Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

SAN - Beyond segmentation

The following paper seeks to outline the security issues surrounding the implementation of a Storage Area Network. It will explain some of the current methods that are used to secure Storage Area Network (SAN's) and explain some of the problems these approaches have in securing SAN's at present. It will then go on to investigate the technology that many of the vendors are now bringing to market that seek to alleviate the issues highlighted with earlier attempts at SAN security. Finally it will outline some steps that c...

Copyright SANS Institute

Author Retains Full Rights

AD

Etienne De Burgh

GSEC Practical Version 1.4b

December 7th, 2003

SAN Security – beyond segmentation

Contents

Abstract....1
Why SAN Security?....1
What is a SAN?....2
SAN Vulnerabilities....4
Methods of SAN Segmentation....7
The Problems of Fibre Channel....9
SAN devices and LAN connections....11
IP based Storage Area Networks....12
What are the Vendors proposing....14
Conclusions and What can you do now?....16
References....17

Abstract

The following paper seeks to outline the security issues surrounding the implementation of a Storage Area Network. It will explain some of the current methods that are used to secure Storage Area Network (SAN's) and explain some of the problems these approaches have in securing SAN's at present. It will then go on to investigate the technology that many of the vendors are now bringing to market that seek to alleviate the issues highlighted with earlier attempts at SAN security. Finally it will outline some steps that can be undertaken to secure a SAN beyond segmentation.

Why SAN Security?

Storage Area Networks (SAN's) are becoming increasingly popular as a technology that allows data to be consolidated onto fewer devices and as a technology that provides high performance connectivity to storage medium. Organisations see SAN's as a mechanism to save costs and to provide greater access to data. The concentration of data onto fewer devices rather than data being distributed around a company's network means that a single security breach can have far greater consequences for an organisation. Frequently the most important data a company possesses will be placed on a SAN and as such ensuring appropriate security is in place, is crucial to protect this data. This point has been expressed in a recent article on 'Why you need (more) storage security' by Nancy Marrone. She states,

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> The recent focus on storage security stems from a greater awareness of the value of data to an organisation and the reality that security breaches can compromise valuable company information. [3]

Threats to SAN's come from a variety of different sources and some of these are already well known, such as issues with IP and arise from SAN components also being connected to LANs and WAN's. Others are threats that relate purely to a SAN implementation, such as weaknesses in the Fibre Channel protocol stack.

To look at these threats we will need to examine what a SAN actually is and how it is put together.

Briefly, a SAN consists of a number of components, Servers with Host Bus Adapters (HBA's), Switches or Hubs and Storage Devices. There may also be a form of management device to configure these components. All these components are linked together to form a SAN in a similar way to the components that are typically linked to form a LAN, Servers, PC's and Switches/Hubs. Usually this linkage is established with fiber optical cabling and the use of the Fibre Channel protocol suite rather than IP. However, Fibre Channel can be run over copper cabling and other protocols can be used on optical cabling such as Gigabit Ethernet and IP to form a SAN.

With emerging technology such as iSCSI, InfiniBand and DAFS, SAN's are evolving to use a variety of interconnects, standards and technologies.

This paper will concentrate on the most common SAN's which are based on Fibre Channel with a fabric topology, but will look to what the future may bring for SAN's and security.

Threats to a SAN can arise as attacks to any of the SAN components but are usually of the following nature. The attacker will seek to gain unauthorised access to data, the attacker will seek to destroy or change data or the attacker will seek to affect the availability of data to legitimate users.

What is a SAN?

A SAN is a network that exists purely to connect devices to storage. Unlike a LAN which facilitates many different types of communication for different purposes a SAN is dedicated to the needs of storage. A typical SAN will be a discrete network and will have a number of servers with one or more HBA's that provide connectivity to the optical cabling. These HBA's will be configured with a World Wide Name (WWN), in a similar fashion to a MAC address on a Network Interface Cards (NIC's), that uniquely identifies that HBA and its host. As explained in Storage Area Networks for Dummies,

> The WWN is a 64-bit hexadecimal number coded onto each device on the network. The WWN is often assigned via a block of addresses that

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> a manufacturer can use on its products. The manufacturer stamps the name into the hardware for every device used in a SAN. [1]

Also present will be a disk array and usually a tape array of some description. This array may have intelligent controllers that provide RAID functionality or it may just be a bunch of disks (JBOD). If it is JBOD then another device usually provides the logic for RAID implementation, such as a separate SAN management appliance. This disk array will also be configured with one or more WWN. In addition the disk array will typically present a series of Logical Unit Numbers (LUN's) to the SAN and the servers attached to the SAN. LUN's are the basic unit of storage on a SAN,

> A Logical Unit Number represents the storage space in disks that are assembled into a RAID set. A logical disk can be created either from all the space in a RAID set or just from a slice of the space, called a *partition*. [1]

LUN's are the pieces of disk that you want your servers to be connected to and see as if they were locally attached. Connecting the servers and disk array will be a Fibre Channel Switch or Hub. This connectivity between servers, switches and disk array is accomplished using a Fibre Channel network topology running over fiber optic cables. There are a number of different Fibre Channel networking topologies

> …the simplest and least expensive of which is *point-to-point*. The most expensive and complex Fibre Channel topology is the *fabric* topology, but it also has the greatest amount of functionality. The remaining topology is *arbitrated loop*, which fits right between point-to-point and fabric with regards to cost and functionality. [2]

Early SAN's frequently used arbitrated loop as their topology, now however a fabric topology is by far the most common used. The Switch will also have one or more WWN defined. Usually the switch will have a WWN assigned to each of its ports. When a device connects to a fabric, by being attached to a switch port it also receives a dynamic 24-bit address the S_ID or native Address Identifier. Fabric switches have different types of ports defined that perform distinct functions and these are explained below.

> There are three basic types of ports: the N_Port, the F_Port and the E_Port……an N_Port is a node port, or a port on a disk or computer. If a port is only an N_Port…it can communicate only with another N_Port on a second node or to an F_Port on a switch…..an F_Port is a fabric port, which is only found on a switch…..and E_Port is an expansion port on a switch that connects one switch to another switches via their E_Ports to form a large fabric.[2]

The importance of these different types of ports is explained later. The switches will also be running a service called the simple name server. This is used to store the WWN of every device attached to the fabric and the switch port it is attached to. Devices use the simple name server service to look up

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the WWN of a device and its associated switch port using S_ID so that data can be transmitted between the devices.

To summarise a SAN is usually a separate network that runs over fiber optical cabling that connects servers to shared storage. These servers are usually also connected to one or more Local Area Networks that provide access to server resources for users.

SAN Vulnerabilities

When considering how SAN's are vulnerable, it is useful to be reminded that it is the confidentiality, integrity and availability of the data they hold, that is at stake. SAN's are usually designed with availability as a priority, with multiple paths of redundancy and highly resilient components. Issues of confidentiality and integrity have often been left with a lower priority.

Like any other network the SAN has vulnerabilities at various points of operation. Vulnerabilities can be found in each of the components that comprise a SAN and as the data moves between those components. There are vulnerabilities whilst data is static or at rest, such as on a storage device such as a disk array and there are vulnerabilities as data is moved or is in flight around the storage network.

There are a number of places where data moves between components that should be of concern. Firstly the connection between servers and fibre channel switches. Secondly, the connection between the fibre channel switches and the disk arrays. Thirdly, the connections between the fibre channel switches themselves. Fourthly, the connections between any management devices and other SAN components. Lastly, any IP based connections that are attached to any device also connected to the SAN. These types of threats and communication paths have been identified many times as the points of weakness in SAN implementations. John Vacca in a series of articles on SAN security [19] saw four main areas of concern and these are mirrored by Darryl Brooks in an article entitled 'Best Practises' for Storagemagazine, the highlighted four areas are

> …device:switch…communications are conversations flowing from management applications such as Veritas' SANPoint Control to the management server
>
> …switch:switch…conversations happen over E_Ports and include application data and switch management frames
>
> …device:device…interaction occurring between initiators and targets and WWN spoofing is the most likely mechanism to be used by a vandal to gain access to you targets.
>
> …user:device…interaction is limited to those interconnect devices that can be compromised by gaining physical access. [14]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The scope of the realm of threats to SAN's is also echoed in a paper by Arthur B. Edmonds Jr of Hitachi Data Systems who finds five areas as expressed by the threat model used as a template for the Fibre Channel Security Protocols

> Server or Storage Array to Network Connection. An attachment could result in an inside or outside party access to data they shouldn't receive.
> Switch to Switch. Here, a switch may attempt to illegally join a fabric or change a fabric topology.
> Server to Storage Array. An unauthorized communication link may be set up by allowing a device to send frames to another device that isn't in its database.
> Management Interface. An outsider who has compromised a server may install a vendor or third-party management interface on a server accessible to an insider
> DoS, Man-in-middle, Spoofing, Hijacking. [11]

Whilst these authors express the range of threats slightly differently it is clear that there are a number of vulnerabilities and areas that an attacker can exploit, relating to how devices interact in a SAN.

The Servers that connect to a SAN are the devices that will often be the most problematic in terms of security. This is because the Servers connect both to the SAN and to the Local Area Network (LAN). This means that there are a number of entry points to these devices which can be exploited and therefore more opportunities are presented to the attacker. The Servers are attached to their storage using their HBA's via the SAN and to the LAN using their Network Interface Cards (NIC's). An intruder can use vulnerabilities in the Server, such as the Server Operating System (OS) to gain access to data on the SAN. Different manufacturers OS's have differing levels of sophistication in support for SAN's and present different vulnerabilities in general operation that can be exploited. These vulnerabilities may affect only the data accessible by that individual server or may compromise the SAN as a whole. If an attacker appreciates that a compromised server has a HBA and is therefore likely to be attached to a SAN, they can safely assume they are close to important company data.

Many SAN vendors provide features such as snapshot copies of data and data cloning. Data cloning in particular should be seen as a security risk, as a clone of sensitive data could be mounted on a server with inappropriate security controls in place, allowing unauthorised access to data.

Servers that are attached to a SAN are hopefully going to be on a LAN protected from the Internet by Firewalls and hopefully protected with an IDS. The placement of servers on an internetwork becomes more of an issue when servers that are connected to the SAN are also connected to networks that are not solely internal, such as a DMZ. If the Web server is attached to the SAN and is also accessible from the Internet, if it is compromised there is potential that the whole SAN can now be compromised from the Internet,

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

rather than just from the internal network. This problem of hackers using a SAN attached host as a vector to attack another host has been discussed by W. Curtis Preston in an article for Storage Magazine entitled 'Protect you SAN from attack'.

> Prior to the advent of FC [Fibre Channel], ….to compromise the data on a disk or tape drive, a hacker first had to compromise the host…..a hacker couldn't hack into one host and reach another host's data each host had to be hacked separately…depending on the configuration, its possible to access one hosts data from another host if both hosts store their data on the same SAN. [12]

The SAN interconnects; the optical cabling and the switches may also be vulnerable to attack. By design SAN's exist to provide access to shared disk sub-systems by a number of servers. The important factors have been performance and compatibility rather then security. Due to the nature of operation of some network operating systems a method of segmentation in SAN's had to be devised. This is because some operating systems will seek to monopolise resources in a shared environment [5]. Windows NT for example will seek to assign a signature to and own any LUN it can connect to and therefore LUN's that are to be used by other operating systems such as Netware and Unix will have to be separated from NT and made invisible to it even if they are on the same disk array [3]. This method of segmentation followed the path of segmentation seen in the LAN arena, namely a form of Virtual LAN (VLAN). In Fibre Channel based SAN's this segmentation can take the form of LUN Masking and or Zoning. These are covered in more detail later. A by-product of this segmentation is a form of primitive security in SAN's.

The Management devices that configure and administer many SAN environments also provide vulnerabilities that can be exploited by an attacker. Typically these management devices use HTTP and SMTP and are vulnerable to the same exploits via these protocols as are other IP capable devices. Management device also often have some form of remote access available to the SAN. This can be for fault reporting or remote assistance by a vendor or for remote administration. Access to management devices by untrained or inexperienced staff can also affect SAN security as configuration mistakes may cause significant security breaches or lead to serviceability issues.

The Storage Arrays that hold data in SAN environments are designed to provide highly available access to data and do not typically encrypt data. This presents opportunities for attackers, because if they are able to get access to shared storage the data will usually be in clear text.

Data travelling across a SAN is also not usually encrypted so hijacked sessions can reveal data. Also there is usually no form of authentication between communicating devices so they will freely exchange information with a device if it posses the correct address (WWN).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Methods of SAN Segmentation

Often cited as SAN security processes, mechanisms to segment SAN's such as Zoning and LUN Masking can provide some level of security although they were not designed as security mechanisms. They are only security mechanisms in the sense that VLAN's in IP networks can be considered security mechanisms. Segmentation is a valuable tool but it is only part of a structured approach to SAN security and it has some inherent weaknesses.

LUN Masking or storage based zoning is a mechanism that allows nodes on a SAN to only see the LUNS that they are authorised to access. It works by mapping the LUN's to WWN and only granting access by certain WWN to certain LUN's and not others. As stated previously this is usually done to prevent some operating systems from attempting to grab all available LUN's on shared storage. LUN Masking can be accomplished in a number of ways. The required mapping can be undertaken by the HBA driver on a server, it can be done on a disk array controller or by a separate management device. The problem with relying on LUN Masking is that an attacker can change or spoof a WWN to defeat LUN Masking. If an attacker compromises a server operating system and LUN Masking is performed at the HBA driver they can alter the LUN's that are valid for that WWN in the mapping stored in the driver. If the LUN Masking mapping is done at the disk array controller the attacker can still access unauthorised LUN's if the server HBA's WWN is changed. This will also hold true with a separate management device that performs LUN Masking. In addition the attacker could seek to make this management device unavailable and thus prevent any node from accessing any LUN's, because all the logic for mapping is done at the management device.

Zoning or fabric zoning is the other method of segmenting resources is a SAN. Larry Hofer from McData a major manufacturer of SAN equipment has defined zoning as

> The ability for a user to specify groups of devices that are supposed to talk to each other [8]

It can be used on its own or in conjunction with LUN Masking. If zones are in operation in a SAN fabric only nodes within the same zone can communicate. Depending on the manufacturer of the fibre channel switch any nodes not in a zone may or may not be able to communicate with other nodes not in a zone.

There are two ways to perform zoning in a SAN called soft zoning and hard zoning. More precisely this means software enforcement of zoning or hardware enforcement of zoning.

Soft zoning takes the WWN of devices to place nodes in the correct zones (or segments) using the simple naming service found on each switch. By referring to the simple name service only devices within the same zone can access each other and this is based on their WWN being registered with the simple name service as being in the same zone. This is persistent even if there are changes to the SAN fabric, such as devices joining or leaving. Typically in a

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

fibre channel fabric all devices receive notification of changes via a mechanism similar to a broadcast in a LAN. As in LAN segmentation, fibre channel segmentation using zoning limits the broadcast to within a zone membership. This broadcast mechanism is explained below

> When a zone change is made, the devices in the database [simple name service] receive Registered State Change Notification (RSCN). Each device must correctly address the RSCN to change related communication paths. Any device that does not correctly address the RSCN, yet continues to transfer data to a specific device after a zoning change, that device will be blocked from communicating with its targeted device. [5]

With soft zoning WWN are the basis for participation in a zone and an attacker can spoof the WWN of a device and gain access to a zone.

There are also other courses of action for an attacker. An attacker could also respond with invalid RSCN information to stop devices in a zone communicating or an attacker could affect the stability of a fabric by continually resetting, adding or removing devices or sending out large numbers of state change notifications (SCN).

Hard zoning can be taken to mean two different things. The more common understanding is to identify a device by its port number on a switch and to only permit data exchange between certain switch ports that are configured to be in the same zone. Hard zoning can also be defined less commonly as not advertising the route table between two ports if those two ports should not communicate. The more common meaning of hard zoning is fairly effective unless the attacker has physical access to the fibre channel switches and can plug a device into a correct port for a given zone. If an attacker spoofs a WWN the use of hard zoning makes this irrelevant as access will still be denied because access is based on port number not WWN. The less common meaning of hard zoning would not prevent two ports from communicating if they did know of a route, it just wouldn't allow the ports to be informed of a route and is therefore not as reliable because if an attacker could guess a route access would be allowed. This is explained by Brocade, a major manufacturer of Fibre Channel switches

> Devices that are not part of the zone are omitted from the query response. If the initiator is not part of a zone or has no targets included in its zone, the nameserver response lists no devices. Note that this does not prohibit access to the device, because the nameserver does not control access to fabric devices. [9]

This means that as there is not a control on access to fabric devices. The attacker can gain access to the fabric with a little guess work or a protocol decoder.

A problem with zoning is that it tends to work well in SAN's with Fibre Channel switches from a single vendor but can be problematic when multiple vendors

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

are used. With multiple vendors it is all too easy to make a configuration mistake and not all implementations of zoning are the same and not all can be applied across different devices in the same way. The capacities of zoning are restricted as a security mechanism because of the capacity of fibre channel to be used as a secure protocol. In his presentation to the Storage Networking Industry Association (SNIA) on the 'SAN Holy Grail: Develpoment, Directions and Map, Richard Lary of Compaq asked the question

> Can zoning provide good security? [10]

His answer

> No, although it will have to do as a stopgap [10]

Whilst it is very important, zoning should only be considered as part of the steps required to secure a SAN.

The Problems of Fibre Channel

The Fibre Channel protocol suite and the fabric topology are the predominant technology for passing data over a SAN. The problem with Fibre Channel is that it possesses many of the security flaws found in other networking protocols such as IPv4. Fibre Channel was designed to facilitate reliable high speed connectivity between devices and security was very much an after thought. It is similar to IP in that it is a protocol that also has a number of different layers in its stack.

One of the most popularly highlighted attacks against IPv4 concerned the ability of an attacker to correctly guess a sequence number because the Initial Sequence Numbers were predictable. [4] In the Fibre Channel protocol stack there is a similar vulnerability at layer two, the framing and flow control layer. This vulnerability relates to the sequence control number (SEQ_Cnt) and sequence ID (SEQ_ID) within the frame header. How this works is explained below by Himanshu Dwivedi of @stake,

> A Fibre Channel Sequence is a series of one or more related frames transmitted unidirectionally from one port to another. All frames must be part of a sequence. Frames within the same Sequence have the same SEQ_ID field in the header. For each frame transmitted in a sequence, SEQ_CNT is incremented by 1. [6]

This means that the SEQ_ID is predictable as it is a constant number. Also the SEQ_CNT is predictable as it is incremented by a known value, one. A sequence series is responsible for keeping the connection alive between two nodes [7]. The sequence series is now a predictable value and an attacker would be able to attempt a session-hijacking attack by incrementing the SEQ_CNT and take control of the session.

Fibre Channel also has weaknesses with regard to flow control, in particular it is susceptible to disruption of its flow control mechanism. How flow control in

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Fibre Channel networks works is described by Robert Spalding in his book on Storage Area Networks, below

> In Fibre Channel networks, devices transmit frames only when each device is ready and able to accept them [6]. Before these devices can send and receive frames, they must be logged in to each other and must have established a credit level to send and receive the correct amount of frames. The establishment of credit from one storage node to the other is conducted at the Exchange_ID level of the frame header. This credit refers to the number of frames a device can receive at a time. This value is exchanged with another device during login, so each node knows how many frames the other node may receive [7]

By injecting a high or low credit value an attacker can disrupt the flow of information. A too high value will cause a node to send more data than can be processed by the receiving node and a too low value will delay the sending of data as the receiving node waits for data to process. This attack can be considered similar to mounting an attack using the sliding window functionality in TCP.

As explained earlier switches run a service called the simple name service that maps fixed WWN addresses to switch ports, using dynamic S_ID. This service is vulnerable to a similar attack as polluting ARP tables in IP and man-in-the-middle attacks. The attacker would generate frames in the SAN that would corrupt the simple name service in a similar fashion by changing the mapping of WWN to S_ID. Basically the attacker introduces a frame that causes the simple name service to update its entry for an existing S_ID with the attackers WWN. Fibre Channel switches usually operate in a cut-through switching mode whereby only the destination address of the frame is checked not the source address. This allows the attacker to receive the frames destined for another node. This can also be accomplished by sending out modified frames upon joining the fabric. When a device needs to join a fabric it sends out a broadcast to login to the fabric, as described below by Himanshu Dwivedi,

> N_Port sends a Fabric login (FLOGI) to the well known address of xFFFFFFE [6].

This is basically a broadcast frame telling the switch that the device wishes to participate in the fabric. The attacker includes, in a generated frame, the source address (S_ID) of another device already on the fabric, usually a switch. This is explained below by Robert Spalding,

> The modified frame has a source address of another trusted entity on the fabric, such as another trusted switch, and the WWN of the attacker. The fabric assumes the attacker is now the legitimate host since the switch's 24-bit address is matched to the attackers WWN. [7].

The attacker can also be confident that the simple name service had been modified for the following reason

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> The switch receives the frame at xFFFFFE and returns an accept frame (ACC). The Service information would then be exchanged. [7]

A major issue here is that if an attacker can get a switch to accept the attackers node as an E_Port, that is as another switch in the fabric rather than just a node, then the attacker will receive all routing and zoning information about the fabric because switches replicate this information via the E_Port without any form of authentication. The information gathered by the attacker would be the Fibre channel equivalent of a mixture of an IP Routing Table and DNS database. The attacker would know all the names and addresses of devices attached to the SAN fabric and how they exchange data.

Fibre Channel is also susceptible to spoofing attacks in a similar fashion to IP. The WWN is configurable on most SAN devices in a similar fashion to MAC addresses also being configurable on NIC's. On a server this can be as simple as loading the HBA drivers and changing the WWN. This is because if a HBA failed, a replacement could be given the WWN of the old card, thus ensuring that no configuration changes would have to be made. However, this functionality allows the attacker to change the WWN of a device to gain access to a part of the SAN that has been segmented using WWN as the identifier. An attacker would change their WWN to match that of a device already defined in the SAN. Fibre Channel switches would allow access to the areas of the SAN that were segmented by WWN, for example by utilizing zoning or LUN Masking.

The fundamental issue with Fibre Channel is that there is no form of authentication between devices by default. This allows attackers to join Fibre Channel networks with relatively simple spoofing and session hijacking methods. If devices in a Fibre Channel network had to authenticate with each other before any data was exchanged these attacks would be much more difficult to successfully deploy.

SAN devices and LAN connections

Many SAN devices are connected to both the SAN and to the LAN. This is usually to cater for remote management of these devices or reporting. This can expose these devices to any security issues that exist on the LAN and to potential access from the Internet. The number of devices that are connected to both the SAN and LAN can be surprising. The obvious candidates are servers, but there is also usually the SAN management appliance, often the fibre channel switches have LAN interfaces for configuration as does the storage array. These devices are typically accessed via HTTP, a clear text protocol, and with only passwords as authentication mechanisms. This is clearly an issue and Arthur B. Edmunds in his white paper 'Towards Securing Information End-to-end: Networked Storage Security Update and Best Practises' rates most other threats to a SAN as Medium but the threat of the Management Interface as high. This is because

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> Not due to the sheer number of possible ingress points. It is rated HIGH risk due to its ability to disrupt a connection to the networked environment, add illegal accounts, copy data to an illegal recipient, and destroy data altogether [11]

The potential for harm to a SAN from its management device cannot be underestimated either by an external attacker of from mistakes by an internal staff member.

The fact that devices are connected to both networks, SAN and LAN can lead to situation where network administrators have segmented their networks and placed devices on protected subnets with layers of security but storage administrators have placed all storage devices within a single security boundary thus negating much of this security layering.

IP based Storage Area Networks

Moving SAN's to IP based networking is becoming a popular idea amongst some vendors and organisations. IP is well known and many organisations have existing IP infrastructures. Some argue that IP networks have available to them many of the technologies that would assist in making SAN's more secure and see it as a solution to the problems of Fibre Channel. The use of IPSec, VPN's and Firewalls would allow more flexible deployment of SAN's especially in the Wide Area Networking arena and the use of public networks. There now exists a range of IP based protocols to use for SAN interconnects, as Deni Connor outlines in her article 'Debate flares over IP storage security' [13]

> …storage is using IP transport via iSCSI, Fibre Channel over IP and Internet Fibre Channel Protocol (iFCP)….iSCSI defines universal access to storage devices and storage-area networks (SAN) over Ethernet-based TCP/IP networks. Fibre Channel over IP bridges two physically separated SAN's over IP, and iFCP is used to link Fibre Channel SAN's with iSCSI networks of bridge Fibre Channel networks over the WAN or MAN. [13]

So now it appears that IP rather than Fibre Channel should be the protocol of choice for SAN's. However, problems with security in IP networks are already well known and the tools for attackers to use are readily available. Not all are convinced by IP in Storage networks. Wayne Lam of Falconstor, a major manufacturer of SAN management equipment has been quoted in an article by Sonia R.Lelii as stating

> Mimicking of hijacking an IP address is child's play, my 6-year-old can do it. IP is very easy to hack, unfortunately. [14]

This is echoed by Robert L. Scheier who writing for Computerworld expressed the following

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

..As more SAN traffic migrates from the relatively unknown Fibre Channel Protocol to IP, it will become vulnerable to the same well-known attacks used against the Internet and corporate networks [17]

So if IP is so easy to hack why is it even being considered in the storage network? Some of the reasons were made clear by Himanshu Dwivedi of @stake

> Fibre Channel networks lack authentication, encryption and authorization normally found in IP networks. [15]

It is the perceived ability of IP to address the above that are causing a push for its adoption. There is also the view that as the IP world has been seeking to solve many of these issues for many years and has made much progress. Therefore, why should storage networks seek to reinvent the wheel or invent other standards and technologies, when what is required is readily available.

However, there are technical issues still to be overcome in using IP for storage. There aren't many if any Firewalls that can handle throughputs of 2Gb/s or that can encrypt data and decrypt data at that rate and this is the speed of most SAN connectivity. Benjamin Kuo in an article for Storage Magazine quotes Kamy Kavianian of Brocade to reinforce this point

> Currently, there is nothing out there that can encrypt at 2Gb/s. Encryption must be well thought out, because a SAN was designed to move large blocks of data in an efficient manner and you don't want to put anything in the way [that degrades SAN performance]. [18]

The use of IPSec for storage networks also introduces other issues such as cost. To handle IPSec at the speeds required by storage networks will require dedicated circuitry on Ethernet adapters thus pushing up their cost. This could lead to problems with customers adopting this technology. This point is also made by Kuo when he quotes Doug Ingraham of Cisco

> Putting IPsec in all of the [iSCSI] endpoints is going to make all the endpoints too expensive. Once IPSec is running in ASIC's and doesn't substantially increase the products cost, it will be great. [18]

There are also other issues with the use of secure protocols in SAN implementations. Encapsulating Security Payload (ESP) with the support of the IETF is to becoming a standard mechanism for securing transmissions in SAN, either as part of ESP over Fibre Channel or as link security for iSCSI. Ganesan Chandrashekar writing in Network World points out that ESP does have some performance issues

> Key management will be an important consideration. For example, high Fibre Channel data rates quickly wrap over the ESP sequence-number window and prompt frequent re-keying. The Fibre Channel standards body will need to address this issue, possibly by increasing the sequence number window size. [20]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Hugo Fruehauf in a paper to the SNIA about Cryptography in Storage Networks also covers the issues of the need for re-keying with ESP when networks are running at 10Gps in some detail and the use of cryptography in Storage Networks in general for encapsulating storage data over IP networks [21]. So it seems further work may still required to bring the twin requirements of security and performance to IP-based SAN's.

The importance of IP to the future directions of SAN's should not be underestimated. By using IP organisations can replicate SAN held data over vast distances and this will be of immense value in the Disaster Recovery and Business Continuity arenas. The use of IP to link SAN's from different vendors to prevent 'islands' of different vendor SAN's in large organisations also needs to be understood.

It is this movement of SAN's out of the confines of the data centre and the security typically in place at these locations, into the realm of WAN's and external connections, facilitated by IP, that is changing the security boundaries for SAN's. Provision for adequate security needs to be considered for each of these boundaries as they evolve.

What are the Vendors proposing

Many of the storage vendors and industry associations have taken on board the vulnerabilities in current SAN implementations and have sought ways forward. Most of the proposals from vendors cover ideas around end-to-end security solutions for SANs, particularly for confidentiality and integrity of data and these should be welcomed. The issues of a secure fabric with authentication, data encryption on the wire and at rest and secure communication for management devices are now starting to be addressed.

Brocade have introduced a Secure Fabric OS for their Fibre Channel switches to help solve a number of issues and eliminate some potential SAN security risks. They are seeking to address many of the issues with segmentation and Fibre Channel that have been discussed. As part of the Secure Fabric OS Brocade have introduced

> Multilevel password controls to prevent unauthorized and unauthenticated SAN access….Management Access Control Lists (ACL's), encryption of passwords and Secure Shell (SSH).. [to counter].. insecure management access. Port-level ACL's …[to counter] ..World Wide Name (WWN) spoofing.
> Enhanced configuration architecture with trusted switches and secure management, as well as Public Key Infrastructure (PKI)-based authentication and security (digital certificates)..[to prevent] .. Management controls allowed from different access points [22]

With this Fabric OS on all switches within a SAN, Brocade suggests that they have provided a solution for the issues of authentication within Fibre Channel.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

With Secure Fabric OS only trusted devices can join the fabric, only trusted devices can make configuration changes to the fabric and WWN's can be locked to specific ports by hardware enforcement.

Nishan Systems have developed SAN Routing which aims to provide stability and authorization for fabric switches in multi-vendor fabric environments. The problem this aims to solve is that a company may have separate fabrics of Brocade and McData switches which understand the fabric in different ways. SAN routing aims to remove instability in SAN fabrics caused by changes to configuration in multi-vendor fabrics. The standards bodies have also been active in this area. Arthur B. Edmunds, Jr. points out that the Fibre Channel Security Proposals Technical Working Group

> Has voted unanimously to adopt CHAP (Challenge Handshake Authentication Protocol) with Diffie-Hellman enhancements as the first fabric interoperable authentication mechanism. What this means is that fabric Fibre Channel switches will use the same security mechanisms from day one. [11]

This will remove some of the interoperability issues that have plagued SAN's and provide the mechanism for multi-vendor authentication In seeking to resolve the issues of different vendors switches operating in the same fabric, especially with regard to zoning, the FC-SW-2 (Fibre Channel Switch Fabric second generation) specification has been agreed. If a vendors switch conforms to this standard it will coexist with other FC-SW-2 compliant switches in a fabric. [19]

Seeking to assist with the problems of authenticating fabric devices, Kasten Chase have introduced a device to handle the automated creation, registration, distribution, management of certificates to all fabric devices. This has been demonstrated to work in conjunction with Brocades Secure Fabric OS to provide easy management of certificates to fabric devices. [23] Falconstor, a manufacturer of SAN management appliances that sit between disk arrays and servers, providing such features as virtualisation, also now offer PKI technology to authenticate devices in a SAN, using their IPStor device.

The issues surrounding the protection of data in transit within a fabric have solutions proposed from a number of companies. Decru with their DataFort product are offering the possibility of encrypting data in transit in the fabric and at rest on the disk array. [24] This approach is also taken up by Neoscale with their CryptoStor product which also offers encryption of data in transit and at rest as well as automated key management. [25]

There are many vendors and products that are now starting to address the real needs of security in SAN's beyond the primitive segmentation that was previously considered adequate.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Conclusions and What can you do now?

There are a number of steps that can be taken now to secure the SAN.

Policy must be in place to define what is and what is not acceptable in terms of security. The importance of securing the network perimeter cannot be overstated especially with the increasing use of IP in storage. If possible all Ethernet interfaces on SAN components should be in their own protected subnet separate from the general LAN. All default passwords on SAN devices should be changed and strong passwords or two-factor authentication used, if possible, to access these devices.

There is readily available advice on some practises that can help secure a SAN. The Evaluator Group suggests viewing SAN security as a series of secure perimeters that an attacker must cross, with the outer perimeter being the network security framework, with firewalls and intrusion detection systems. The middle perimeter consists of host hardening practices on server operating systems and the inner perimeter consists of measures to secure the storage fabric itself. [26]

Himanshu Dwivedi of @stake after explaining many of the inherent weaknesses in Fibre Channel frames and Fabric segmentation also offers advice to overcome some of these problems to secure the SAN. For segmentation, hard zoning based on physical ports is recommended. Also Port Binding, the locking of physical ports to authorized WWN on switches is recommended. Further, locking port types on a switch is recommended i.e. an N_Port will only be an N_Port it will not dynamically renegotiate to become an E_Port. The disabling of any switch ports that are not in use is also good advice.[27] Dwivedi goes on to not recommend doing the following, implementing LUN masking on the client node or relying on it as your sole source of security. Also a single zone for the entire SAN is heartily rejected. Zones should try to replicate the security boundaries on the IP network, secure hosts should be in their own hard port based zones. Dwivedi concludes that the methods of authentication and encryption that vendors are now offering should be readily considered.

Hewlett Packard (HP) a major supplier of SAN equipment and solutions have a series of security recommendations for the design of SAN's in different environments, such as within an enterprise, at a service provider and for a secure environment [28]. The HP SAN Design guides cover security issues ranging from the physical security of the SAN, through good employment practises and security awareness training, to the use of zones and passwords enabled on all configuration ports. It is at the design stage of a SAN that security issues should be addressed not as an afterthought to an implementation.

SAN's are evolving and changing to allow them to meet the storage needs of organisations. They are increasingly becoming amongst the most important parts of a company's network, holding data that must be available. Segmentation is a crucial component of securing data in a SAN, but it has its

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

problems and should be considered as only part of the effort that needs to go into securing a SAN. Vendors are bringing to market a number of products that should help to provide solutions for other aspects of SAN security, such as secure fabrics and encryption on the wire. Where possible it would be recommended to utilize these new technologies in existing SAN implementations. For new or planned SAN's the design stages must spend time to consider proper security measures, especially as there are now a variety of options available.

References

[1] Poelker, Christopher and Nitkin, Alex. Storage Area Networks for Dummies. New York. Wiley Publishing Inc, 2003
[2] Preston, Curtis W. Using SANs and NAS. O'Reilly 2002
[3] Marrone, Nancy. "Why you need (more) storage security". InforStor April 2003.
URL.http://is.pennnet.com/Articles/Article_Display.cfm?Section=Archives&Subsection=Display&ARTICLE_ID=173287
[4] Dr K. A complete Hacker's Handbook. Carlton.
[5] Datalink. "SAN Data Security and Fabric Management". URL. http://www.storagesearch.com/datalink-art1.html
[6] Dwivedi, Himanshu – "Storage Security". URL http://www.snia.org/apps/group_public/download.php/%201630/WhiteHats.pdf
[7] Spalding, Robert. Storage Networks, the Complete Reference. McGraw-Hill/Osbourne. 2003
[8] Hofer, Larry, McData Corp. "Zoning for Security". URL http://www.snia.org/apps/group_public/download.php/%201633/Zoning_for_Security.pdf
[9] Brocade. "Zoning Implementation Strategies for Brocade SAN Fabrics". URL http://www.brocade.com/san/white_papers/pdf/Zoning_Imp_WP_00.pdf
[10] Lary, Richard, Compaq, "The SAN Holy Grail: Development, Directions and Map". URL
[11] Edmunds, Arthur B., Hitachi Data Systems,white paper "Towards Securing Information End-to-end:Networked Storage Security Update and Best Practises" URL http://www.hds.com/pdf/wp_129_security.pdf
[12] Preston, W. Curtis. "Protect you SAN from attack". Storage Magazine, August 2003
URL.
http://storagemagazine.techtarget.com/strgFeature/1,291266,sid35_gci917665,00.html
[13] Connor, Deni, "Debate flares over IP storage security". Network World, 01/21/02. URL http://www.nwfusion.com/news/2002/0121stor.html
[14] Lelii, Sonia R., "How Secure is IP-Based storage?". VARBusiness 31st Jan 2002.
URL http://www.sansecurity.com/articles.shtml
[15] Smith, Mark. "SAN Security by Obscurity", Windows &.Net Magazine. URL http://www.winnetmag.com/Article/ArticleID/39752/39752.html
[16] Brooks Darryl. "Best Practises – avoiding failure in the SAN". Storage Magazine. URL

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

http://storagemagazine.techtarget.com/strgColumn/1,291266,sid35_gci843285,00.html
[17] Scheier, Robert L. Computerworld
[18] Kuo, Benjamin. “The Road to practical SAN security”. Storage Magazine Sept 2002. URL http://storagemagazine.techtarget.com/strgFeature/1,291266,sid35_gci850726_login,00.html
[19] Vacca, John. “Basics of SAN Security parts 1&2”. Enterprise Storage Forum. URL http://www.enterprisestorageforum.com/sans/features/article.php/1431341
[20] Chandrashekar, Ganesan, “ESP over Fibre Channel secures SANs”, Network World Fusion, 12/02/02. URL http://www.nwfusion.com/news/tech/2002/1202techupdate.html
[21] Fruehauf, Hugo, “Cryptography in Storage Networks”, SNIA paper September 6, 2002. URL http://www.snia.org/apps/group_public/download.php/%201631/Cryptography_in_Storage_Networks.pdf
[22] Brocade, “Advanced Security in Storage Area Networks”, URL http://www.brocade.com/san/Feature_Stories/advancing_security.jsp
[23] Brocade, Kasten Chase, “Certificate-Based Authentication for Storage Area Networks”. SNIA paper September 2002. URL www.snia.org/apps/group_public/download.php/1625/ Certificate-Based_Authenication_for_SAN.pdf
[24] Salo, Andy, Decru, “Securing Storage Networks”, SNIA paper September 2002. URL http://www.snia.org/apps/group_public/download.php/%201629/Securing_Storage_Networks.pdf
[25] Neoscale Systems, “Data Storage Protection Risks and Returns”, October 2002. URL http://www.neoscale.com/English/Solutions/Whitepapers.html#dataprotection
[26] Dennis Martin, Evaluator Group, “SAN’s heighten storage security requirements”. URL http://www.evaluatorgroup.com/cgi-bin/start.cgi/HTMLOS_Pages/Request_Articles.html
[27] Himanshu Dwivedi, “Storage Security”, BlackHat 2003
[28] Hewlett Packard, “SAN Design Reference Guide”, Chapter 9 SAN Security URL. ftp://ftp.compaq.com/pub/products/storageworks/techdoc/san/AA-RU5YD-TE.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**