Securing Authentication of TCP/IP Layer Two By Modifying Challenge-Handshake Authentication Protocol

M. W. Youssef
Head of Computing and Information Centre,
The SHOURA Assembly
Cairo, Egypt.
drwagdyyoussef@yahoo.co.uk

Hazem El-Gendy
Chair of CS Dept., Faculty of CS & IT
Ahram Canadian University in Egypt,
and Assistant Minister of Endowments of Egypt.
h_elgendy@masrawy.com

Abstract

*Computer communications have been playing a vital role in the world economy. Government organizations, large companies and banks are using those networks in trading their data. This imposed a challenge due to the increasing need for protecting the sensitive data traded over those networks. This research presents a mechanism to protect computers communication over open un-trusted networks, primarily, that mechanism relies on securing communication authentication. In order to do that, the communication protection mechanism modifies the Challenge-Handshake Authentication Protocol (**CHAP**) which is responsible for the authentication of communication of layer two High-level Data Link Control (**HDLC**) protocol.*

Keywords: *Computer Security, Computer Network, Network Security, Network Protocols, Network Addressing, RFCs, Cloud Computing.*

1. Introduction

Computer networks have always been a target for malicious attacks [1]. The key of computer networks security lay within networks design [2,3]. As the TCP/IP consists of several layers [4], it was found that putting more emphasis on securing layer two presents a good approach [5]. Tat is because, securing layer two, will subsequently secure all the subsequent layers [6,7]. Layer two is responsible for communication authentication [8,9]. When designing a network security solution, authentication has always been the core of many security mechanisms [10,11] wich has a vital importance for arias such as eGovernment and eCommerce [12]. There have been several researches in networks authentication; in [13], they applied common authentication advanced technology project using sign-on authentication. In [14], they proposed an authentication approaches based on using passwords utilizing public keys. Finally in [15,16], they presented a methodology to securing information exchange over open network by changing layer two packet structure.

The layer two, Point-to-Point Protocol (PPP), was selected for this research because it can perform transmission of multi-protocol datagrams over point-to-point links [17], provide connection authentication [18], transmission encryption, and compression [19]. Additionally, PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET. PPP is also used over both, broadband connections and dial-up access to the Internet. One of the many features of the PPP is it can be used for connections over synchronous and asynchronous

circuits. Finally, an important reason for selecting the PPP is its ability to work with numerous network layer protocols, including Internet Protocol (IP), TRILL, Novell's Internetwork Packet Exchange (IPX), NBF and AppleTalk [20].

In previous work several mechanisms to secure computer communication over layer two HDLC communication protocol were presented by the authors. In [22], a mechanism for securing computer networks communication by modifying computer network communication protocols was presented. In [23], a mechanism for applying open networks communication authentication was discussed. Finally, in [24], a mechanism for applying open networks communication authentication by scrambling and encrypting layer two packet content was explained, this is similar to the research presented in [27]. This paper presents a proposed extension to that work; it presents a mechanism for authenticating computer networks connections by applying modifications to the challenge-handshake authentication protocol.

Layer two authentications can utilize either Challenge-Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP). CHAP has been selected for this research because CHAP provides more security than PAP [24]. A technique for securing computer communication by modifying the Challenge-Handshake Authentication Protocol (CHAP) is discussed in the following sections. This approach benefits from the imbedded features which make the Challenge-Handshake Authentication Protocol (CHAP) one of the highly secured procedures for connecting systems, one of those features is having identifiers change frequently and authentication can be requested by the server at any time [25].

Section two, presents the relevance to previous researches in communication authentication. Section three, presents the basis of selecting challenge-handshake authentication protocol (CHAP). Section four, contains a brief description of the challenge-handshake authentication protocol (CHAP). Section five, discusses the (CHAP) workflow. Section six, explains the (CHAP) packets header structure. Section seven, discusses the proposed security technique - computer authentication using modified chap. Finally, section eight, is the paper conclusion and future work.

2 Relevance to Previous researches in communication authentication

In previous work a security mechanism that aims at securing remote data exchange among network nodes by applying several layers of authentication was presented [22]. That mechanism was built on layer two, Point-to-Point Protocol (PPP) [23]. Authentication is achieved when building new Request For Comments (RFCs) [24] 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. In that research a new format of PPP packet was built by adding a new field to the frame. Accordingly, the new frame becomes a proprietary authentication field to the proposed security system.

The following Figure, 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

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.

But that work was not enough on its own to fully secure nodes communication in a highly secured environment. As PPP has Its own authentication protocols, Password Authentication Protocol (**PAP**) and Challenge-Handshake Authentication Protocol (**CHAP**) [**25**, **26**] those protocols were required to be secured.

3. Basis of Selecting Challenge-Handshake Authentication Protocol (CHAP)

In Point-To-Point protocol (**PPP**) two authentication choices are available: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
PAP is used by Point to Point Protocol to validate users before allowing them access to server resources. Despite having the advantage of being known by almost all network operating systems, PAP suffers from some serious pitiful; PAP transmits unencrypted ASCII passwords over the network and is, therefore, considered insecure.
Accordingly, CHAP has been selected for this research because it is more secured than Password Authentication Procedure (PAP). That is due to several reasons:

- It provides protection against playback attack by the peer through the use of an incrementally changing identifier;
- It has a variable challenge-value; the exchanged variable is never sent over the network;
- At any time, the server can request the connected party to send a new challenge message.

4. The Challenge-Handshake Authentication Protocol (chap)

CHAP is an authentication scheme used by Point to Point Protocol (**PPP**) servers to validate the identity of remote clients. Challenge Handshake Authentication Protocol, or CHAP, is one of two authentication protocols supported by PPP. Similar to PAP, CHAP is works with Link Control Protocol (LCP) to authenticate a connection after the link establishment phase. Unlike its counterpart, however, CHAP constantly rechecks the validity of the connecting host to protect against unauthorized access. CHAP packets use a challenge system, meaning that authenticators transmit a challenge packet continuously until the connecting system responds with a packet containing a response. If this message contains a correct value, calculated using a hash function, the authenticator sends back a success packet. If not, the connection fails.

5. Chap Work Flow

The CHAP verifies the identity of a client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret, in this research a set of MAC addresses. CHAP works as follows:

1. After a link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained by using a one-way hash function.
2. The server checks the response by comparing its own calculation of the expected hash value.

3. If the values match, the authentication is acknowledged; otherwise the connection is usually terminated.
4. A new challenge with a new ID must be different from the last challenge with another ID in a new packet. Additionally, if the success or failure is lost the same response can be sent again, and triggers the same success or failure indication in new packets.

6. The Chap Packets Header Structure

A CHAP packet header consists of 40 bits, it is fully defined in RFC 1994. The header CHAP specification is composed of the following fields:

- **Code**: The code field determines the function of the CHAP packet. Possible values are as follows: 1 - Challenge 2 - Response 3 - Success 4 - Failure
- **Identifier**: The identifier field contains the actual information that determines whether or not a host will authorize the connection and allow it to take place.
- **Length**: The length field is the total size of the packet, including the data field that follows the CHAP header.

The CHAP has four different packet layouts for: Challenge, Response, Success and Failure. The layouts of those packets are as follows:

1. Layout of the Challenge Packet:

Description	1 byte	1 byte	2 bytes	1 byte	Variable	variable
Challenge	Code = 1	ID	Length	Challenge length	Challenge value	Name

The authentication value chosen for the CHAP challenge is stored in challenge packet header. That value is used by both the sender and the receiver in the corresponding response.

2. Layout of the Response Packet:

Description	1 byte	1 byte	2 bytes	1 byte	Variable	variable
Response	Code = 2	ID	Length	Response Length	Response value	Name

The response packet contains the authenticating authentication value chosen for the CHAP challenge is stored in challenge packet header. That value is used by both the sender and the receiver in the corresponding response.

3. Layout of the Success Packet:

Description	1 byte	1 byte	2 bytes	1 byte	Variable	variable
Success	Code = 3	ID	Length		Message	

The success packet contains the success response of the authentication process.

4. Layout of the Failure Packet:

Description	1 byte	1 byte	2 bytes	1 byte	Variable	variable
Failure	Code = 4	ID	Length		Message	

The failure packet contains the failure response of the authentication process.

7. The Proposed Security Technique - Computer Authentication using Modified CHAP

In the presented security mechanism, both the sending and the receiving computers, authenticate themselves to each other during remote information exchange by using a modified **CHAP** packet.

This is achieved by presenting the identity of all computers working on the network to each other through the Medium Access Control (**MAC**) address of the Network Card. 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 other devices sets up a connection-oriented communication with a remote device by creating a session which is called a "**three way handshake**".

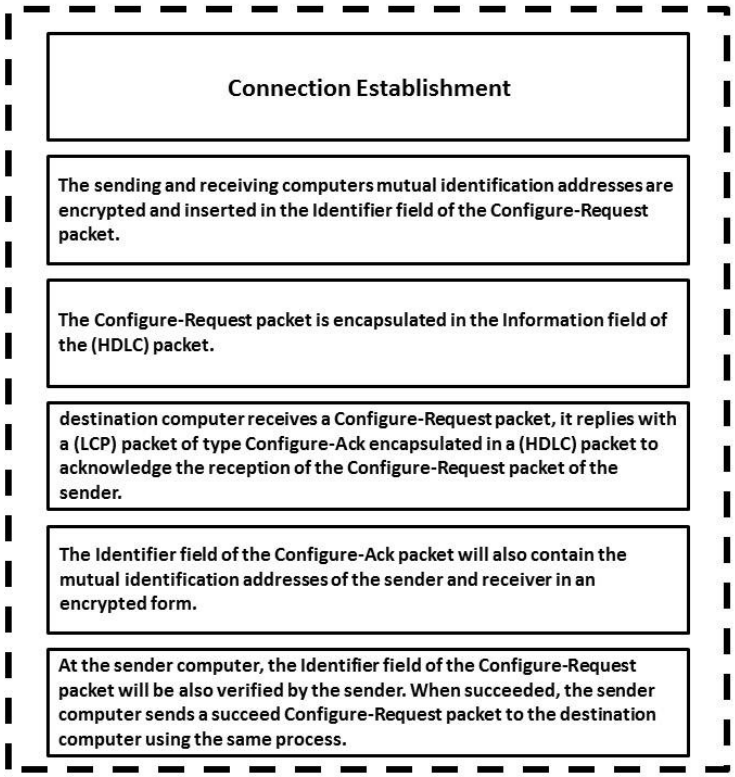
This mechanism is performed over two phases taking into account the modification takes place after testing the link. To test the link the communication goes into the usual steps without the researchers' interference. This is achieved as presented in Block Diagram 1 and works as follows:

- 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 mutual identification addresses are encrypted and inserted in the Identifier field of the Configure-Request 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 mutual identification 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.

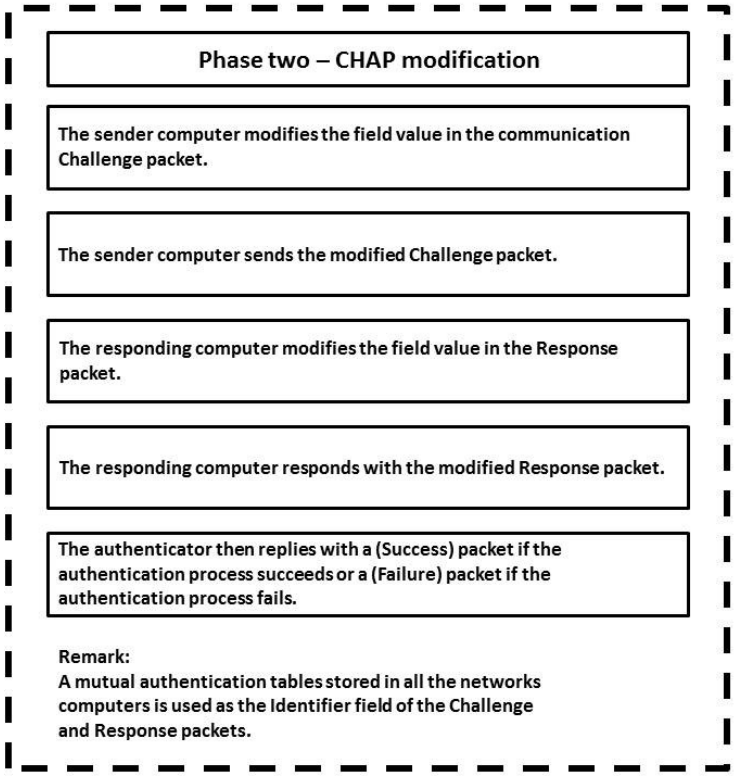
Phase two of authentication: Modification of the CHAP

In this phase, the Challenge Handshake Authentication Protocol (**CHAP**) is modified by changing the challenge field in the challenge packet and in the response packet. This phase is presented in Block Diagram 2 and works as follows:

- The sender computer modifies the field value in the communication **Challenge** packet.
- The sender computer sends the modified **Challenge** packet.
- The responding computer modifies the field value in the **Response** packet.
- The responding computer responds with the modified **Response** packet.
- The authenticator then replies with a (**Success**) packet if the authentication process succeeds or a (**Failure**) packet if the authentication process fails.
- In this research, a mutual authentication tables stored in all the networks computers is used as the Identifier field of the **Challenge** and **Response** packets.



Block Diagram 1: Connection Establishment



Block Diagram 2: Authentication: Using Modified CHAP

8. Conclusions

This research presented a security mechanism based on modifying the challenge field of the CHAP protocol. That modification added an extra layer of security to the originally secured CHAP protocol, **CHAP** protocol was selected against the PAP protocol because the PAP suffers some inherent security problems.

This technique was adopted to participate in solving cloud computing security. It would allow having a central authentication node to perform could sub-networks segregation which has a vital importance in cloud networking security.

This research is aiming to perform this research in a large cloud to measure the effect of that technique on both performance and security.

References

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

[2] J. F. DiMarzio, "Network Architecture and Design: a field guide for IT consultants", SAMS, 2001.

[3] Debra Littlejohn Shinder," Computer Networking Essentials", Cisco Press, 2001.

[4] Joe Casad "Teach yourself TCP/IP in 24 Hours", SAMS, Second Edition, 2001.

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

[6] National Computer Security Association (NCSA), "Internet Security", Techmedia, 1997.

[7] M. Kaeo, "Designing Network Security", Cisco Press, 1999.

[8] C. Brenton,"Mastering Network Security", McGrew-Hill, 1999.

[9] P. Norton, M. Stockman, "Network Security Fundamentals", SAMS, 2000.

[10] W. Stallings, "Network Security Essentials", Person Education Inc, second edition, 2002

[11] M. S. Merkow, CCP, J. Breethaupt, "The Complete Guide to Internet Security", McGrew-Hill, 2000.

[12] H. Makhlouf, M. W. Youssef and S. Ismaeel, "التجارة الالكترونية الحكومة الالكترونية", Ain Shams Press Inc, second edition, 2008

[13] 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.

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

[15] M. W. Youssef, T. Sultan,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.

[16] Mervat Helmy Huissin Ahmad, "A Proposed Mechanism for Securing Remote Information Exchange among Computer Nodes", MSC Thesis Submitted to Faculty of Computers & Information, Information Systems Department, Helwan University, finished in June, 2008.

[17] W. Simpson, Request for Comments 1331: The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links, Network Working Group, California, 1992.

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

[19] PPP Encapsulation:

[20] http//www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/intwork/inbb_ras_afou.mspx#top#top, 2007.

[21] W. Simpson, Request for Comments: PPP in HDLC Framing, Network Working Group, Michigan, 1993.

[22] Youssef M. W., "Securing Computer Networks Communication By Modifying Computer Network Communication Protocols", An IEEE communications society Security and Applications Workshop, the 11th International Conference on Telecommunications for Intelligent Transport Systems "ITST-2011", St. Petersburg, Russia, Aug. 2011.

[23] Youssef M. W. and H. El Gendy, "Applying Open Networks Communication Authentication", An IEEE communications society Security and Applications Workshop, the 11th International

Conference on Telecommunications for Intelligent Transport Systems ”ITST-2011”, St. Petersburg, Russia, Aug. 2011.

[24] Youssef M. W. and H. El Gendy, "Applying Open Networks Communication Authentication By Scrambling and Encrypting Layer Two Packet Content.", International Journal of Computer Science & Network Security (IJCSNS), June, 2011.

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

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

[27] Devarakonda John Livingstone et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (1) , 2012, 3157 – 3161