Robust Two-Way Locking Protocol for Key Exchange

Shivaraj Shetty, Saumya Hegde, and Mohit P. Tahiliani

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal, India
shettyshivaraj@gmail.com

Abstract. Sharing of symmetric key between the sender and receiver for encryption and decryption is considered to be one of the major issues in the communication networks. It is due to the fact that the strength of cryptosystem depends not only on the strength of the key, but also on the underlying key exchange protocol. In this paper, we propose a Robust Two-way Locking Protocol which overcomes the drawback of Diffie-Hellman key exchange protocol in terms of flexibility provided to the sender for selecting the desired key. Moreover we demonstrate the applicability of the proposed protocol in TCP handshake and compare it with Secure TCP which is based on Diffie-Hellman (DH) key exchange protocol. Based on the simulation results it is observed that Robust Two-way Locking (RoToLo) Protocol incurs negligible overhead in the network while providing greater flexibility of key selection to the sender as compared to Secure TCP.

Keywords: Diffie-Hellman, Flexibility, Key Exchange, Secure TCP.

1 Introduction

Widespread use of internet fostered by the advent of mobile computing devices has posed several challenging issues for securing data communication. Both Symmetric key cryptosystem and Asymmetric key cryptosystem are widely used by the applications of internet. However, Symmetric key cryptosystem is preferred for applications that are delay sensitive (*e.g.,*: telnet, web browsing *etc.,*) since Asymmetric cryptosystems are computation intensive.

The major concern while using Symmetric key cryptosystem is the *secure key exchange* between the communicating end hosts. Several key exchange algorithms have been proposed for the same, however, Diffie-Hellman (DH) algorithm and its variants remain the most popular and widely accepted ones. Though Diffie-Hellman algorithm and its variants [1], [2] have proved to be successful for several years, they provide limited flexibility to the end hosts in terms of key selection *i.e.,* the end hosts can select only the *key length* but not the *desired key* itself. Selecting only key length does not guarantee the desired strength of the key. Thus in this paper we propose a Robust Two-way Locking (RoToLo)

K.R. Venugopal and L.M. Patnaik (Eds.): ICIP 2011, CCIS 157, pp. 226–232, 2011.

Key Exchange Protocol that provides the flexibility of selecting the *desired key* to the end hosts.

There has been a lot of interest in enhancing the transport protocols such as Transmission Control Protocol (TCP) to provide security features for process to process communication [3], [4]. Since TCP is the most widely used transport protocol in internet for majority of the applications, it reduces the overhead of enhancing application protocols to provide security features. Thus, in this paper, we demonstrate the applicability of RoToLo Key Exchange protocol in TCP handshake procedure and compare it with Secure TCP[3] which is based on Diffie-Hellman key exchange protocol.

The remainder of the paper is organized as follows: Section 2 highlights the possible drawbacks of Diffie-Hellman key exchange protocol and the motivation for designing RoToLo key exchange protocol. The working of RoToLo key exchange protocol is described in Section 3. Section 4 explains the modifications required in TCP handshake procedure. Section 5 presents the simulation results and possible drawbacks of RoToLo key exchange protocol. Section 6 concludes the paper with future directions.

2 Motivation

Diffie-Hellman (DH) key exchange algorithm is the most widely accepted key exchange algorithm in many networking protocols including IP Security (IPsec), Secure Socket Layer (SSL) and Secure Shell (SSH). DH security depends on the difficulty in solving the Discrete Logarithm Problem (DLP) [5]. The basic working of Diffie-Hellman key exchange algorithm represented in Fig. 1.

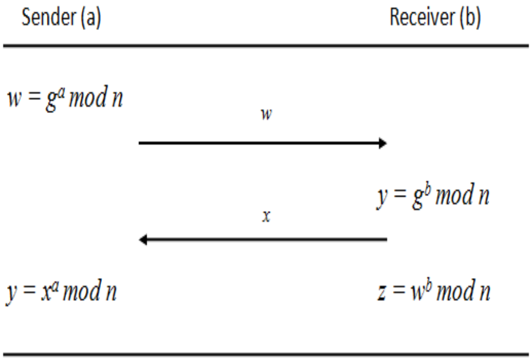

Fig. 1. Diffie-Hellman key sharing

Based on the algorithm it can be noted that in DH key exchange algorithm the strength of the shared key mainly depends on the combination of *a* and *b*.