SECURING INTERNET PROTOCOL (IP) STORAGE: A CASE STUDY

SIVA RAMA KRISHNAN SOMAYAJI M.Tech I.T (NETWORKING) VIT UNIVERSITY Vellore, INDIA somayaji1984@gmail.com

Abstract - Storage networking technology has enjoyed strong growth in recent years, but security concerns and threats facing networked data have grown equally fast. Today, there are many potential threats that are targeted at storage networks, including data modification, destruction and theft, DoS attacks, malware, hardware theft and unauthorized access, among others. In order for a Storage Area Network (SAN) to be secure, each of these threats must be individually addressed. In this paper, we present a comparative study by implementing different security methods in IP Storage network.

Keywords: iSCSI; Target; Initiator; Wireshak; SSLv2; IPsec.

I. INTRODUCTION

The proliferation of higher performing networks with multi-Gigabit Ethernet backbones, easier access to high-performance global networks such as Multiprotocol Label Switching (MPLS), and increasing popularity of Internet Simple Computer System Interface (iSCSI), an IP-based protocol which enables block-level I/O, IP storage networks are in dire need of secure transport which will not impact performance. In addition to storage performance, a practical IP- based security solution must also be simple, compatible, non-intrusive and cost- effective.

In a heterogeneous environment, we have the option of securing communication at both the application layer, using protocols such as Secure Sockets Layer (SSL) or the Transport Layer Security (TLS), and on the IP level using IPSec. The starting point for a systematic approach to storage security is to take stock of the various types of data being stored and classifying it according to how important it is and how costly it would be to the business if it were lost or stolen. Then for each classification, appropriate security policies should be set. The next step is to enforce password and World Wide name Ch.A.S MURTY Systems and Network Security Team C-DAC Hyderabad, INDIA chasmuty@cdac.in

identification (for Fibre Channel) and logical unit number (LUN) authorization to ensure that only authorized users, devices or applications can access data, and to implement LUN masking so that particular storage volumes can only be seen by authorized users, devices or applications. iSCSI protocol and its related iSCSI drivers provide authentication features for both the initiator and target nodes. This can prevent unauthorized access and allow only trustworthy nodes to complete communications.

In order to transfer data to and from the storage securely on an iSCSI network, iSCSI can employ Ipsec that offers strong encryption and authentication functions for IP packets. However, the encryption processing triggers performance degradation when mass volume of data should be transferred. Specifically in a long-latency environment, ACK or a SCSI Command takes a long time until it arrives at the other machine. Moreover, Ipsec is implemented in IP layer located on the lower-level. If we try to improve the performance of Ipsec encryption processing, IP and other codes inside a kernel of operating systems are required to be modified.

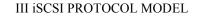
In this paper, we have shown the performance analysis of IP storage network in different scenarios.

II. RELATED WORK

There has been lot of work done in the implementation of IP-storage. Soumen Debgupta[1] proposes a software approach of iSCSI by exploiting the optional features like multiple connections to improve performance. Yi-Cheng[2] presented a methods for implementing the implementation of the iSCSI virtualization switch used in SANs. The proposed method reduces the overheads of protocol processing by using a packet forwarding model based on caching the structure ID of the iSCSI session.

Dimitar[3] proposed that iSCSI host bus adapters, also called iSCSI NICs or Storage NICs (SNIC), are optimized in hardware with realization of a TCP/IP off-load engine (TOE) to minimize processing overhead to achieve better performance in IP-SAN. Kamisaka[4] presented a method of optimization for encryption processing in the upper-layer instead of using Ipsec.

Dr. Rekha Singhal[5] proposes two novel techniques for improving the performance of iSCSI protocol. First proposed technique is the elimination technique for reducing latency caused by redundant overwrites and the second technique reduces the latency caused due to multiple reads to the same storage sector. Dr. Zia Saquib[6] propose a method of using clusters of inexpensive nodes with Redundant Array of Inexpensive Nodes using iSCSI for high performance using commodity hardware and setting up efficient iSCSI target controllers for block virtualization.



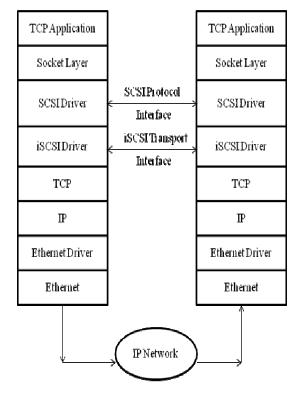


Figure 1: IP storage layered model

The above figure shows how a communication is taken place by an initiator and target. The iSCSI system is a layered structure consisting of SCSI/iSCSI and TCP/IP.

A. DETAILS OF INITIATOR

In the implementation we have used Windows Vista systems as the initiators and target. In Windows Vista, the iSCSI initiator driver software is readily available.

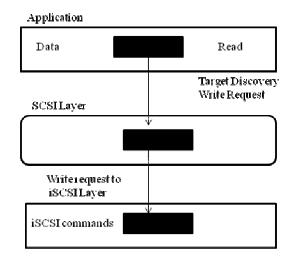


Figure 2: Data processing in Initiator

Figure 2 describes the basic model of how data is processed in the initiator. First the initiator searches for targets available. This is the discovery phase. When the initiator discovers a target, a data write request command is initialized and data is sent to lower iSCSI/SCSI layer where iSCSI commands are processed and then the data is sent to the appropriate target.

B. DETAILS OF TARGET

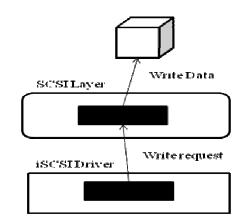


Figure 3: Data processing in Target

Figure 3 describes how the data is sent to the disk arrays. The data comes from the TCP layer to SCSI/iSCSI layer where a write request is called. The data segments are passed to the *handle cmd* function at iSCSI/SCSI driver and they are written in the target's disk sequentially.

IV. Performance Analysis of IP-Storage network without any security implementation

The traffic analysis is done using a tool *wireshark* which is a open source and a free downloadable software for protocol analysis.

linen kar.		12	() (pet rimane)
1771.9894 117.98721	11.18.2.1	Ŋ	10 separt of a massed
Dirani debie	14.10.2.	P	Count of 1 manes
107.900 17.1821	11.18.71	Ţ	TT count of a reason
			a and a second
11.10.11 H.10.1.	102.100.2.1	V	C spect of a model
182392 19.1821	10.16.27	N.	(17 segurit of a ressound
W2.301 W.W.1	102.00.2.2	p	TO repet of a number
1007), 20000, 197, 1087 ([9].[6.].)	191	stati data ta Luci dali da

Figure 4: Traffic analysis between initiator and the target

The above figure shows us the interaction between initiator (192.168.2.1) and the target (192.168.2.2). Whenever the initiator sends a request to store data, the target checks which device that particular initiator is connected to and then the target sends acknowledgment along with disks the initiator is related to. The initiator sends the data to be stored to the target or controller which again redirects the iSCSI data to respective disks.

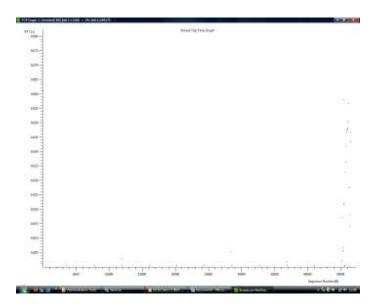


Figure 5: Round Trip Time Graph

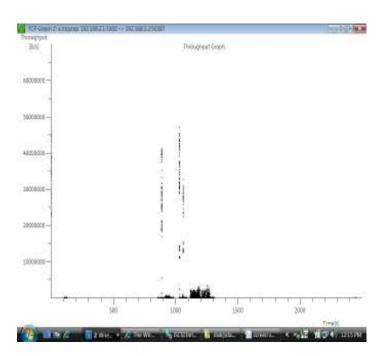
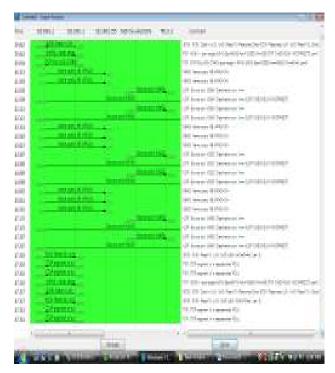


Figure 6: Throughput Graph

In above two graphs we can see the time taken for the data to travel between the initiator and target.



IV. Performance Analysis of IP-Storage network by implementing SSLv2.

Figure 7: Graph Analysis with SSLv2 enabled in IP-

Storage

In the above figure, the initiator contacts its local system Name query through port 137 and at the source port 53564 the encryption process is started at the initiator and at port 62864 the UDP checksum is performed by link local multicast name resolution at the destination.

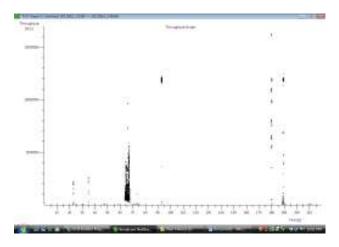


Figure 8: Throughput Graph

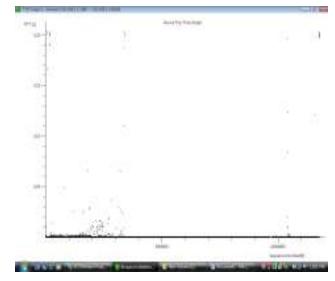


Figure 9: Round trip time graph

When we compare figure 8 (Throughput graph) and figure 9 (Round trip time graph) we notice that there is a slight decrease in the performance in the IPstorage network. This decrease is due to the fact that SSL generates some source code for every application.

V. Performance Analysis of IP-Storage network by

implementing IP-sec.

Posc Policy Agent	Here:	Description	2010.0	Serve Type	109 (0x A)
	Application Eigen	Processes a	Stated	Automotic	Local System
App the service	Application Indos.	Facilitates t_	Instead	Manual	Lotal Syttle
Volum the service	C. Application Layer	Provides to-		Manual	Local Service
	C Application Mana.	Precises e-		Manual	tanal System
	Antematest Soften	Service runni-	Stated	Automatic	Local Syste-
Ownerptore	C. Background Intelli.	Transfers Mi.,	Stated	Automatic (B.,	Local System
internet Protocol security SPaed	C. Base Pillering Engl.	The Date Pd.	Statut	Automatic	Local Service
Lassorts network-level peer	C Block Level Backs.	Traine to g.		Manual	Local Syste
uthentication, data origin	C-DAC Security CL.			Disabled	Local Syste
wthentication, data integrita.	Curtificate Propest	Provident-		Manual	Local System
lata confidentiality (encryption).	CHi Key balation	The CNG te	Idented	Manual	Inial Sylde-
ind replay protection. This	CON+ Svent lyst-	Inspervets Sp-	Statled.	Automatic:	Local Service
ervice enforces Place policies	COM+ System Ap-	Manages I'v		Manual	Tarol Syste
ceated through the P Security	Computer Browner	Maintains a	Stated	Automatic	Local Byste
folicies snap-in or the	Cyptographic Ser.	Provides to	Stated	Automatic	Retwork S
ommand-line tool 'netst-	C. DCOM Server Pre	Provideo Inu	Statut	Automatic.	Local Syste
part. If you stop this service.	C Desitop Western	Provided Do	Statut	Automatic	Local Syste
too may experience network	C DPS Replication	Deather you		Manual	Local Syste
ennectivity saves if your policy	C DHCP Cheet	Registers an	Skilled	Automatic	Local Service
equives that convertions use	Dispositio Palicy	The Degree-	Idented	Automatic	Inial Service
Piec. Also remote	Dispersio Series.	The Gages-		Manual	Local Service
nanapement of Windows	Departy System.	The Days.	Stoned	Manual	Tetal Syste
reveal is not evaluate when	Distributed Link Te.,	Attaining in.	Started	Automatic	Local System
his service is stopped.	C Dotnibulost Transa	Coordinates		Manual	Network 5
	CHIS Client	The DNS CE.	Statut	Automatic	Network 5
	C Edendible Hathen	The Edward_	Statut	Menual	Local Syste
	Q, Fat	Deakine you		Manual	Network 5
	G Function Discover_	Heat proces		Manual	Local Service
	Energie Doover-	Publishes D-	Internet	Automatic	Intel Service
	12 Gaugle Updater 5			Manual	Loral Syste-
	12 Onice Policy Clent	The service -	Stated	Automatic:	Territ Syste-
	C. Haplith Key: and Ca	Previden 4.3		Manual	Local Syste
	C. Human Interface	Enobles pen		Manual	Local Syste
	C, BE and Autor Dr.	The BZDIT	Statut	Automatic	Local Syste
	C Interactive Service	fraities ton-		Matrical	Local Syste
	Chineset Connect.	Provides no		Manual	Local Syde
	C.P.Heijer	Prevides alo-	Sint	Automatic	Local Syste-
	C. Pres, Caller, Agent	Barrent Cha-	Inches .	A4444	10-10-10-10-1
	SI, OCICAR	WC9 Cake I	Statted.	Automatic	Annal System:
	C. Kimfley for Dotation	Coordinates	Stated	Automatic (D.).	Network 5

Figure 10: Enabling IPsec Policy Agent

ìÈ

100

b

10

IPsec can be enabled by msc services. We can find the IPsec policy disabled. Starting this service enables IPsec.

	Darlay Hended							
		Vale	hin	ļα.	Mij)	hibbe.	latipa .	la Ma
au -		3.05	- 80	BOC.	100	- 1	- 1	
loval		365	- 64	900 (400		-	1
 Saud Poto 9 		200			5.97		- 9	1
 Description Control Protocol 		205		88.		1	1	
0.000		200		80.		18	100	
8 101		61.5	-03	14.0	00	18	1966	1
8.93		585	- 88	200	10	18	3.88	1
0.0005		165	1	144	1.5	1	4	į,
Mathematika ing		165	1	111		i i	184	1
0.02000		100		10,1	10	-	- 0	
Malassan Parist		135	. 3			- 2	343	1
10		665	1	20	100	1	2.0	
line have		165	1	÷.	1	1	10	
0.000		035	1				- 0	
# (C)		0.0	- 0			1	- 69	1
10		555	1		1		14	1
kas		125	- 6	62		1	603	
101		625	- 1			1		1
1 Miles		199		100	10	1	100	1
1 F1 F1		665	1	194	58			1
Velocal Veloc		105	1			1	184	1

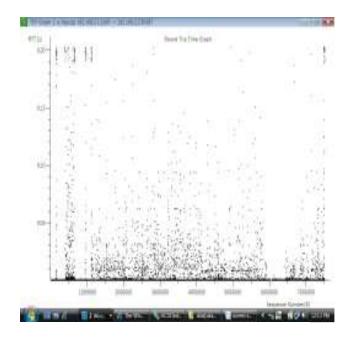


Figure 13: Round trip time graph

Figure 11: Protocol Hierarchy Statistics

In the above figure we can see the packet transfer percent, number of packets transferred, and throughput in Mbps at each protocol layer. A remote procedure call has been invoked called the DCE/RPC (Distributed Computing Environment / Remote Procedure Calls).

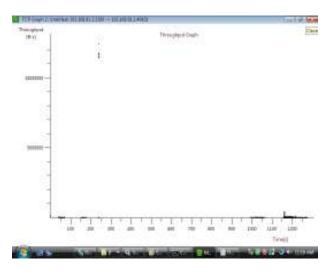


Figure 12: Throughput graph

In the above throughput graph, there is drastic performance degradation after 1000 seconds.

The above figure clearly tells us that that is much delay when we implement IP-sec as there are lots of peaks (bottle-necks) at different time instances as compared to the SSLv2 implementation.

VI. Comparison of Performance Analysis of Implementation of SSLv2 and IPsec

	Round trip time values (Sequence no, Time)	Throughput values (Time, No of bits)				
	(1000, 0.01)	(25, 1000)				
SSLv2	(3000, 0.005)	(70, 5000)				
	(5000, 0.07)	(90, 12000)				
	(10000, 0.02)	(190, 20000)				
	Round trip time values	Throughput values				
	(1000, 0.01)	(20, 1000)				
IPsec	(3000, 0.03)	(70, 50000)				
	(5000, 0.057)	(90, 100000)				
	(10000, 0.12)	(190, 300000)				

Table: Comparative values of Round trip time graph and throughput graph

The above table shows that when we implement SSLv2 there is a decrease in the Round Trip Time and an increase in the throughput as compared to implementation of IPsec in the storage network. This is due to the fact that IPsec is implemented in the lower layers along with IP protocol and the IP needs to perform addition function i.e. securing the packets and then route them. In case of Secure Socket Layer (SSLv2), the security is implemented in sockets or at the port level and is transparent to the end application.

VII. CONCLUSION

In this paper we have implemented an IP-Storage network using iSCSI protocol. We have analyzed the performance of the IP Storage network without any security implemented and also by implementing SSLv2 and IPsec. We present a comparative analysis IP storage network performance in each case.

VIII SCOPE FOR FUTURE WORK

We plan to implement IP Storage network using InfiniBand Architecture as defined by InfiniBand Trade Association which "is industry standard, channel-based, switched fabric, interconnected architecture for servers. Infiniband architecture changes the way servers are built, deployed, and managed." In short, it is basically a high-speed I/O switching fabric.

We also plan to use Fibre Channel over Ethernet (FCoE) which enables the consolidation of both SANs and Ethernet traffic onto a one common network adapter, reducing the ever growing number of adapters required. It allows an evolutionary approach towards I/O consolidation by preserving all Fibre Channel constructs, maintaining the same latency, security, and traffic management attributes of FC while preserving investments in FC tools, training, and SANs. One of the challenges with passing Fibre Channel frames over Ethernet is that FC provides a lossless transport. Fortunately, classical Ethernet has a PAUSE capability so that a busy receive port can send a control frame to the transmit port requesting a pause in transmission.

ACKNOWLEDGMENT

The authors thank the Dr.Sarat Chandra Babu, Director, C-DAC, Hyderabad for his encouragement and giving permission to publish this paper. We also thank to Prof. H.R.Vishwakarma, School of Computing Sciences, VIT University, Vellore for his continuous support and guidance. Finally we thank Dr. Sankaran, Scientist-'G', Head of Environmental Geophysics, National Geophysical Research Institute, Hyderabad for his moral support throughout this work.

REFERENCES

- Soumen Debgupta, Dr. Rekha Singhal, C-DAC "Design and Implementation of an Efficient iSCSI Target", National Conference on Advancements in Information & Communication Technology (NCAICT), March 15-16,2008.
- Yi-Cheng Chung, Stanley, Industrial Technology Research Institute "A Packet Forwarding Method for the iSCSI Virtualization Switch", International workshop on Storage Network Architecture and Parallel I/Os, IEEE 2008.
- 3. Dr. Rekha Singhal, C-DAC, "Use of Operation Semantics for Parallel iSCSI Protocol", Conference on software engineering, Parallel and Distributed Systems (SEPADS '08), University of Cambridge, UK, Feb 20-22, 2008.
- Shubhada Nandarshi, C-DAC, "Faster Access using Caching Technology for improving iSCSI performance", National Conference on Advancements in Information & Communication Technology (NCAICT), March 15-16, 2008.
- MingHua Jiang, Ming Hu, Jingli Zhou, Tao Peng, Key Laboratory of Data Storage System (Huazhong University of Science and Technology), Ministry of Education, Wuhan 430074, China, "Design and Implementation of IP-SAN Based on Third Party Transfer Protocols", International Colloquium on Computing, Communication, Control, and Management (ISECS), IEEE 2008.
- Dr. Zia Saquib, C-DAC "An Architecture for Continuous Available Commodity Storage", Intel Storage Workshop on High Performance Computing (HiPC), December 2007.
- 7. Dimitar Todorov's "Storage Networks on IP infrastructure", International Workshop NGNT.
- 8. Joe Little, **"Multi-Tier Storage"**, Stanford University's whitepaper.
- Kamisaka, Saneyasu Yamaguchi, Masato Oguchi, "Implementation and Evaluation of Secure and Optimized IP-SAN Mechanism", Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia.
- W. T. Ng, B. Hillyer, E. Shriver, E. Gabber, and B. Ozden, "Obtaining High Performance for Storage Outsourcing," Proc. FAST, USENIX Conference on File and Storage Technologies.
- P. Sarkar, S. Uttamchandani, and K. Voruganti, "Storage over IP: When Does Hardware Support help?" Proc. FAST, USENIX Conference on File and Storage Technologies.
- S. Aiken, D. Grunwald, A. Pleszkun, and J. Willeke, "A Performance Analysis of the iSCSI Protocol," Proc. 20th IEEE Symposium on Mass Storage Systems and Technologies.

13. C. Gauger, M. Koehn, S. Gunreben, D. Sass, and S. G. Perez, "Modeling and Performance Evaluation of iSCSI Storage Area Networks over TCP/IP-based MAN and WAN networks," The Second International Conference on Broadband Networks, vol.2

14 "Storage Networking Industry Association,"

http://www.snia.org/.

15. **"iSCSI Draft,"** http://www.ietf.org/rfc/rfc3722.txt.

16. "iSCSI Protocol Concepts and Implementation," www.cisco.com.