Security in IP Storage Networks

Ushaditya Pulugurta, Amarnath Jasti*, Kamesh Namuduri and Ravindra Pendse

Department of Electrical and Computer Engineering, College of Engineering

1. Abstract

Network security is a very important parameter and is always been a challenge for the emerging technologies especially for high-speed data networks. The storage industry is sprouting at a faster pace with efficient and faster methods of data transfer and storage. Security should be camouflaged with these methods from the beginning in order to provide reliable and secure access to the users. Some known protocols in IP storage networks, which are reliable on IP networks, are SCSI over internet (iSCSI), Fiber channel over IP (FCIP), and internet fiber channel protocol (iFCP). These protocols use IP networks for data transport and it is necessary to provide a secure channel over these networks. As IP networks were not traditionally designed with security in mind, different mechanisms like IPSec are used for securing data at the network layer. Protocols like iSCSI do not provide per packet protection techniques. Since Storage Area Network (SAN) consists of block transfers between the clients and the server, encryption and cryptography need to be implemented for each block being transmitted and received along with the control data. Though block level security provides more reliability, it can be more time consuming and costly. In this research work, authors propose a novel security mechanism for IP storage networks that can be implemented with any protocol using object-based data transfers.

2. Introduction

Security protocols in storage can be classified according to the type of medium through which the data would pass through. The security mainly involves the authentication and integrity of the data being carried along with a mechanism of encryption throughout the transmission. These solutions must not only be cost-effective but also efficient. Simple protections like encryption and passwords can be implemented in a more stable network. It is also important to determine the level of security since it reduces the cost of providing security to unimportant data. Encryption can be done at various layers depending upon the type of protocol. There can be encryption for control packets, data packets or both depending on the level of encryption required. Storage networks consist of various mediums through which information is transferred. Fiber cables, Small computer Systems Interface (SCSI) & Serially Attached SCSI (SAS) interfaces are the most commonly used media for communication.

3. Security in Storage Area Networks

Fiber channel is a technology that takes storage networks to great heights with its exceptional performance and gigabit speed factor [1]. Initially fiber channel did not have much security concerns as the data being transmitted was a beam of laser that was sent along a fiber cable in different modes. Gradually, security was introduced in order to provide secure communication between fiber channel devices. Fiber channel security protocols (FC-SP) provide two kinds of protection [5]. It provides different security mechanisms for various portions of fiber channel traffic. The ESP header protocol in the IP encapsulation payload provides security to the data traffic and the CT authentication protocol secures the control traffic. The fiber channel security protocol uses an authentication mechanism which is a combination of Diffie-Hellman algorithm and Challenge Handshake Authentication Protocol (CHAP) algorithm [4]. Both protocols belong to the FC2 layer of the fiber channel protocol suite and are responsible for authentication of the fiber channel frames. Since these protocols are the network layer protocols, they are only responsible for secure transmission of data over the networks and do not aid in securing the data when it is in halt as shown in Fig 1.

Though fiber channels have a great effect on performance, they do not span much larger distances. IP networks span large distances and are easily accessible. So, they had to be encapsulated with IP networks in order to enhance the usage. As a result, FCIP and protocol (iFCP) came into existence. Since iFCP, FCIP rely upon IP networks to transport the information, it is necessary to provide a secure encapsulation over these networks as the IP networks were traditionally not designed with security in mind. iFCP, FCIP rely on IP security protocol (IPSec) authentication and confidentiality which is a protocol suite used for secure communication at the network layer between two peers. IPSec is an IP layer protocol unlike SSL, which is an application layer protocol.

Initial authentication mechanisms may include a Kerberos sever to validate the integrity of the sessions. Since storage area network consists of block transfers between the clients and the server or between the storage devices, encryption and cryptography can be implemented for each block being transmitted and received along with the control data that is being sent. Though block level security provides more reliable data transfers, it can be more time consuming and costly. The Encapsulation security payload (ESP) header protocol and the Common header authentication (CT_Authentication) protocol are other known security protocols defined for fiber channel communications [6]. The former is physical layer protocol which is applied to fiber channel frames for authentication, integrity of the fiber channel frames. The latter provides an authentication mechanism for layer 4 protocol which encapsulates other protocols such as Small systems computer interface (SCSI).

SCSI is a physical standard which is used for communication between computer peripherals [2]. SCSI is mostly used for large servers and high performance computers. Typically, SCSI does not involve security as it connects much of the components inside a computer or a server. When this protocol is encapsulated and transported over a TCP/IP network, it is known as iSCSI. iSCSI is also susceptible to all IP network security vulnerabilities.

Object based storage devices (OSD) protocol is a new capability based protocol in client server architecture which converts the fixed block sizes to variable sized objects [3]. It involves a security manager which authorizes the client with a capability key in order to access the object store. This protocol provides a fine grained access to both client and the object based storage by a shared key mechanism. The keys are managed by the SAN security managers both at the server and the clients in order to improve the efficiency. This provides a strong confrontation towards the network attacks. Even though OSD protocol provides a better solution for block storage, it cannot overcome the limitation of a secure channel, i.e. only if the channel is secure. When the channel is insecure it provides security but with certain trade offs like having only command verification but not data integrity. The OSD protocol has various stages of encryption on which the access control mechanisms, command and data integrity depend upon. When the channel is completely secured and the data is encrypted, it results in a sort of duplication work which in turn results in wastage of bandwidth and CPU time. Also, different levels of authentication to data being exchanged provide different levels of resistance against different attacks.

In this research work, authors are proposing a robust security mechanism which will provide enough block level security without compromising network security. The new security mechanism will remove any CPU intensive processes like duplication and provide a faster secure channel for the data. Like any other security protocol, the proposed mechanism will be tested against various network attacks like spoofing, Denial-of-service (DoS) attacks, Man-in-the middle attacks, replay attacks etc.

4. Analysis and Conclusion

The proposed algorithm is in developmental stage. No simulation results are available yet.

[1] Information Technology - Fibre Channel Protocol for SCSI, Fourth Version (FCP-4)
[2] Information technology - SCSI Parallel Interface-5 (SPI-5)
[3] M. Factor, D. Nagle, D. Naor, E. Riedel, J. Satran, The OSD Security Protocol, Proceedings of Third IEEE International Security in Storage Workshop, December 2005
[4] C. DeSanti, L. Hofer, F. Maino DH-CHAP Specification, 03-047v0, January 2003
[5] Fibre Channel Security Protocols (FC-SP) REV 1.74, INCITS working draft proposed American National Standard for Information Technology, February 17, 2006
[6] E. Hibbard, Fibre Channel Security Protocols and Hitachi Storage**,** Technology Brief

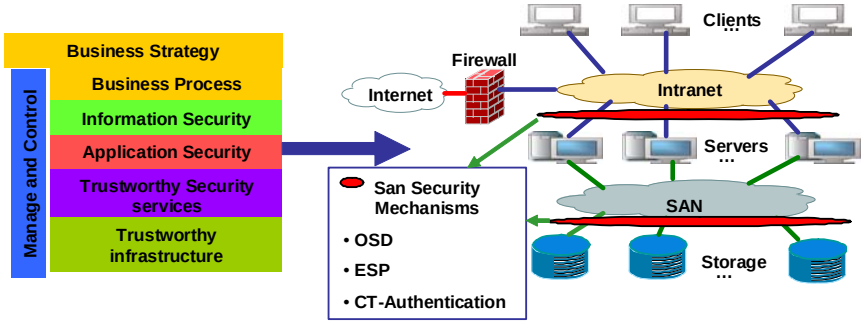

Fig -1 Security in Storage Area Networks