Security Framework for Storage Area Network (SAN)

[1*]Eneh, A.H., [2]Obi, A.M. & [3]Arinze, U.C.
[1,2,3]Department of Computer Science, Faculty of Physical Sciences,
University of Nigeria, Nsukka-South East, Nigeria.
E-mails: agozie.eneh@unn.edu.ng; obiadaobi08@gmail.com; uchechukwu.arinze.pg79296@unn.edu.ng
Phones: +2348076756975, +2348067821960, +2348066532557

ABSTRACT

Over the years, storage network technology has been faced with significant changes and there are many new innovations trying to improve the level of service and reliability in storage area. Due to the explosion of internet and the e-commerce, a tremendous amount of data has been created and made available to users. In addition to this, new type of data such as images, audio and video have been stored and integrated with applications and databases, further accelerating the demand for storage capacity. The need for storage of data and information as well as the increase of security awareness in the general population has brought the concept of a Storage Area Network to the forefront. SAN security risks are often misunderstood or underestimated, the critical issues associated with SANs, combined with the lack of communication concerning defenses has created a security gap in storage. In this paper, we will discuss about Storage Area Network (SAN) architecture. This paper will touch upon common threats to a SAN and the precautions a business can take to protect itself. The main focus of this paper will be on securing a Storage Area Network by using best practices in setting up a SAN as well as securing the data on a day-to-day basis. Security threats and solutions available in SAN environments. Fibre channel protocol will be used to implement the SAN security and DH-CHAP will be evaluated.

Keywords: SAN security, Fibre channel, DH-CHAP, vulnerabilities.

1. INTRODUCTION

Storage Area Network (SAN) security framework generally requires analysis of the possible loop holes. The need for storage of data and information as well as the increase of security awareness in the general population has brought the concept of a Storage Area Network to the forefront. Every business faces risk as long as they have something of value. The more valuable the assets of the company are, the more risk they face, due to the growing number of Information Technology (IT) users all around the world, consequently the amount of data that needs to be stored increases day by day. Data Attached Storage (DAS) and Network Attached Storage (NAS) cannot manage the storage of these large amounts of data. The emergence of SAN technology combined with data protection, privacy, and regulatory concerns has made storage security an important topic. Storage area network (SAN) is a network designed to attach computer storage devices such as disk array controllers and tape libraries to servers. Storage area network (SAN) security refers to the collective measures, processes, tools and technologies that enable the securing of a SAN infrastructure [1]. A storage area network can offer many benefits to a business.

It can allow storage and tape backup resources to be pooled and shared effectively among host servers. Storage area networks also separate storage traffic from general network traffic. Security is defined as the "management of a risk". Security has always been highest priority in such networks for network administrators, working with information and sensitive data of their companies. These networks encounter different attacks and storages on their own do not have any security features.

2. RELATED WORK

Considerably amount of works has been carried out in this area, the few once are reviewed as follows, the first work was on Evaluation of security network, the writer[2] emphasized that knowing the vulnerabilities is one of the critical task for making storage system secure and improving the performance and reliability of the network. Another article titled "Data at rest encryption addresses SAN requirement'' shows how data-at-rest encryption, when used with physical SAN security and techniques such as zoning and LUN masking, address all the major security risks that are faced by IT storage administrators. Encryption of data at the media (data-at-rest encryption with self-encrypting drives), in conjunction with physical SAN security, addresses all major storage administrators' security concerns. This type of encryption allows for minimal disruption of existing SAN infrastructure deployments and maintains interoperability [3]. Furthermore, [4] stated that a storage area network security analysis and design methodology by which creates a SAN analysis and design that could not only be used to create the most cost effective SAN solution that will work best for every unique scenario, but it could also determine if a SAN is indeed the solution to a company s storage needs or if a Network Attached Storage (NAS) or Direct-Attached Storage (DAS) solution might be preferable.

[5] points out that since SAN is usually used in highly critical systems in which requires high availability, confidentiality and integrity, organizations must be aware of all potential points where a security breach might occur and to include these into considerations when designing SAN security solutions. Ability to identify the points of vulnerability and implement a reliable security solution is the key to securing a SAN fabric infrastructure.

3. OVERVIEW OF STORAGE AREA NETWORK (SAN)

The Storage Network Industry Association (SNIA) defines SAN as a network in which the main purpose is to transfer data between servers and storage locations [7]. The network consists of several computers, servers and devices that are interconnected with each other; this infrastructure allows different computers to communicate with each other. The operation of each SAN consists of basic elements for communication, which manages the physical connections, management layers for organizing the available connections, computer system and storage devices for reliable and secure handling of data. SAN manage the data at the block level and thus not at the file level for keeping track of and allocating free space on disk to the data. SANs are used to make a high speed connection between storages and servers.

The importance of SAN cannot be overemphasized. It provides the basis for improved application availability (e.g., multiple data paths), enhance application performance (e.g., off-load storage functions, segregated networks. Increase storage utilization and effectiveness (e.g., consolidate storage resources, provide tiered storage, etc.), improves data protection and security. In addition, SANs typically play an important role in an organization.

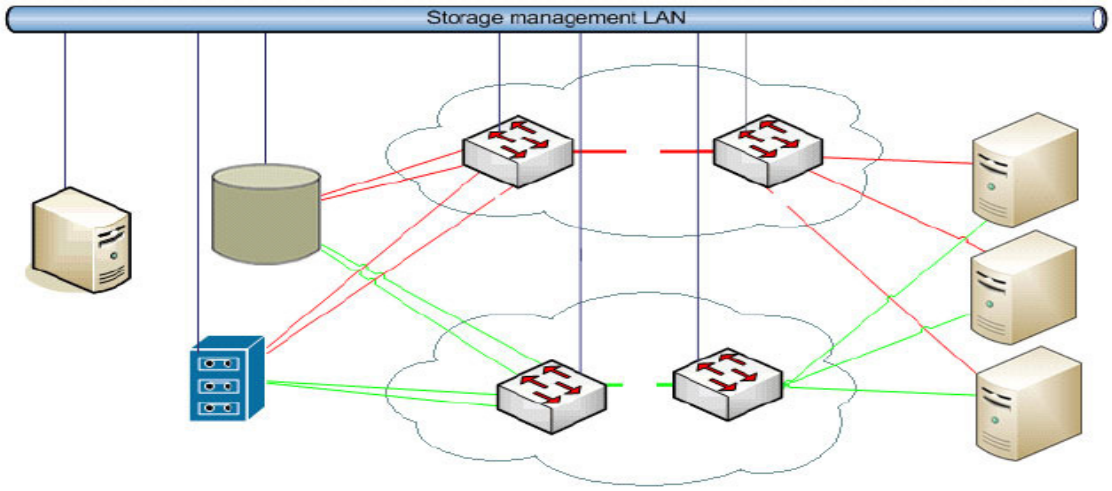

Figure 1: Storage Area Network Architectural Framework [6]

SAN is an independent network of storage systems that removes today's server-based storage installation into a scalable, high speed and direct access to the storage, without server ownership of storage subsystems [7]. The information in Fibre channel SAN that the attackers try to gain access to are as follows [10]: Domain identification; Switch name server information; World-Wide Name – WWN; FC layer-2 frame information; 24-bit address and Session control number (SCN) respectively.

4. SAN SECURITY THREAT AND WEAKNESS

A storage area network is susceptible to risk because of the critical data it passes and stores. In order to understand the threats that a SAN faces, the different levels of threat must be understood. Below are the threats associated with SAN security.

4.1 Man-In-The-Middle Type Attacks

Man in the middle attack is the act of an untrusted third party intercepting communication between two trusted entities [9]. There are several possible man-in-the-middle types of attacks to SAN such as World Wide Name (WWN) attack on the Management Admin attack in which admin password unencrypted via telnet. In MITM attack, an attacker needs some information from architecture of the network. An entity using IP, such as a switch or an operating system, will send out ARP requests when it is trying to communicate with other entities. For example, if server A wanted to communicate with server B, which has the IP address of 172.16.1.1 and the MAC address of 00-0A- CC-69-89-74, server A would send out an ARP request asking, "Who is 172.16.1.1?" Then the switch or the operating system (OS) would respond, replying with its MAC address, which is 00-0ACC69-89-74.

The issue with ARP, which we will also address with Fibre Channel name servers, is that any malicious entity could send out an ARP reply instead of the actual serve. Since there is no authentication with ARP, similar to how there is no authentication with PLOGI in Fibre Channel fabrics, an entity receiving an ARP reply from an attacker would update their routing table with the incorrect information.

Furthermore, even if a node did not send out an ARP request, which would request the MAC address of a specific IP address, it doesn't mean it won't receive an ARP reply and update its own routing table [7]. For example, a malicious user could send out ARP replies to the entire network segment, telling each entity that the MAC address of the router, which is 172.16.1.1, is actually the MAC address of the malicious entity. When one node tries to communicate to any other node by going through the default router, it will actually be going to the malicious entity first, since it is using the MAC address of the malicious entity for layer 2 routing. Several steps can be taken as protection measures against this type of attack, such as using SAN management software that encrypts password from some interfaces like Management Console, to a switch fabric. Management Console can also be placed in an isolated, dedicated network to protect it from 'Man-in-the-middle' type attack.

We can also use the FC (fiber channel) protocol which has authentication methods such as Switched Link Authentication Protocol (SLAP) and Fibre Channel Authentication Protocol (FCAP), SLAP is used to make trust area between switches that wants to connect to each other and FCAP is a public key infrastructure that use cryptographic authentication for making trusted area between switches and HBAs and do this task by exchanging the certificate between switches and fabrics [7].

4.2 Spoofing

Spoofing is another threat that is related to unauthorized access. Spoofing has many names and forms and is often called impersonation, identity theft, hijacking, masquerading and WWN spoofing [9]. Spoofing gets its names from attacking at different levels. One form of attack is impersonating a user and another attack is masquerading as an authorized WWN.

To prevent spoofing, authentication services are required to catch a lying intruder. If the intruder still manages to obtain physical access to the infrastructure and attaches a sniffer onto a link to steal data, encryption can render the stolen data worthless. The way to prevent spoofing is by challenging the spoofer to give some unique information that only the authorized user should know [11]. For users, the knowledge that is challenged is a password. For devices, a secret is associated with the WWN of the Nx_Port or switch. Management sessions may also be authenticated to ensure that an intruder is not managing the fabric or device. To authenticate every point, four types of authentication are possible, User Authentication, Ethernet CHAP Entity Authentication, CT Message Authentication, Fibre Channel DH-CHAP Entity Authentication. Spoofing can be checked at the following points of attack [12] viz:

I. Out-of Band Management Application – When a management application contacts the switch, the switch may authenticate the entity that is connecting to the switch. Authentication of the users is addressed in point of attack.

II. User to Application – When the user logs into the application, the management application will challenge the user to present a password, secret or badge. The application could authenticate the user with biometric data like fingerprints, retina

III. Devices to Fabric – When a device sends a Fabric Login (FLOGI) command, the switch could respond with a CHAP request to authenticate the user. The Nx_Port should respond to the CHAP and challenge the switch as well for mutual authentication.

4.3 Session Hijacking Attack

Access to the session between two trusted nodes by untrusted third-party attacker to gain the control to connection among them is known as session hijacking attack [12]. In Fibre Channel architecture, in order for two Fibre Channel nodes to communicate with each other, an established session must be made. The session information is managed by the Sequence Count number (Seq_CNT) and the Sequence Identification number (SEQ_ID). The Seq_ID and Seq_CNT will tie each frame to a particular session and place it in its correct order. In this attack, attacker try to corrupt the information on the name server and change them with the wrong information from the attacker node. The issue with session management starts with the lack of Fibre Channel authentication when sending or receiving frames. Any malicious user could send frames to an authorized node with the correct Seq_ID and Seq_CNT (using the source address (S_ID) as the attacker and not the original session holder) thus transferring the session's control to the malicious user [11].

In order to fully understand the Fibre Channel session hijacking attack, the following steps describe the attack process A makes an established connection with B. A and B exchange frames for communication using a Fibre Channel traffic analyzer, the malicious user, identifies the static value for the Seq_ID and the Seq_CNT number. Then injects frames to B with the Seq_ID, taken from the frames between A and B and then increments the Seq_CNT number by one, which will identify the next frame in the session. B receives the frame(s) from C and because the frames have the correct SeqID and the correct value for the Seq_CNT, the frames are regarded as the next set of frames in the session. Because the S_ID of the C's frames are from a different address, the session is then handed to that node wherever the session last left off. In conclusion, C has hijacked the session from A and now has an established connection to B without any authentication or authorization.

To mitigate and prevent this type of sophisticated attack requires deep knowledge of Fibre Channel frames and the use of a hardware and software traffic analyzer. The first step would be to enumerate the frame information from the two trusted entities using any type of Fibre Channel fabric analyzer or IP sniffer with an IP to Fibre Channel connector. For example, if a fabric loop topology had been deployed (FC_AL), the analyzer can see all the traffic in the loop of every node connected to the fabric. In a switched architecture, the analyzer would need to be connected to the core FC switch and also within the same routing segment of the target. Once the targets have been identified and enumerated by the traffic analyzer, the following fields in the header part of the frame are considered: S_ID, D_ID, OX_ID, RX_ID, Seq_ID, and Seq_CNT [13].

Within Fibre Channel layer 2, you would modify the header information with your traffic analyzer of the frame that you will generate in order to complete the attack. When crafting the frame, the S_ID would change from the original source fabric address to the fabric address of the attacker. The D_ID would remain the same, which is the fabric address of the target (while both entities are technically targets, the entity that is on the receiving end of the session is the real target) [8]. The Seq_ID field will also need to remain identical to the original in order to ensure the target node considers the frame(s) as part as the legitimate session. Unlike the Seq_ID, the Seq_CNT field will not remain identical but rather will need to be incremented by one in order for the target to consider that frame as the next legitimate frame in the session. This is probably the trickiest part of the attack; even though the act of incrementing the Seq_CNT by one is a trivial procedure, it is not as easy to determine what Seq_CNT is the last one. For example, using your traffic analyzer, you are able to view the Seq_CNT number of all sessions, but by the time you send your frame(s).

The way that can improve the risk of this attack is to examine the PLOGIN frame when they want to update their information on the name server to do not let them to interfere and change the information tables on the name server. Encapsulating Security Payload (ESP) can encrypt the Fibre Channel traffic to ensure confidentiality. Ethernet traffic can be encrypted with Secure Sockets Layer (SSL) or similar protocols. These encryption techniques can use different levels of encryption to make stolen data worthless.

5.0 EVALUATION OF SAN SECURITY BASED ON BEST MECHANISM

5.1 Challenge-Handshake Authentication Protocol (CHAP)

DH-CHAP is a secure key-exchange authentication protocol that supports both switch-to-switch and host-to-switch authentication, MD-5 and SHA-1 algorithm-based authentication. Diffie-Hellman Challenge Handshake Authentication Protocol is a password based authentication and key management protocol that uses the CHAP algorithm (RFC 1994) augmented with an optional Diffie-Hellmann algorithm. It provides bidirectional and optionally unidirectional authentication between an authentication initiator and an authentication responder. The Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a 3-way handshake [16].

The Way DH-CHAP Works

i. After the Link Establishment phase is complete, the authenticator sends a "challenge" message to the peer.
ii. The peer responds with a value calculated using a "one-way hash" function.
iii. The authenticator checks the response against its own calculation of the expected hash value. If the values match the authentication is acknowledged; otherwise the connection should be terminated.
iv. At random intervals, the authenticator sends a new challenge to the peer, and repeats steps 1 again.
v. In conclusion, this scheme is considered the best because it covers all angles of SAN including switch-to-switch, switch-to-device, and device-to-device authentication, frame-by-frame FC-2 level encryption which provides authentication, integrity and privacy protection to each frame sent over the wire.

6.0 CONCLUSION

A storage area network is only as secure as its weakest link. Therefore, every element of the SAN must be considered when addressing security needs. To ignore a weakness in the SAN would be to put critical systems and information at risk. As a result, a company puts itself at risk for losing money as well as competitive advantage. Storage area network security is a serious matter and preventative measures should be used to safeguard against any possible security hole. SAN security not only needs to be considered during the initial setup, but constant risk analysis needs to be performed throughout the SANs life cycle and dealt with on a continual basis. Knowing the security and performance features of these protocols can help the storage administrators to have better configuration on their network with the respect to performance. Security is not a single task that can do just by single configuration; security is like a chain that all the circles in this chain are needed to be connected to each other. This work can be helpful for the people who want to start working with SAN technology to have better understanding that how it works and what are security risks and their solutions to improve these vulnerabilities on SAN and about the performance aspect. Along with the positive changes that storage area networks have brought about, there are also inherent risks associated with SANs.

Companies and its customers need to be confident that information that is being routed through the storage area network is safe and secure. This is crucial as the SANs infrastructure continues to evolve. More and more businesses are moving towards a SAN solution for their storage and backups because of the benefits it offers. SAN have proven to reduce management costs as a percentage of overall storage costs.

REFERENCES

[1] Storage Area Network. Wikipedia, the free encyclopedia
[2] http://en.wikipedia.org/wiki/Storage_area_network Retrieved November 10, 2005. Storage performance, R. Lucchsi, 2008 , Network Industry Association (SNIA), www.snia.org. Storage performance, R. Lucchsi, 2008 , Network Industry Association (SNIA), www.snia.org.
[3] Storage performance, "R. Lucchsi, 2008 , Network Industry Association (SNIA), www.snia.org.
[4] Inmon,Bill, "Encrption at rest-Information managemrnt magazine article", 2012.
[5] T. Clark, "Designing storage area network'' second edition. Addison Wesley", 2003.
[6] HaronI "San Security section, para" ,2002. All San storage area network solutions, 2001, www.allsan.com.
[7] J.Tate, F.Lucchese, et R. moore, "Introduction to Storage Area Networks", Fourth edition. IBM, 2006.
[8] G. Geiselhart, R. Brennman, T. Gutenberger, J. Lafitte, W. Ventura, and S. Williams, " fiber channel protocol implementation guide", first. IBM, 2004.
[9] G.Silberschatz, "Operating System concepts, chapter 17 Distributed file systems. Addison-Wesley Publishing Company", ISBN 0-201-59292-4`,1994.
[10] H. Dwivedi," Securing storage: A practical guide to SAN and NAS security", First edition. 2012.
[11] Dwivedi, H. and Hubbard, A.," Whitepaper: Securing Storage Networks" , April 2003.
[12] Doraswamy N., Harkins D., "IPSec The New Security Standard for the Internet, Intranets and Virtual Private Networks", Prentice Hall PTR 2000.
[13] Monia, C. at al., iFCP–"A Protocol for Internet Fibre Channel Storage Networking", IETF Internet Draft, May 2003. .
[14] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994.
[15] Snively R., at al., Fibre Channel Security Protocols (FC-SP) Rev 1.3, January G31st, 2009.

Author(s)

Dr. Agozie Eneh is a Senior Lecturer in Computer Science. His research interests include computer network security, analysis of authentication protocols, performance evaluation of systems, optimization theories, and communicating sequential processes. He teaches on both the undergraduate and postgraduate programs of Computer Science, and has supervised several projects since joining the University of Nigeria. Dr Eneh has worked both in the private and public sectors of the economy before joining the world of academia.

Obi Adaobi Maria is currently an M.Sc student in the department of Computer Science, University of Nigeria, Nsukka. She obtained her B.Sc in Computer Science, University of Nigeria, Nsukka. She is skillful in programming and web design, but has been trained to be more proficient in Networking.

Mr. Uchechukwu Christian Arinze is a Doctoral candidate in Computer Science at the University of Nigeria, Nsukka. He holds B.Sc and M.Sc in Computer Science from the Ebonyi State University and University of Nigeria, Nsukka. He is currently an ICT staff at the Nigerian Nuclear Regulatory Authority (NNRA) with broad range of professional certifications in various fields of nuclear security, safety, safeguards and radiation protection from IAEA Vienna, Austria, Texas A&M University (U.S.A) and World Institute for Nuclear Security (WINS) Vienna, Austria respectively. His areas of research interests are in the development of algorithms for improved congestion control in wireless telecommunication and data communication network systems, data center costing models; numerical algorithms, optimization models and Database systems.