the communication between hosts on IP networks. The ICMP server executes on all IP end system computers and all IP intermediate systems (i.e. routers). The Protocol is used to report problems with delivery of IP datagram's within an IP network. It can be used to show details like when a Particular End System (ES) is not responding, when an IP network is not reachable, when a node is overloaded, when an error occurs in the IP header information, and so on. The protocol is also frequently used by Internet managers to verify correct operations of End Systems (ES) and to check that routers are correctly routing packets to the specified destination address. Internet Control Message Protocol is a network layer protocol. Even though it belongs to network layer, its messages are not passed directly to data link layer. Instead massages are first encapsulated inside IP datagram before going to lower layer. The value of protocol field is to indicate that IP data is an ICMP message.[2]

ICMP is connectionless because it does not require hosts to handshake before establishing a connection. Connectionless protocols have advantages and disadvantages. The main advantage of connectionless protocols is less overhead: These protocols do not have the overhead of establishing a connection before sending a simple communication error message. The main disadvantage of connectionless protocols is that delivery of ICMP messages is not guaranteed. If an ICMP message gets lost in transmission, the communication error must occur again, prompting another ICMP message to be transmitted.[1]

A. Operation of ICMP:

ICMP is a protocol that defines control messages. It primarily deals with providing a mechanism for any IP device to send control messages to another device. Various types of messages are defined in ICMP that allow different types of information to be exchanged. Consider the following figure here ICMP message is generated by router R2, in response to message sent by the host sys A to sys B and forwarded by R1. This message for instance, could be generated if the MTU of the link between R1 and R2 is smaller than size of the IP packet, and the packet has the Don't Fragment (DF) Bit set in the IP packet header. The ICMP message is returned to Sys A, since this is the source address specified in the IP packet that has the problem

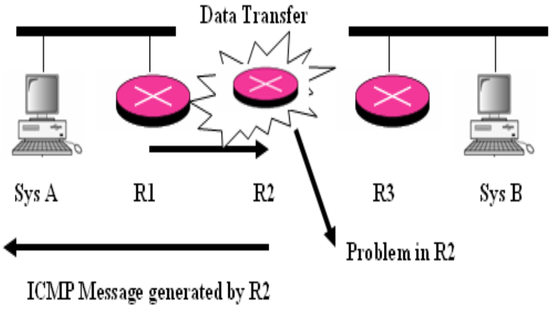


Fig. 1. Operation of ICMP Protocol

The general format of ICMP messages is shown below.

Type	Code	Checksum
Rest of Header		
Data section		

Fig. 2. General Packet Format of ICMP Messages

Type: Identifies the ICMP message type. For ICMPv6, values from 0 to 127 are error messages and values 128 to 255 are informational messages. Code: Identifies the “subtype” of message within each ICMP message Type value. Thus, up to 256 “subtypes” can be defined for each message type. Checksum: 16-bit checksum field provides error detection coverage for the entire ICMP message. Message Body: Contains the specific fields used to implement each message type.[2].

III RELATED WORK

Several attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets. Denial of service attacks primarily use either the ICMP "Time exceeded" or "Destination unreachable" messages.[3] The "Time exceeded" message indicates that the Time-To-Live field in the IP header has expired; this can normally be caused by routing loops or trying to reach a host that is extremely distant. "Destination unreachable" messages can have several meanings (based on a sub-field in the ICMP message), but all basically indicate that packets cannot successfully be sent to the desired host. Both of these ICMP messages can cause a host to immediately drop a connection (this is the desired result if the ICMP message is legitimate). An attacker can make use of this by simply forging one of these ICMP messages, and sending it to one or both of the communicating hosts. Their connection will then be cut ICMP messages can also be used to intercept packets. The ICMP "Redirect" message is commonly used by gateways when a host has mistakenly assumed that the destination is not on the local network (and thus attempting to send the packet via the gateway to). If an attacker forges an ICMP "Redirect" message, it can cause another host to send packets for certain connections through the attacker's host. This attack is similar to a RIP attack, except that ICMP messages only apply to existing connections, and the attacker (the host receiving redirected packets) must be on a local network [6].

ICMP messages may be subject to various attacks. ICMP messages may be subject to actions intended to cause the receiver to believe that the message came from a different source from that of the message originator. The protection against this attack can be achieved by applying the Authentication mechanism ICMP messages may be subject to actions intended to cause the Message or the reply to it to go to a destination different from that of the message originator's intention. ICMP messages may be subject to changes in the message fields or payload. The authentication or encryption of the ICMP message protects against such actions. ICMP messages may be used to attempt denial-of-service attacks by sending back to back erroneous IP packets [7].

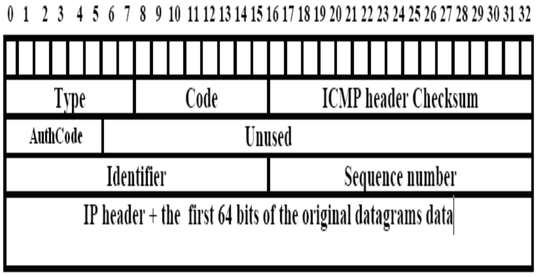


Fig. 3. Modified Packet Format

The IP header is organized in such a way that there are many marked and many unused bits. All those bits can be used to store information, that is, to create covert channels. This technique is similar to hiding information on system that do not occupy all "real" disk space [8]

IV PROPOSED WORK

The above mentioned problems can be solved by providing the authentication mechanism to ICMP Messages. The proposed method includes an extra field AuthCode in the ICMP message format. The unused portion of the ICMP packet can be used for this purpose. In this message format the Type field identifies the ICMP message type. For ICMPv6, values from 0 to 127 are error messages and values 128 to 255 are informational messages. Code field identifies the "subtype" of message within each ICMP message Type value. Thus, up to 256 "subtypes" can be defined for each message type. Checksum field is a 16-bit checksum field provides error detection coverage for the entire ICMP message.. Message Body: Contains the specific fields used to implement each message type. The AuthCode field contains the Secret key which is generated by Kerberos authentication algorithm. If there is any problem in the network, the ICMP message will be generated by the host or router based on the nature of the problem. The ICMP message reaches the source machine, and then the source by using Authcode it knows the actual reason for the message. In between this if any person tries to retrieve the information such as source address, destination address, network address he will not be able to access any information unless he knows the authentication code.

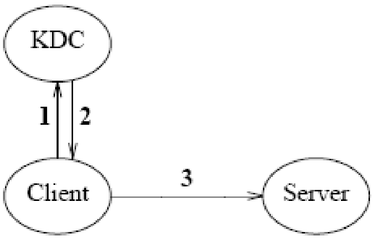
A. Algorithm

Kerberos algorithm is used here to provide the authentication for the ICMP Messages. The method that can be used for limiting an attacker's spoofing abilities is to add authentication onto the application layer. Of course, just adding authentication is not enough without adding encryption; otherwise, after some initial application-level authentication, a hijacking attack may still be successful. An authentication between two parties which exchanges a session key, however is secure; even though the IP packets transmitted back and forth are not individually authenticated, they are all encrypted with the secure session key. This scheme is the goal of the Kerberos Authentication System, developed at MIT. The Kerberos system uses cryptographic authentication algorithms to ensure that a user is really who s/he claims to be, and once this is established, an exchanged session key is used to encrypt all transmissions of whatever service the user has requested. Without knowledge of this session key, it is impossible for an attacker to spoof meaningful transmissions between sources. Since this key is generated based on secret keys known only to the actual user and the trusted server, it is very hard for an attacker to acquire. The Kerberos system is resilient to replay attacks as well. Kerberos is generally considered to significantly increase the security of a network [11]

B. Working Scenario

The following figure shows the messages† required for a client to prove its identity to a server. A typical application uses this exchange when it first establishes a connection to a server. Subsequent connections to the same server require only the final message in the exchange. In the first message the client contacts the KDC, identifies itself, presents a nonce, and requests credentials for use with a particular server. Upon receipt of the message the KDC selects a random encryption key Kc,s , called the session key, and generates the requested ticket. The ticket identifies the client, specifies the session key Kc,s , lists the start and expiration times, and is encrypted in the key Ks shared by the KDC and the server. Because the ticket is encrypted in a key known only by the KDC and the server, nobody else can read it or change the identity of the client specified within it. The KDC next assembles a response, the second message, which it sends to the client. The response includes the session key, the nonce, and the ticket. The session key and nonce are encrypted with the client's secret key Kc

Upon receiving the response the client decrypts it using its secret key. After checking the nonce, the client catches the ticket and associated session key for future use. In the third message the client presents the ticket and a freshly-generated authenticator to the server



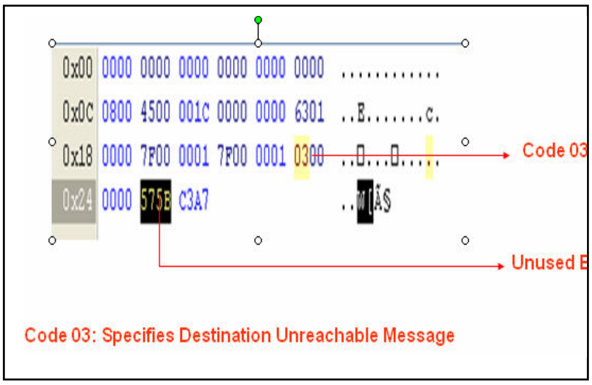
1. Client → KDC: c, s, n
2. KDC → Client: $\{K_{c,s}, n\}K_c, \{T_{c,s}\}K_s$
3. Client → Server: $\{A_c\}K_{c,s}, \{T_{c,s}\}K_s$

(In version 4, message 2 is $\{K_{c,s}, n, \{T_{c,s}\}\ K_s\}K_c$)

Fig. 4. Kerberos Key exchange

The authenticator contains a timestamp and is encrypted in the session key Kc,s . Upon receipt the server decrypts the ticket using the key it shares with the KDC and extracts the identity of the client and the session key Kc,s . To verify the identity of the client, the server decrypts the authenticator and verifies that the timestamp is current. Successful verification of the authenticator proves that the client possesses the session key Kc,s ,which it only could have obtained if it were able to decrypt the response from the KDC. Since the response from the KDC was encrypted in Kc , the key of the user mentioned in the ticket, the server may reasonably be assured that identity of the client is in fact the principal named in the ticket. If the client requests mutual authentication from the server, the server responds with a fresh message encrypted using the session key. This proves to the client that the server possesses the session key, which it could only have obtained if it was able to decrypt the ticket. Since the ticket is encrypted in a key known only by the KDC and the server, the response proves the identity of the server.[11]

With this algorithm, the secret key is generated. The secret key will be stored in Auth_code of ICMP Message. The following figure shows the modified ICMP Packet format. In that format the field called unused is present. Here the unused field is named as Auth_code in which the secret key that is generated by Kerberos algorithm is stored.



```
0x00 0000 0000 0000 0000 0000 0000  ............
0x0C 0800 4500 001c 0000 0000 6301  ..E.......c.
0x18 0000 7F00 0001 7F00 0001 0300  ..□...□.....
0x24 0000 575B C3A7                 ..W[Ã§
```

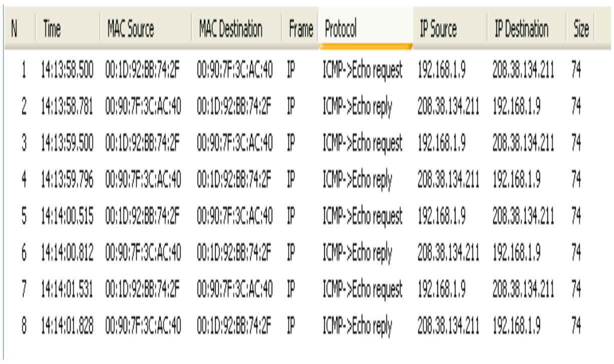
Code 03: Specifies Destination Unreachable Message

Fig. 5. Modified Packet Format with unused bits

Code 03 indicates that the message is Destination unreachable. The following Packet is created using Network simulator. It is represented in hexadecimal format. The source address used here is 192.168.1.9 and the destination address is 208.38.134.211.

V RESULTS

The ICMP packet that is mentioned above is tested in a small network that contains 150 systems. The source IP address is 192.168.1.9 and the destination ip address is 208.38.134.211. The same packet is tested for multiple source and destination using network analyzer tool and we get the following data which contains s.no, time, mac source, mac destination, frame , protocol, IP Source, IP Destination and size.



N	Time	MAC Source	MAC Destination	Frame	Protocol	IP Source	IP Destination	Size
1	14:13:58.500	00:1D:92:BB:74:2F	00:90:7F:3C:AC:40	IP	ICMP->Echo request	192.168.1.9	208.38.134.211	74
2	14:13:58.781	00:90:7F:3C:AC:40	00:1D:92:BB:74:2F	IP	ICMP->Echo reply	208.38.134.211	192.168.1.9	74
3	14:13:59.500	00:1D:92:BB:74:2F	00:90:7F:3C:AC:40	IP	ICMP->Echo request	192.168.1.9	208.38.134.211	74
4	14:13:59.796	00:90:7F:3C:AC:40	00:1D:92:BB:74:2F	IP	ICMP->Echo reply	208.38.134.211	192.168.1.9	74
5	14:14:00.515	00:1D:92:BB:74:2F	00:90:7F:3C:AC:40	IP	ICMP->Echo request	192.168.1.9	208.38.134.211	74
6	14:14:00.812	00:90:7F:3C:AC:40	00:1D:92:BB:74:2F	IP	ICMP->Echo reply	208.38.134.211	192.168.1.9	74
7	14:14:01.531	00:1D:92:BB:74:2F	00:90:7F:3C:AC:40	IP	ICMP->Echo request	192.168.1.9	208.38.134.211	74
8	14:14:01.828	00:90:7F:3C:AC:40	00:1D:92:BB:74:2F	IP	ICMP->Echo reply	208.38.134.211	192.168.1.9	74

Figure 6 Data from Network Analyzer

The following graph shows the status of incoming and outgoing packets of ICMP message. It shows that after the modification of ICMP Packet, there is no major time delay in sending and receiving ICMP messages. It also shows that it does not affect other protocols operations such as IGMP, TCP and UDP that operates at the time of sending and receiving ICMP packet.

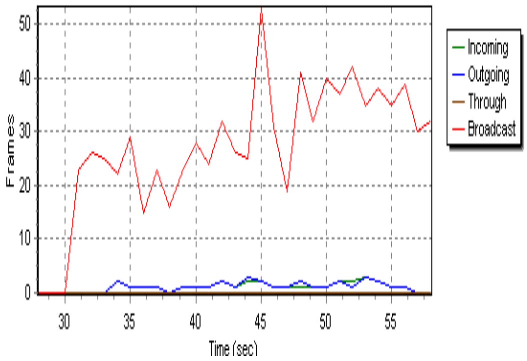


Figure 7 Analysis

It also indicates that there is no major change in the traffic when executing the proposed ICMP packet. It shows that 80 frames of ICMP protocol is transmitted at the time of testing. The 29 frames of TCP and 89 frames of IGMP are transmitted during the testing.

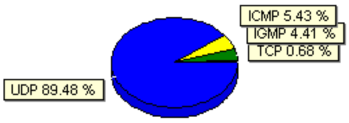


Figure 8 Graph showing percentage

VI. CONCLUSION

In this paper, we presented the existing security flaws in the TCP/IP Protocol especially in ICMP Protocol and how to provide the authentication mechanism for ICMP messages. We also propose enhanced Packet format for ICMP message in such a way that authentication can be done. Kerberos algorithm is used for authentication mechanism which uses private key encryption method. Using Network Simulator-2 we have created the suggested ICMP Message. It is tested in a suitable environment. The result shows that there is no major effect in the performance of the network after the modified packet is executed over the network. With this the ICMP message can be used for trouble shooting network in a secured manner with art affecting the performance of the network.

ACKNOWLEDGMENT

I acknowledge my thanks to our Chancellor Dr.R.Vasanthakumar, Advisor and Registrar for their encouragement and motivation to complete this work as successful one.

REFERENCES

[1] Behrouz A. Forouzan, ”TCP/IP Protocol Suite”,.3rd Edition. New Delhi: Tata McGraw Hill Publication. 2003

[2] Buck Graham. “TCP/IP Addressing”, 2nd Edition, Harcount India Private Limited, New Delhi, 2007.

[3]. Andrews S. Tanenbaum. “Computer Networks”. 4th Edition, New Delhi: Prentice Hall of India Private Ltd, 2003.

[4]. M. Anand Kumar, K. Appathurai, P.Nagarajan, “Troubleshooting Networks using Internet Control message Protocol”, CiiT International Journal of Networking and Communication Engineering, 2009.

[5]. D. W. Davies and W. L. Price. Security for Computer Networks. ohn Wiley & Sons, second edition, 1989.

[6]. Steven M. Bellovin,” A look Back at Security Problems in the TCP/IP Protocol Suite”, AT&T Labs—Research, 2004.

[7] Conta Transwitch, S. Deering “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, RFC 4443, 2006.

[8] Prof. Dr. Alaa H. Al- Hamami, Mohammed A.Al-Hamami, Aseel K.Al- Noaimy,”Information hiding in ICMP Protocol”, AL-Rafidain University College,2004

[9] Richard Popa,”An Analysis of steganographic techniques”, the “Politehnica” University of timisoara, faculty of automatics and computers, department of computer science and software Engineering,1998.

[10] Mohammed A.Al-Hamami ,”Information Hiding Attack in Image “, M.sc thesis ,the informatic Institute for postgraduate Studies of the Iraqi committee for computers and Informatic ,2002

[11] www.Cmu.edu/computing/doc/software/kerberos/kerberos-pdf.pdf