Running Head: SECURITY CONSIDERATIONS FOR STORAGE AREA NETWORKS

Security Considerations for Storage Area Networks

Colleen Rhodes

East Carolina University

Abstract

In this paper I will describe Storage Area Networks (SANs) and the benefits they can bring as well as the emerging need for them in businesses today. I will discuss the importance of SAN security and why it is crucial for protecting a company's assets. 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 Considerations for Storage Area Networks

What is a SAN?

As Wikipedia, the free encyclopedia (2005) explains it, "a storage area network (SAN) is a network designed to attach computer storage devices such as disk array controllers and tape libraries to servers." SANs support disk mirroring, backup and restore, archival and retrieval of archived data, data migration from one storage device to another, and the sharing of data among different servers in a network. According to the GIAC Security Essentials Certification (2003, What is a San section, para. 1),

> A Storage Area Network establishes a direct connection between storage element and servers or clients. This concept is similar to a Local Area Network (LAN) with the exception of allowing greater storage capacity and faster subnetworks. A SANs device allows multiple direct host connections or connections through a fiber hub or switch.

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. Biran, O., Meth, K., Sarkar, P., Satran, J. & Voruganti, K. (2003, Benefits section, para. 3) report,

> In a storage area network, it is possible to perform LAN-free and server-free backup operations that copy data from a storage device directly to another storage device without transferring the data across the general-purpose network and the

servers. In other words, data are sent across the dedicated storage area network directly between the source and destination storage devices.

The Need for SANs in Businesses

"Storing data has become an increasingly important and complex issue thanks to concerns about capacity, accessibility, security, and of course, cost." (Starkman, 2005, ¶4) More and more businesses are moving towards a SAN solution for their storage and backups because of the benefits it offers. McNamara (2005, ¶6) reports, "SANs…have proven to reduce management costs as a percentage of overall storage costs." By consolidating storage in a SAN, a business can reduce the number of physical devices to manage, reduce complexity, centralize storage management tasks, simplify growth and expansion and maximize storage utilization and return on investment. Sarker et al. also points out that "having a separate storage area network also makes it easier to both secure and manage storage traffic, as there is no interference from the general network traffic."

In the past, most businesses relied on a decentralized storage network with many dissimilar network-attached storage (NAS) devices deployed throughout the organization. With traditional centralized storage, each server is connected to a separate storage device. This can result in multiple storage devices with some being under utilized while others are near capacity. With storage area networks, data is consolidated into a single storage pool that all servers in the SAN can access directly. This can save a company money by

increasing the efficiency, flexibility, and scalability of that organization's existing storage resources.

Essentially, a storage area network will transfer network storage from a file server to a network separate from the local area network (LAN). Walder (2002, What is the Storage Area Network section, para. 2) explains that "a SAN is thus a dedicated storage network that carries I/O traffic only between servers and storage devices – it does not carry any application traffic, which eliminates the bottlenecks associated with using a single network fabric for all applications." Removing bottlenecks from the network allows employees to do their work more efficiently. It also permits customers to do business with the organization without the inconvenience of network congestion.

Along with cost savings to the organization and increasing the efficiency of its local area network, a SAN can also provide superior scalability options. Since it is no longer necessary to have separate storage devices attached to individual servers, SAN administrators can scale their storage requirements as needed. This is true for tape backup in the SAN as well. In addition, servers and storage can be added independently without affecting disrupting applications' ability to access data.

Importance of SAN Security

Before an organization can safeguard the storage area network from threats, it must first understand the importance of SAN security. McDATA (2005, Introduction section, para.

1) says it best when they report that “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.”

As Haron (2002, San Security section, para. 1) points out,

> 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.

In addition to the aforementioned reasons of SAN security importance, laws such as the Sarbanes-Oxley Act of 2002 and The Health Insurance Portability and Accountability Act of 1996 (HIPAA) make an organization accountable on how information is processed and stored. Storage area network security is not only important for an organization looking out for their best interests, but it is also a responsibility for many organizations under the law.

Threats to a SAN

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. McDATA (2005, Threat Levels section, para. 1) reports,

> Threats can be broken up into three basic levels. The first level of threats is unintentional and due to accidents or mistakes…The second level of threats is a simple malicious attack that uses existing equipment and possibly some easily obtained information. These attacks are…usually from internal sources. The third level of threat is the large scale attack that requires an uncommon level of sophistication and equipment to execute the attack…Third level attacks are extremely rare in SANs today and may take considerable knowledge and skill to execute.

Level One Threats

Although level one threats are unintentional, they are just as serious, if not more so than the other threats because they are the most common in the workplace. Serious consequences can happen as a result of these mistakes, such as downtime and loss of revenue. Luckily for SAN administrators and for security concerns, level one threats are the easiest to prevent.

Simply plugging in a wrong cable, or for that matter unplugging a correct cable, can cause a level one threat. Therefore, the easiest way to avert this from happening is to

limit physical access to the SAN environment. This is not only best practice for preventing accidents, but also for securing against malicious threats to the SAN.

Storage area network switches have an Ethernet port and serial port that can be used for management purposes. To further secure physical access to the SAN, one can "[create] a private network to manage the SAN that is separate from a company's Intranet. If the switch is connected to the company Intranet, Firewalls and Virtual Private Networks can restrict access to the Ethernet port." (McDATA, 2005, Unauthorized Access section, para. 2) User authorization and authentication can be used for serial port access. These protective measures used for physical security can avert staff who know just enough to be dangerous, as well as any illicit users from accessing the SAN.

It is not enough to just secure physical access to the SAN. Logical access must be controlled as well. Just as a private network can avoid unauthorized users from accessing the SAN, other measures can be taken to protect the SAN once users have physical access. "Controlling access with Access Control Lists (ACLs) prevents accidents from leading to catastrophes." (McDATA, 2005, Unauthorized Access section, para. 10). Access Control Lists can provide a basic level of security to the SAN by restricting access to certain hosts.

There are many ways that Access Control Lists can be used to secure the storage area network. A few examples of using ACLs in a SAN given by Brocade ("Advancing Security," 2005, Key Components in a SAN Security Framework section, para. 1) are:

- Management Access Controls: Management policies and ACLs control access to the switch from different management services
- Switch Connection Controls: ACLs and digital certificates within the switch authenticate new switches and ensure that they can join the fabric
- Device Connection Controls: Port-level ACLs lock particular WWNs to specific ports.

Physical security and logical security are not only ways to prevent Level One threats, but they are also a good foundation for preventing Level Two threats. It is always best practice to take the necessary actions to prevent accidents or mistakes caused by Level One threats. However, Level Two threats deal with people who have malicious intent. In this case, security needs to be taken to a new level.

Level Two Threats

Level Two threats usually involve internal sources. There are many motives behind these attacks such as a disgruntled employee looking to destroy information or someone looking to gain profit or an advantage from the information obtained. Preventive measures used against Level One threats can help thwart off Level Two attacks. However, a person who "maliciously tries to steal data or cause disruption of service" (McDATA, 2005, Threat Level section, para. 3) is not only going to look for easily accessible information, but he or she may deceive in order to get that information.

There are numerous ways an intruder can swindle his or her way into getting information under false pretenses. Posing as an authorized user or device could result in gaining

access to the SAN. This is also known as spoofing. "The way to prevent spoofing is by challenging the spoofer to give some unique information that only the authorized user should know." (McDATA, 2005, Spoofing section, para. 2). Verifying that the information given is genuine is referred to as authentication. Authentication requirements should not only apply to users, but also to the devices and applications. Authentication should be in place for user access to the management interface, management console access to the fabric, server access to the fabric, and switch access to the fabric.

Authentication is an excellent prevention mechanism in theory. However, it should be noted that

> The strength of any authentication mechanism is based on the quality of the implementation and the strength of credentials. If the credentials are weak, or if authentication data is exposed due to faulty implementation, the mechanism itself can and will be defeated. (Dwivedi & Hubbard, 2005, Authentication section, para 3)

Zoning is a method of arranging storage area network devices into logical groups over the physical configuration of the fabric. Zoning adds another level of security to a storage area network because it controls access to a SAN from a host device. Only devices that are authorized to access a particular storage resource are allowed to do so. "Accessibility of data can be restricted by the administrator to certain users to prohibit sensitive information from being read by those who are not authorized to read it." (Bhatt, 2003,

Zoning section, para. 3) Zones not only provide security to the SAN by restricting access, but they allow maintenance to be performed to certain areas of the SAN without disturbing any other groups.

Authentication and zoning are very important in preventing Level Two threats. Still, if the intruder can access the data while in transit, then zoning and authentication won't help. Packet sniffing on a computer network is similar to wire-tapping a phone network. Sniffing is difficult to detect, so it is very important that the data is encrypted in order to avoid this security threat.

As Dwivedi & Hubbard (2005, Encryption section, para. 3) explain,

> As a security best practice, storage environments must have the ability to encrypt data both in transit and at rest…Steps should be taken to ensure that data is encrypted before it even reaches the storage network…This is especially important for users of shared storage environments.

Although sniffing is considered a Level Two threat, if the perpetrator has the equipment to crack encrypted data then it can be considered a Level Three threat.

Level Three Threats

It usually requires expensive equipment and a high level of skill to cause a Level Three threat. Even though these types of attacks are rare, they are the most taxing on a storage area network. These types of attacks are usually from an external source and take a great

amount of effort to execute. Therefore, theses types of attacks are the hardest to defend against.

As mentioned earlier, using equipment to crack encrypted data would be an example of a Level Three threat. The only way to prevent this threat is take the necessary precautions to avoid data from being stolen. Physical and logical access, as discussed before, are crucial aspects that need to be addressed when taking into consideration security for a storage area network.

Another example of a Level Three threat would be a Denial of Service attack. Bhatt (2003, Types of Attacks on Storage Area Networks section, para. 3) defines a Denial of Service attack as "overloading its target system to impair its ability to communicate with the authorized user as well as delay response of the system to the requested command."

In order to protect a storage area network against Level Three threats, the storage area network must have the proper security groundwork to protect itself against Level One and Level Two threats. Since Level Three attacks are so uncommon and complex, it is difficult to discuss protecting the SAN from them in the scope of this paper. The best practice is to do a constant risk analysis on the SAN and to fix any security holes as quickly as possible.

Conclusion

Businesses are relentlessly fighting the problems associated with managing high volumes of data on overburdened LANs. These problems include trying to reduce administrative and equipment costs while adhering to high availability requirements for mission-critical applications. Storage area networks help with these problems even as freeing up network capacity by doing backups and writing to disk quietly behind the scenes. Storage area networks allow Information Technology (IT) managers to do more with less and as a result, save the organization money.

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. Along with other reasons mentioned in this paper, organizations are also being held responsible for the sensitive data they transmit and store with such laws as the Sarbanes-Oxley Act of 2002 and The Health Insurance Portability and Accountability Act of 1996.

Security, whether it is for a storage area network or anything else, is not something that can be set up once and then forgotten about. Security is an incessant process. As Bhatt (2003, Conclusion section, para. 1) summarizes, “Proper management of the SANs is an ongoing task to ensure that data quality has not been tampered with or that the level of security has not been compromised.”

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.

References

Advancing Security in Storage Area Networks: The Growing Security Concern. (2005). Brocade. Retrieved November 18, 2005 from http://www.brocade.com/san/Feature_Stories/advancing_security.jsp

Bhatt, Neha. (2003). *GIAC Security Essentials Certification (GSEC)*. Storage Area Networks and Security. SANS Institute 2003. Retrieved November 10, 2005 from http://www.giac.org/certified_professionals/practicals/gsec/2900.php

Biran, O., Meth, K., Sarkar, P., Satran, J. & Voruganti, K. (2003). *Internet Protocol Storage area network.* IBM Systems Journal Volume 42, Number 2, 2003 Storage Systems. Retrieved November 11, 2005 from http://www.research.ibm.com/journal/sj/422/sarkar.html

Haron, Mohammed. (2002). *Is Your Storagae Area Network Secure? An overview of Storage Area Network from security perspective.* Retrieved November 20, 2005 from http://www.sans.org/rr/whitepapers/storage/516.php

Dwivedi, Himanshu, & Hubbard, Andy. (2005). *The Storage Security Problem.* Information Storage & Security Journal Volume 2, Issue 1. Retrieved November 19, 2005 from http://issj.sys-con.com/read/48056.htm

McDATA. (2005). *Risks and Threats to Storage Area Networks.* Retrieved November 10, 2005 from http://www.mcdata.com/downloads/mkt/wpaper/wp_risks_threats_to_SAN_328.pdf

McNamera, Michael. (2005). *Deploying a SAN to Centralize Storage Across the Enterprise*. Information Storage + Security Journal. Retrieved November 10, 2005 from http://issj.sys-con.com/read/130104_1.htm

Starkman, Neal. (2005). *Go Ahead and Back Up.* T.H.E. Journal Online. Retrieved November 10, 2005 from http://www.thejournal.com/thefocus/featureprintversion.cfm?newsid=51

Storage Area Network. (2005). Wikipedia, the free encyclopedia. Retrieved November 10, 2005 from http://en.wikipedia.org/wiki/Storage_area_network

Walder, Bob. (2002). *Storage Area Network Overview.* Techonline. Retrieved November 18, 2005 from http://www.techonline.com/community/ed_resource/feature_article/20663?print