Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Implementing Security in Storage Area Networks– A Review

Soumya Mahalakshmi A
Student, Department of Computer Science and Engineering,
R. V. College of Engineering, Bangalore, India

Abstract -- In recent times, the demand for storage devices have increased considerably as the amount of data generated every day increases exponentially. To address this huge requirement, constant advances in storage technology are the need of the hour. Storage area networks (SANs) are a result of this drive towards innovation in storage techniques. A storage area network comprises of a high speed network of storage devices which are in turn connected to a server. Due to its excellent functionality, it has gained universal acceptance. Today, most of the data handled by large computing companies are managed on SANs. It is therefore absolutely vital to secure the data on a SAN, to maintain competitive advantage of the organization over its peers, apart from the need for privacy and protection. The aim of this paper is to understand the need for security in a SAN and the various techniques that have been identified to tackle the known security problems. The essential features of mandatory security are discussed. The possibility of using Artificial Immune Systems (AIS) to eliminate virus attacks and act as an Intrusion Detection System (IDS) in a SAN has also been discussed. The available solutions are analysed, compared and conclusions are drawn based on the loopholes in these methods and the requirements for better secured SANs in the future.

Keywords -- Storage Area Network, storage, security, mandatory security

I. INTRODUCTION

The dawn of the era of information and knowledge has resulted in an enormous amount of data being generated every day. This data has to be further stored and processed to enable companies to cater to the growing need for data analytics. This data must also be capable of being accurately accessed and processed to generate more information. The demand for storage devices and their economical worth has reached new heights. To address this huge requirement, constant advances in storage technology are the need of the hour. Storage Area Networks(SAN) is one such technology that emerged to quench this need to store, manage, process and access data efficiently and securely.

A Storage area network, or SAN, maybe defined as a high-speed network of storage devices. Also, these storage devices are connected to the servers. Applications running on any of the networked servers can access and use this storage. Due to its versatile functionality and their apparent property of being able to relieve overburdened LANs from high volumes of data, SANs have becomes overwhelmingly popular in the global market. They reduce administrative and equipment costs, provide high data availability and ensure regular backups. However, companies and its customers need to ensure the safety and security of the information that is being routed through the storage area network.

Today, most of the data handled by large computing companies are managed on SANs. Hence, it is important to place and devise security requirements in a SAN, to ensure safety of data globally. This requires one to understand the possible security threats to a SAN, which have to be eliminated to ensure 'mandatory security'. The idea of mandatory security has four main features as discussed by Benjamin Aziz, Simon N. Foley, John Herbert and Garret Swart, in their paper "Configuring storage area networks using mandatory security". They are listed below.

- Data privacy – protecting data from unauthorized readers who are not present on the network
- Data integrity – protecting data from unauthorized updates to maintain consistency of data
- Additional privacy of the data traffic – protection of data during transmission
- Prevention of an attack by an authorized user of the SAN, caused when members of the network modify data that they are not privileged to handle.[1]

In this paper, an additional feature, which would be the safety of data has been discussed. Data has to be maintained in a manner such that there is minimum risk of losing data due to unwarranted circumstances like natural disasters. Loss of data, in such cases, has to be compensated with an efficient recovery mechanism. [5]

Further, any network is also susceptible to virus attacks. Security also entails protection of SANs from viruses and worms. It has been noticed that the propagation of viruses and worms on computer networks and the proliferation of pathogens in cellular organisms are similar. [15] Banking on this evident similarity, Artificial Immune Systems (AIS) was developed. In artificial intelligence, AIS are a class of computationally intelligent systems inspired by the principles and processes of the vertebrate immune system. The algorithms typically exploit the immune system's characteristics of learning and memory to solve a problem. Security models using principles of AIS can be used to eliminate virus attacks in SANs, in a way similar to that of the vertebrate immune system which fights invading pathogens. This involves two stages.

1. Intrusion Detection- which helps to prevent known viruses from entering the network [13]
2. Immunization algorithms- which help to contain the spread of the virus and prevent it from attacking more nodes in the network [19]

It is evident that certain security requirements have to be placed on the SAN to arrive at an acceptable SAN configuration that will maintain security. There are various feasible models based on the above criteria that have been proposed by several authors. These solutions and models have been listed, analysed and compared in this paper.

Mohammed Haron, in his paper "Is your storage area network secure? An overview of storage network from security perspective" also emphasises on the need for security measures in a SAN. He says that physical isolation and exclusivity of the SAN is not enough to maintain security in a SAN as more often than not, multiple departments may be sharing the same SAN resources. Therefore, security measures are necessary. A good SAN ensures that data is confidential and available at all times. [2]

Colleen Rhodes, in his paper, "Security consideration for storage area networks", provides a new angle on the need for security. He stresses on the ethical issues surrounding SAN security. He mentions that, laws such as the Sarbanes-Oxley Act of 2002 and The Health Insurance Portability and Accountability Act of 1996 (HIPAA) make an organization responsible and accountable on how they process and store information. He goes on to state that SAN security is not only important for an organization to maintain competitive advantage, but it is also a responsibility for organizations under the law. [4]

He also believes that a SAN is only as secure as its weakest link and advices that SAN security needs to be considered during the initial setup as well as during the SAN's life cycle.

According to the data compiled by Mohammed Haron from various surveys, a compromise on implementing security in networks proves to be immensely expensive later. This is evident from the survey conducted by International Data Corporation (IDC) which deduced that the number of IT personnel responsible for administering storage and systems is growing at only 5% per year while the requirement for stored data is growing at 80% annually. Also, incidents reported by Cryptec Secure Communications on Enterprise Security showed that, 85% of computer crimes originated inside the network. Moreover, the FBI states that the average cost of an insider breach can be as large as $2.4 million whereas that of a break-in from the Internet is only $27,000. [2]

Therefore, it is evident that the need to implement security in a SAN is of utmost importance. While Benjamin Aziz and team elucidate on the potential security threats to a SAN, Mohammed Haron quotes statistical data to prove the importance of SAN security economically and globally. Colleen Rhodes on the other hand, stresses that SAN security is now the responsibility of organizations under the law. He also mentions the importance of ensuring security beyond the initial setup, by constantly updating and maintaining the security arrangements.

II. DESCRIPTION

Benjamin Aziz and his team provide solutions to implement the basic security requirements that were listed earlier in the introduction. Their suggestion involves securing each of the devices used to provide the SAN service, thereby yielding to the first three security requirements that constitute mandatory security. A combination of security kernels and firewalls are used to ensure that only authorised client machines can use the service and access the SAN Therefore, two levels of security must be breached before an attack takes place.[1]

However, security threats need not always adhere to the four types specified above. Mohammed Haron explains that some types of attacks are specific to a SAN. These may be

- **Man-in-the-middle type of attack**

Time and again, it has been proved that an insider breach is the most dangerous attack against data security. Hence, this type of attack can prove to be detrimental, and should not be taken for granted. This attack can occur in two ways, World Wide Name (WWN) attack on the HBA and Management Admin attack.

When a machine with different HBA and WWN ID is gaining access to unauthorized storage resources through the SAN network, then a WWN attack is said to have occurred. The solution that the author offers is to bind a particular WWN to a specific switch port or set of ports using Device Connection Controls, thereby preventing ports in another physical location from assuming the identity of an actual WWN.

When the Administrator password is obtained by the users of a network by using sniffer software that snatches passwords in the network, then this is termed as a SAN management attack. The solution Mohammed Haron suggests is to use SAN management software that encrypts password from some interfaces like Management Console, to a switch fabric.

- **SNMP vulnerabilities**

Simple Network Management Protocol (SNMP) is a protocol where current operational state of devices in a network is communicated to a central system. However, this protocol has been considered as insecure and this was also proven by The Oulu University Secure Programming Group in Finland. Unfortunately, many SAN products have been supporting this protocol for a long time. Thankfully, in recent times, SAN vendors tend to implement higher-level functions using proprietary technology. [2]

It is known that a storage area network is typically assembled using three principle components: cabling, host bus adapters (HBA) and switches. Mohammed Haron suggests that while these components are bought, security requirements must be taken into consideration. [2]

Ensuring privacy of data during storage as well as during transmission in a SAN were emphasised to be important for the concept of mandatory security. One approach to data privacy as described by Benjamin Aziz and team is to encrypt the data before the application writes it to the dataset. Encryption is a popular technique of scrambling the contents to enhance the security of a message or file so that it can be read only by someone who has the right encryption key to unscramble it. [1]

Computer encryption systems generally belong in one of two categories:

- Symmetric-key encryption
- Public-key encryption

Data integrity was another requirement specified as mandatory. It comprises of three conditions. These are

1. Prevention of redundancy in data
2. Prevention of inconsistency in data
3. Prevention of unauthorized updates

To preserve data integrity, it is vital to use storage resource management tools. Storage resource management (SRM) are applications that have been designed to monitor and manage SAN resources that are physical and logical. SAN management tools are available from McData Corp., EMC Corp., Hewlett-Packard Co., Symantec Corp. (Veritas), IBM, CA Inc. and Sun Microsystems Inc.

Functions of an SRM program include SAN performance analysis, data storage, storage virtualization, data collection, storage provisioning, data backup, forecasting of future needs, data recovery, user authentication, maintenance of activity logs, management of network expansion and protection from hackers and worms.

According to the final security requirement, users of the network must be able to access and use only those resources they are entitled to use. Implementing this requirement ensures that insider breaches are avoided, and this can be achieved in many ways.

One common solution to prevent unauthorized access as suggested by Mohammed Haron is to mask the Logical Units (LUNs) that are not legitimately available to users. This can be done in various ways. [2]

The Host Bus Adapter (HBA) level can be masked by using HBA drivers that contain a masking utility that uses the WWN supplied with each HBA. However, he mentions that the above has a limitation. This method requires coordination for a large SAN island with large number of hosts and a large number of LUNs on the storage devices. [2]

Another popular approach is zoning. Zoning of servers and LUNs can be done through Fibre Channel switch, which allows a given server to access only a certain set of storage elements and not those of another server. This method is advantageous as it is expandable and can control a large number of servers. [2]

Benjamin Aziz and team also provide a solution to prevent an attack by an authorized user of the SAN. It is known to usually take place when a wide range of organizations share large enterprise SAN environment, where these different organizations are often competitors. [1]

They proposed a mathematical model to configure a secure SAN and explained that a SAN is composed from the following elements, as illustrated in Figure 1, where the terminal connectors express many-one and many-many relations among the different elements of the model.

As shown, disks, disk controllers, logical volumes, datasets, applications, streams, servers and switches are sets. Some functions are defined as follows. partOf : DISK → LV

serves : CNTR → (LV)

storedOn : DATASET → LV

runsOn : APP → SERVER

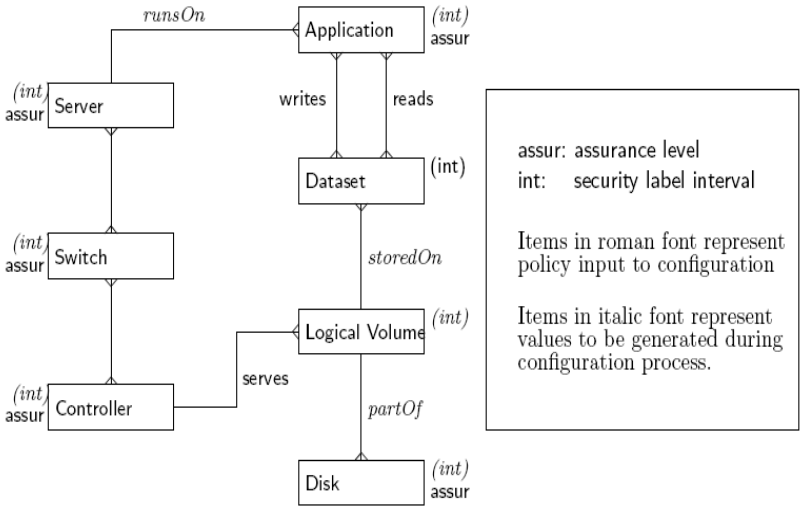

Figure 1. The structure of a SAN

Courtesy : "Configuring storage area networks using mandatory security", Benjamin Aziz, Simon N. Foley, John Herbert, Garret Swart

They introduce the concept of a label-based security policy, which is a lattice of security labels. They state that int(e) = [x, y] means that an entity, e, can be trusted to properly manage multilevel information within the security interval, [x, y]. Solving the configuration problem will result in finding values for the partOf, serves, storedOn, runsOn functions that define a particular instance of a SAN system. [1]

Henceforth, it can be inferred that while Mohammed Haron made some hardware based and architectural changes to prevent insider breaches, Benjamin Aziz and team propose a mathematical model for organization of data, to achieve the same goal.

Security also entails data safety. This essentially means that data has to be preserved safely even in the event of disasters and other unforeseen circumstances. Sandeep P. Abhang, and Girish V. Chowdhay, in their paper 'WDM-Based Storage Area Network (SAN) for Disaster Recovery Operations' suggest a Wavelength Division Multiplexing (WDM) technology-based SAN for all types of Disaster recovery operations. It maintains and initiates the recovery of data when all the paths in the network, the main SAN site and all backup sites fail due to the effect of natural disasters such as earthquakes, fires and floods, power cuts. [5] It is illustrated in Figure 2.

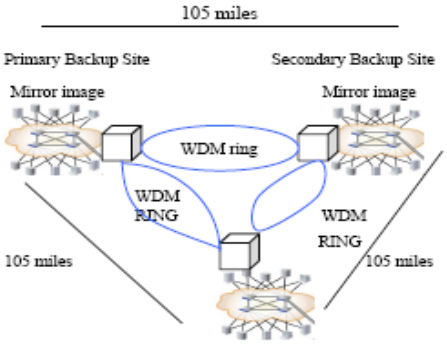

Figure 2. Architecture of proposed WDM-based SAN

Courtesy : "WDM-Based Storage Area Network (SAN) for Disaster Recovery Operations", Sandeep P. Abhang, and Girish V.

Lastly, it is of utmost importance to protect any network from viruses and worms, largely due to the scope and ease of spread which can result in heavy damage, compromising on security. Hence, a SAN is also susceptible to viruses and worms, whose adverse effects are being eliminated through the innovative use of emerging technologies, such as an Artificial Immune System.

The key to the functioning of the AIS is to identify the working of the vertebrate immune system. This idea has been explored by Sanjay Goel and Stephen F.Bush, in their paper, "Biological models of security for virus propagation in computer networks". They explain that the human immune system uses the underlying principles of detection, recognition and pattern matching match the patterns of complementary protein structures of the antigen and the detector. They also mention that the genetic mechanism in the thymus and bone marrow generate proteins with different physical structures. [15]

They further elucidate on the working of viruses to explain their work. Virus detection systems use the mechanism gleaning a piece of code to obtain any portion of the code called 'signature', that is a characteristic of the virus. The signature is usually a pattern that specifies the behaviour of the virus, and hence can be identified by the virus detection systems by matching it against the known database of virus patterns. As new virus strains are released, the database in virus detection programs becomes obsolete. [15] This necessitates the requirement of an algorithm that can detect strains of viruses that have been derived from older viruses. The Genetic Algorithm can hence be used, to detect such intruding viruses. The method has been described in detail and implemented by Karamjeet Kaur and Er. Navdeep Singh in their paper, "Genetic Algorithm based Detection of Malicious Activities in the Network", which yielded the following results. [13]

TABLE I ACTUAL NUMBER OF INTRUSIONS AND DETECTED INTRUSIONS

Population size	Actual number of intrusions	Intrusions detected by proposed method	Percentage
50	181	130	68.78
100	380	311	81.84
150	1424	1176	82.58
200	1806	1611	89.2
350	1851	1588	85.75
440	1895	1790	94.45
Average percentage			**83.77**

Courtesy : "Genetic Algorithm based Detection of Malicious Activities in the Network", Karamjeet Kaur, Er. Navdeep Singh

Cai Tao and Ju ShiGuang, ZhenJiang, in their paper, "Two-layered Access Control for Storage Area Network", elucidate on the introduction of an artificial immune algorithm to detect abnormal access request, thereby implementing two-layer access control in a SAN. The two layers are

1. Top access control module in metadata server which generate all detectors and preserves many of them.
2. Lower access control module in intelligent disk, which preserves a small number of detectors. [6]

An AIS based data storage model specially adapted for the SAN, called AIS-DS, has been proposed and explained by Lei Wang, Yinling Nie, Weike Nie and Licheng Jiao, in their paper, "Artificial Immune Strategies Improve the Security of Data Storage". Here, each user of the SAN has a special code assigned to them called a 'vaccine'. It also ensures data integrity and privacy, both of which were discussed to be essential for mandatory security. [7]

We can gather that AIS has been used in different ways to achieve the goal of eliminating viruses and worms. While the first two techniques implement a mechanism to detect virus strains and prevent their intrusion, the third technique emphasizes on the need for specific model of storage to enhance security. The concepts of genetic algorithms and access control had been explored as options for implementation.

However, if the virus has already entered the network, it becomes important to contain its spread and minimize the damage and the area that will be affected. The solution to this has been explored by George Giakkoupis, Aristides Gionis, Evimaria Terzi and Panayiotis Tsaparas in their paper, "Models and Algorithms for Network Immunization". The solution is general for all networks and is called an Immunization algorithm. They have modelled two models of virus spread using graph theory. [19]

1. The *independent-cascade model*
2. The *dynamic-propagation models*

The immunization algorithm is now used to immunize a set of nodes. An immunized node cannot receive or transfer the virus. The efficiency of the above algorithm for SAN is yet to be tested.

Hence, it is evident that AIS is an innovative emerging technology that can be efficiently utilized in versatile ways to ensure security in SANs. [19]

III. CONCLUSIONS

- Storage area networks have become highly popular and have gained universal acceptance. Since they are now used in highly critical systems and handle sensitive data, compromising on its security will have far reaching consequences. Hence, implementing security in a SAN is of utmost importance.
- With the advent of advanced technology to improve the functionality of a SAN, there has also been a fair share of issues, threats, attacks and security breaches in a SAN.
- Ensuring security is a continual cycle. It requires constant updates throughout its life cycle and not just during the initial setup.
- The major security issues come under four categories, data privacy, data integrity, privacy of data traffic and prevention of an attack by an authorized user. Further, there are certain attacks specific to a SAN like Man-in-the-middle type of attack and SNMP vulnerabilities. Different techniques have been proposed by various authors to tackle these issues and these have been compared and analysed.
- Insider breaches prove to be most expensive. Architectural changes as well as organizational changes using mathematical models have been proposed by various authors to tackle this issue.
- Security also implies data safety. Hence, recovery of data during disasters is also essential. WDM-based SAN makes disaster recovery operations possible.
- Security entails prevention of attacks from viruses and worms. It was seen that using the concepts of working of human immune system, an analogy was drawn to obtain the solution to provide network security for a SAN using AIS. Hence, when a known virus attacks the system, it uses pattern matching to identify the virus's signature and prevent it's intrusion. However, if the virus has been mutated and is not known, the genetic algorithms have to be employed to obtain the desired result.
- In the meantime, if the virus has spread to other nodes in the network, then immunization algorithms, obtained by studying virus spread models, are used to contain their spread.
- AIS based intrusion detection model for two-layer access control as well as effective data storage (AIS-DS) have been considered.
- A SAN can revolutionize the future of the computing world. It is, therefore, absolutely vital to let this technology flourish with no hindrances from security obstacles.

REFERENCES

[1] "Configuring storage area networks using mandatory security", Benjamin Aziz, Simon N. Foley, John Herbert, Garret Swart

[2] "Is your storage area network secure? An overview of storage area network from security perspective", Mohammed Haron

[3] "Storage area network overview", Stephen J. Bigelow, www.computerweekly.com

[4] "Security consideration for storage area networks", Colleen Rhodes, East Carolina University
[5] "WDM-Based Storage Area Network (SAN) for Disaster Recovery Operations", Sandeep P. Abhang, and Girish V. Chowdhay
[6] "Two-layered Access Control for Storage Area Network", Cai Tao, JuShiGuang, ZhenJiang, 2009 Eighth International Conference on Grid and Cooperative Computing
[7] "Artificial Immune Strategies Improve the Security of Data Storage", Lei Wang, Yinling Nie, Weike Nie, Licheng Jiao, ICNC 2005, LNCS 3611, pp. 839 – 848, 2005
[8] "An Artificial Immune System Architecture for Computer Security Applications", Paul K. Harmer, Paul D. Williams, Gregg H. Gunsch, and Gary B. Lamont, IEEE Transactions On Evolutionary Computation, Vol. 6, No. 3, June 2002
[9] "Unknown non-self detection & robustness of distributed artificial immune system with normal model", 2008 , Page(s): 1444 – 1448, IEEE
[10] "Research on immune pathology in artificial immune system", Xuanwu Zhou, 2009 , Page(s): 1366 – 1370, IEEE
[11] "A multi-layer network defense system using artificial immune system", Elhaj, M.M.K. ; Hamrawi, H. ; Suliman, M.M.A., 2013 , Page(s): 232 – 236, IEEE
[12] "Network Intrusion Detection Method Based on High Speed and Precise Genetic Algorithm Neural Network", Jingwen Tian, Meijuan Gao, Volume 2, Page(s): 619 – 622, IEEE
[13] "Genetic Algorithm based Detection of Malicious Activities in the Network", Karamjeet Kaur, Er. Navdeep Singh, International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume 3, Issue 11, November 2013
[14] "Artificial Immune System (AIS) Research in the Last Five Years", D. Dasgupta
[15] "Biological models of security for virus propagation in computer networks", Sanjay Goel, Stephen F.Bush
[16] "Components Based Key Management Algorithm for Storage Area Networks", P.Mahalingam, Dr.N.Jayaprakash, Dr.S.Karthikeyan
[17] "ARTIFICIAL IMMUNE SYSTEMS – MODELS, ALGORITHMS AND APPLICATIONS", J.R. Al-Enezi, M.F. Abbod, S. Alsharhan
[18] "Building Secure SANs", Ron Dharma, Veena Venugopal, Sowjanya Sake, Vin Dinh, EMC^2 Techbook, Version 4.0
[19] "Models and Algorithms for Network Immunization", George Giakkoupis, Aristides Gionis, Evimaria Terzi and Panayiotis Tsaparas
[20] "A Storage Area Network Analysis and Design Methodology", Alicia Mackey

