Scrambling and Encrypting- Based Authenticating for Open Networks Communication

M. W. Youssef

Head of Computing and Information Division,
The SHOURA Assembly
Cairo, Egypt.

Hazem El-Gendy

Chair of CS Dept., Faculty of CS & IT
Ahram Canadian University in Egypt, and
Assistant Minister of Endowments of Egypt.

Summary:
With the increase in the importance and utilization of information, grows the importance of developing security mechanisms for the information exchanged over various types of communications networks. In this paper, we present a novel method to authenticate open communications systems by using scrambling and encryption. It involves the enhancement to the data link layer format that involves utilization of unused segments. Authentication has proven to be a deterrent to intruders and ensures that information is transmitted from trusted senders to a trusted receiver. It presents a scrambling and encrypting mechanism to authenticate information in packet headers of the data link layer, HDLC – PPP protocol.

Keywords:
Computer Communications, Computer/communications Protocols, Network Security, Authentication, Scrambling, Encryption, Standard Protocols, ISO Open System Interconnections (OSI) Model.

I. Introduction

This era is characterized by the huge growth to both the importance of information and the exchange of information among various communicating entities over different types of networks. These networks include both private and public networks. Consequently, some of these networks or some of the users of these networks cannot be trusted. This increased the importance of developing security mechanisms for the various communicating entities and communicating computers to secure the information exchanges and accessed [1-22].

In the same time, the need for open architectures and open communications systems has grown significantly. This motivated the development of systems for open communications.

In this paper, we develop authentication for open networks that is based on scrambling and encryption for layer 2.

As activities grew over open networks, hacking has always been an issue to computer security [**1**]. Intruders have been using strategic hacking to terrorize commercial and governmental entities on the internet [**2**]. Many people proposed security solution [3, 4]. Authentication has proven to be one of the best ways to secure exchanged information between computer networks nodes, especially when they are connected in an open network [**5, 6**]. Data link layer has been chosen to be the main candidate to apply that. Layer two, by nature, conveys many security features [**7**]. In several researches,

In previous work, a methodology for securing information exchange over open network by changing layer two packet structures was presented in [**8**]. In [**9**] the authors secured computers communication based on layer 2 security mechanism and finally in [**10**], the paper presented a methodology to securing computer networks communication using mac address based security mechanism. However, all the previous work proved to be quite capable of securing computer communication, it still requires a robust encryption technique to prevent intruders from breaching the system security. This paper is an extension to that work; it combines the security techniques presented in [**8, 9, 10**] with an encryption technique to harden communication authentication of the packets transmitted in a Point-to-Point Protocol (PPP).

The importance of this research stems from the facts that providing authentication on a **PPP** link is optional. Moreover, though authentication does verify that a peer is to be trusted, **PPP** authentication does not provide confidentiality of data. Accordingly, for confidentiality, robust encryption is required [**11**].

Section two presents a brief description of communication authentication. Section three discusses previous researches in communication authentication. Section four presents a description of the proposed scrambling and encryption techniques. Section five, is the paper conclusion and proposed future work.

II. Communication authentication

Computer authentication means verifying the identity of both the sending and the receiving computers to each other during remote information exchange. This is done to ensure that the packet is sent from a known safe computer to the dedicated node. That means presenting the identity of both computers on the link to each other through an authentication value.

In this research, authentication is achieved by trading authentication values, those values are encapsulated in each packet transmitted over a Point-to-Point Protocol

Manuscript received June 5, 2011
Manuscript revised June 20, 2011

(**PPP**) link. The Information field of the PPP packet encapsulates that authentication value. The sender encapsulates in packet header an authentication value that is associated with an address that is selected randomly from many stored addresses in the sending computer and known to the receiver. When a receiver receives a packet, opens the packet to get the authentication value, which reveals the original identity of the sender.

Accordingly, authentication in this research is very similar to combining both authentication protocols - Password Authentication Protocol (**PAP**) and Challenge-Handshake Authentication Protocol (**CHAP**) [**12**, **13**]. That was implemented by building for each protocol a chamber of secrets (secrets database) that contains identification information, or security credentials, for each caller that is permitted to link to the local machine. Those secrets are encrypted.

III. Previous researches in communication authentication

In previous work [**8, 9, 10**], communication security were implemented in stages, each of which, represents a layer of security. According, several layers of authentication were presented. In [**8**], securing information exchange over open network by changing layer two packet structures was described. In [**9**], securing computers communication based on layer 2 security mechanisms were presented. Finally in [**10**] securing computer networks communication using MAC address based security mechanism was discussed. The presented mechanism achieved open network security and ensured achieving the following security functions:

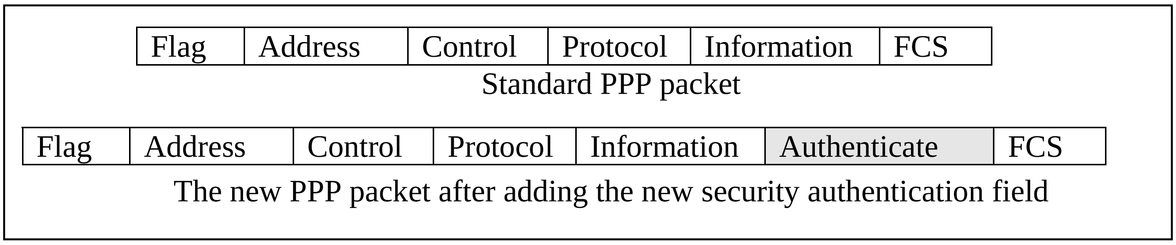
- Link establishment only between trusted nodes.
- Authenticating the nodes of the link before data transmission.
- Authenticating the sender of a PPP packet and covering the real structure of that packet (By adding a new Authenticate field to the packet).
- Changing protocol identification to prevent monitoring based on protocol by using a new protocol number.
- Only virtual addresses are transmitted over the link not real addresses to prevent impersonation of the data sender.

The point is all of them were without handmade encryption. The following sections describe that research and shows where encryption should talk place.

III.1 Securing information exchange over open network by changing layer two packet structures

This paper presented a security mechanism that aims at securing remote data exchange among network nodes by applying several layers of authentication. The security mechanism that is presented in this work was built on layer two Point-to-Point Protocol (PPP). Authentication is achieved when building new Request For Comments (RFCs) [**14**] for encapsulating data packets in a secured packet with a private authentication to meet the author’s own authentication. This is done by applying a program that uses PPP to transfer multi-protocol datagrams over point-to-point links. PPP has also authentication protocols that authenticate the two peers of the link before data transmission [**15**]. In this research a new format of PPP packet was built by adding a new field to the frame. Accordingly, the new frame is proprietary authentication field to the proposed security system.

Figure 1 shows the difference between standard PPP packet as it looks before the change and the way it looked after adding the new field to it.



Flag	Address	Control	Protocol	Information	FCS

Standard PPP packet

Flag	Address	Control	Protocol	Information	Authenticate	FCS

The new PPP packet after adding the new security authentication field

Figure 1: Comparing the standard PPP packet format with the new PPP packet

The proposed PPP packet contains an extra field that has one main function which is to “Authenticate" the packet. This field contains identification data that can decide the identity of the packet sender. The content of this field is known only to the sender of the packet and the receiver of the packet. Consequently, as a result, it provides a high level of authentication for the data exchanged across the open network.

III.2 Securing computers communication based on layer 2 security mechanisms and Securing computer networks communication using MAC address based security mechanism

In the presented security mechanism, both the sending and the receiving computers, authenticate themselves to each other during remote information exchange. This is done to ensure that the packet is sent from a known safe computer to the intended destination node. This is achieved by presenting the identity of all computers working on the network to each other. All secured communicating computer nodes addresses are encapsulated in the transmitted layer two (**HDLC**) packets.

The research utilized a connection reliability mechanism in order to do that. In TCP/IP flow control mechanism, data integrity is ensured by allowing users to request reliable data between computer nodes. In reliable transport operation, a device that wants to transmit data to another, sets up a connection-oriented communication with a remote device by creating a session which is called a "**three way handshake**". Figure 2 shows how the three-way handshake is established [**16**].

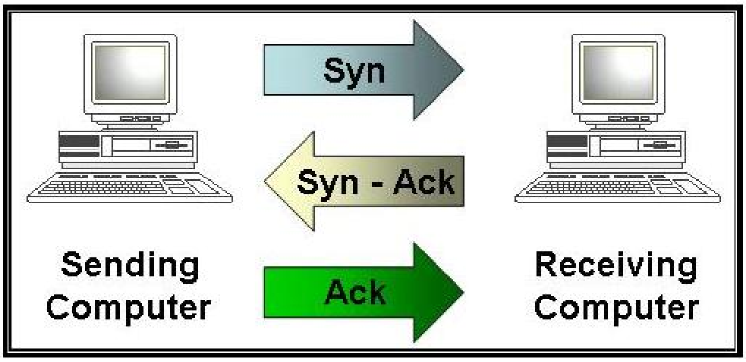


Figure 2: Steps of the Three-way handshake

Steps of the Three-way handshake are as follows:

1. The first "**connection agreement**" segment is a request for synchronization.
2. The second and third segments acknowledge the request and establish connection rules between hosts. The receiver's sequencing is also requested to be synchronized as well, so that a bidirectional connection is formed.
3. The final segment is also an acknowledgment, it notifies the destination host that the connection agreement has been accepted and that the actual connection has been established. Data transfer can now begin [**16**].

In data link layer, the problem is that each time a packet is sent between routers, it is framed with control information at the data link layer, but that information is stripped off at the receiving router and only the original packet is left completely as a whole [**16**]. That strips the packet from its authentication data. In order to overcome this problem, we include in the information field of the (**HDLC**) packet an encrypted (**MAC**) address of the sending and receiving computers which will be authenticated in the destination computer. This is done by storing every (**MAC**) address of every sending computer on the network in an authentication table in every computer on the network. When the receiving computer opens the packet and gets both (**MAC**) addresses (sender and receiver), it decrypts the addresses and verify them against its authentication (**MAC**) addresses check list.

An example of the (**MAC**) addresses lockup table is presented in table 1. In that example, the network is supposed to contain ten sending computers.

Table 1: Lookup table for (MAC) addresses of the sending computer

Computer Number	MAC Address
1	00-3F-01-CC-4D-7C
2	01-33-4E-2C-56-6A

3	00-02-5D-07-6E-DC
4	01-7F-02-5D-11-55
5	02-02-5A-B0-5D-3E
6	40-03-3A-E2-11-00
7	11-23-2B-F1-3C-DB
8	22-2D-D3-22-2D-12
9	0D-21-A1-D1-01-22
10	00-05-D2-B2-F3-E3

The security mechanism works in two phases as given in the Security_Algorithm as follows:

Security_Algorithm:

Phase one of authentication: Testing the Link

A test of the link between communicating computers must be completed before data transmission takes place, this is achieved as follows:

- A Link Control Protocol packet of type Configure-Request is sent from the sending computers.
- The Configure-Request packet is encapsulated in the Information field of the (**HDLC**) packet.
- The sending and receiving computers (**MAC**) addresses are encrypted and inserted in the Identifier field of the Configure-Request packet.
- The structure of the encapsulated Configure-Request packet is shown in figure 3 as follows:

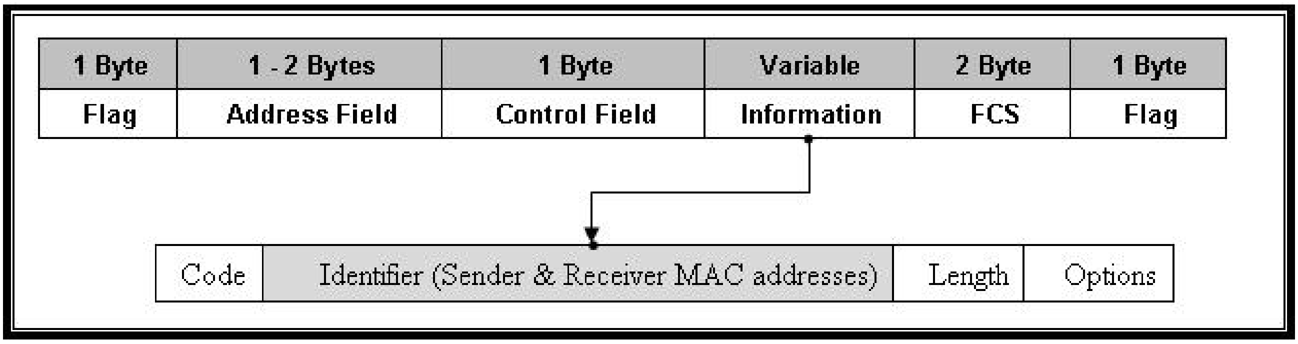


Figure 3: A Configure-Request Packet encapsulated in a (HDLC) packet

- When the destination computer receives a Configure-Request packet, it replies with a (**LCP**) packet of type Configure-Ack encapsulated in a (**HDLC**) packet to acknowledge the reception of the Configure-Request packet of the sender.
- The Identifier field of the Configure-Ack packet will also contain the (**MAC**) addresses of the sender and receiver in an encrypted form.
- At the sender computer, the Identifier field of the Configure-Request packet will be also verified by the sender. When succeeded, the sender computer sends a succeed Configure-Request packet to the destination computer using the same process.

Phase two of authentication: Authenticating the Transmission

A second phase of authentication between the communicating computers uses Challenge Handshake Authentication Protocol (**CHAP**). This phase works as follows:

- The sender computer sends a **Challenge** packet containing data intended to check the identity of the remote computer.
- The remote computer responds with a **Response** packet containing its authentication data.
- The authenticator then replies with a (**Success**) packet if the authentication process succeeds or a (**Failure**) packet if the authentication process fails.
- In our case, it is the MAC addresses of the sender and receiver which is used as the Identifier field of the Challenge packet.
- When Challenge packet is received, a (**Response**) packet is sent with the Identifier field containing the same (**MAC**) addresses in the Challenge packet.
- Similarly, the Success and the Failure packets are sent with the Identifier field containing the

same (**MAC**) address contained in the Response packet.

End_Security_Algorithm

III.3 Pitfalls and shortcomings

As noticed in all the previous work, data exchanged between communication nodes in plain clear form, which make it vulnerable to hackers. To solve this

IV.1. Data Scrambling

The first technique proposed is data scrambling. To protect the integrity of packets' contents', a data scrambling phase is run prior to data encryption phase. Data scrambling means scramble the contents of the frame of information in a random manner that cannot reveal their original manner to any attacker. Data Scrambling is implemented in the following sequence:

- A message is encapsulated in a given frame
- The whole frame is cut into equal size parts.
- These parts are rearranged in a random manner that is different from their original arrangement which cannot reveal the original text sequence of the message easily.

An algorithm is used to scramble the stream of bytes. Many algorithms for scrambling can be used [17-20]. This algorithm works as follows:
The following stream of bytes shows a frame of data:

7E FF 7D 23 C0 21 7D 21 7D 20 7D 21 7D 5E B0 7D 5D 2B 7D 20 7D 29 73 61 6C 6C 30 30 7D 20 7D 20 7D 20 7D 28 0C 7E

To scramble data in this frame:
Count the number of digits in the whole stream
Ex: here the count equals 76 digits
Cut the stream into 18 parts numbered from 1 to 18 starting from right to left of equal number of digits. This is done by dividing the length of the stream by 18 using integer division to get a result and dividing the length another time using the Modulus division in order if there is a remainder.

Ex: 76 \ 18 = 4, therefore there are 18 parts of 4 digits each,
76MOD 18 = 4, therefore there is 4 digits as a remainder part.

So, the 18 parts are to be (from right to left):

Part 1: 0C 7E
Part 2: 7D 28
Part 3: 7D 20

problem another layer of security is required, that layer could be scrambling and encrypting exchanged data.

IV. Data Encryption and Scrambling

As noticed in all the previous work, data exchanged between communication nodes in plain clear form, which make it vulnerable to hackers. To solve this problem another layer of security is required, that layer could be scrambling and encrypting exchanged data.
Part 4: 7D 20
Part 5: 7D 20
Part 6: 30 30
Part 7: 6C 6C
Part 8: 73 61
Part 9: 7D 29
Part 10:7D 20
Part 11: 5D 2B
Part 12: B0 7D
Part 13: 7D 5E
Part 14: 7D 21
Part 15: 7D 20
Part 16: 7D 21
Part 17: C0 21
Part 18: 7D 23

Remainder part is: 7E FF

3- These parts will be scrambled and arranged in a reverse order starting from left to right in the following manner so we have the stream to be:

part1 & part2 & part3& part4 & part5 & part6 & part7 & part8 & part9 & part 10 & part11 & part12 & part13 & part14 & part15 & part16 & part17 & part18 & remainder part

So, the scrambled frame will be:
0C 7E 7D 28 7D 20 7D 20 7D 20 30 30 6C 6C 73 61 7D 29 7D 20 5D 2B B0 7D 7D 5E 7D 21 7D 20 7D 21 C0 21 7D 23

and will be transmitted in this sequence.

That technique protects frame contents from being read due to the difficulty of extracting the original information. That scrambled frame cannot be unscrambled to acquire its original arrangement except by using a given unscrambling algorithm exists at the receiving user computer which is only known to the sender and the receiver.

When scrambling phase is complete, the whole message enters to a second phase for encryption.

At the receiving node, after decryption, the receiver unscrambles the frame with the reverse manner of the scrambling technique used at the sending node to scramble the frame. After unscrambling the received frame, the original frame is set back to its original arrangement that was sent with.

IV.2 Encryption

Encryption is used to prevent attackers from revealing the original written message. Encryption protects the message content to be read by any intruder and might break its integrity. Many encryption algorithms exist in the literature [21-22].

V. Conclusions

Authentication technique provided a great means towards securing connected computers in an open network. Previous effort, presented in this paper, have been put in order to secure computers communication, but all required encryption to harden the authentication mechanism.

This research presents a methodology of scrambling PPP packet datagrams and then encrypting it. This secures the authenticity of the packet when transmitted over open network. By applying the proposed techniques, a PPP packet is transmitted safely between layers, from the data link layer up to the higher layers of the TCP/IP stack until received by the remote node.

This work can be taken further by combining it with a firmware encryption box that prevent hackers from steeling sensitive information regarding the encryption mechanism from the computer node.

References

[1] J. Scambray, M. Schema, “Hacking Exposed”, Second edition, McGrew-Hill, 2002.

[2] K. M. A. Nassar, W. A. Ali, “Using Strategic Hacking To Terrorize Commercial And Governmental Entities On The Internet”, ICICT Conference, 2003.

[3] W. Stallings, ”Network Security Essentials”, Person Education Inc, second edition, 2002

[4] J. Ramachandran, “Designing Security Architecture Solutions”, Robert Ipsen, 2002.

[5] Richard E. Smith, Authentication from Passwords to Public Keys, Addison Wesley Longman, Inc.2001.

[6] Tom Arons, Paul Drobny, Bill Grabert, David Johnston, Robert Ono, Donald Stitt, Common Authentication Advanced Technology Project: Sign-on authentication, Advanced Technology Project community and University of California New Business Architecture vision of web-based Single, 2002.

[7] Data Link Layer, CSC 343·643 Wake Forest University. Department of Computer Science 2006

[8] Youssef M. W., T. Sultan and M. Helmy, "Securing Information Exchange over Open Network By Changing Layer Two Packet Structure", "International Journal of Intelligent Computing and Information Science", July 2007, Ain Shams University, Cairo, Egypt.

[9] Youssef M. W., “Securing Computers Communication Based on Layer 2 Security Mechanism", Scientific Conference on Cyber Crime and Information Security at ACU, May, 2009.

[10] Youssef M. W., "Securing Computer Networks Communication Using MAC Address Based Security Mechanism", International Conference on Cyber Crime and Information Security (ICCS) at ACU, Dec, 2010.

[11] G. Meyer, Request for Comments 1968: The PPP Encryption Control Protocol (ECP), Network Working Group, Columbus-Ohio, 1996.

[12] G. Zorn, Request for Comments: 2759: Microsoft PPP CHAP Extensions- Version 2, Network Working Group, Microsoft Corporation, 2000.

[13] W. Simpson, Request for Comments 1994, PPP Challenge Handshake Authentication Protocol (CHAP), Network Working Group, California, 1996.

[14] PPP Encapsulation: http//www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/intwork/inbb_ras_afou.mspx#top#top, 2007.

[15] W. Simpson, Request for Comments 1334: PPP Authentication Protocols. Network Working Group, California, 1992.

[16] Irvine, Edward, Understanding the Internetworking Protocol, Second Draft, April 18, 1999.

[17] Common Scrambling Algorithm, http://en.wikipedia.org/wiki/Common_Scrambling_Algorithm

[18] DVB Common Scrambling Algorithm, http://www.dvb.org/technology/standards/a011r1.pdf.

[19] Analysis of the DVB Common Scrambling Algorithm, http://academic.research.microsoft.com/Paper/2318905.aspx..

[20] Data scrambling using PHP and MySQL , http://etl-tools.info/en/examples/php_mysql-data-scrambling.htm

[21] Encryption Algorithms, http://www.mycrypto.net/encryption/crypto_algorithms.html.

[22] The Easy Explanation of Encryption Algorithms, http://www.encryptionalgorithms.org/