Security for the SAN Workgroup

by Jeffrey D. Coffed

ATTO Technology, Inc.
155 CrossPoint Parkway
Amherst, NY 14068
716-691-1999
www.attotech.com

SECTION 1 *Overview*

In today's competitive environment, the amount of information that is captured, stored and retrieved is growing at a staggering clip, making the job of managing it increasingly difficult. Adding to the dilemma is the fact that resources are not growing at the same rate. Fibre Channel technology and Storage Area Network (SAN) architectures have emerged to balance this data explosion with available resources, allowing businesses to keep pace.

As SANs improve information sharing and workflow, it is becoming increasingly apparent that making the data secure is a critical requirement in their design and implementation. This is true for workgroup as well as for entire Enterprise installations. This paper will focus on security challenges faced by workgroup SANs, the various hardware and software methods of securing information and ultimately illustrate the method that permits the greatest flexibility and manageability SAN administrators and workgroup users find essential. But before tackling those issues, the benefits of a SAN, how a workgroup can profit from a SAN and why security is important to the adoption and acceptance of this emerging architecture will be discussed.

SECTION 2 *Storage Area Networks – The Need is Clear*

Recent research indicates what most in the Information Technology (IT) industry have recognized for some time, that the need for additional storage is growing at amazing rates. IDC reports that the requirement for stored data is growing 80% annually. However, the number of IT managers responsible for administrating storage and systems is growing at only 5% per year. So how are IT managers going to manage this explosion of data without a tremendous increase in resources?

More and more IT managers are turning to Storage Area Networks to help them solve the paradigm of managing rapidly expanding amounts of data with only a few new resources. A SAN is an independent network for storage subsystems, free from the rest of the computer network. As will be further discussed, a SAN can make it possible for any workstation to gain access to any storage device regardless of the physical location of the storage or the user. This in effect makes managing stored data much easier by freeing the storage from the binds of the server.

The need is clear, but are SANs being implemented? The answer is yes. Fibre Channel products, the infrastructure of SANs, have experienced tremendous growth. In 1999 revenues soared 227% to $236.4 million. In fact, Dataquest predicts that 80% of external direct-attached storage revenue will transition to a SAN infrastructure by the end of 2002.

SECTION 3 *What is a SAN?*

As previously stated, a SAN is an independent network for storage subsystems. In effect, a SAN removes the storage from the servers, in essence, liberating the storage devices from the ownership of the servers. Previously, each storage server on a network had dedicated storage and sharing of data between workstations was accomplished via the Local Area Network (LAN). Sharing data over the LAN can be time consuming and will impact total bandwidth. In a SAN installation, where no server has ownership of storage subsystems, any workstation can gain access to any storage device. In other words, any user can gain access to all of the storage systems on the SAN, regardless of the location of the storage or the user.

In addition to offering any-to-any connections, a SAN creates a scaleable environment. The number of nodes on a Fibre Channel-based SAN can grow and isn't limited like today's server-based storage installations. As a workgroup or Enterprise expands, its SAN can readily accommodate that growth.

Fibre Channel-based SANs are frequently utilized to enhance data availability by increasing the speed at which data is shared. Creating an environment where any workstation has access to any storage device leads to data being more readily available. Furthermore, SANs capitalize on the speed of Fibre Channel technology while allowing for dedicated bandwidth between the storage and the workstation.

The creation of an independent SAN further increases the flow of information among storage devices and other systems on the network. Additionally, moving storage-related functions and storage-to-storage data traffic to the SAN relieves the front end of the network, the LAN, of time consuming burdens such as restore and backup.

Scalability and availability are the main SAN attractions that drive and shape the transformation of data into a more readily available asset and make the ever-growing amount of data easier to manage. Liberating storage devices from servers opens the door for increasing storage capacity as the need arises. Availability of information is enhanced as SAN storage devices are no longer dependent on or tied to a particular controlling server. Thus, overall network performance is positively impacted.

SECTION 4 *The Workgroup SAN*

In today's creative environments the sharing of ideas, concepts and work is more vital than ever. Certain workgroup applications have special storage needs – they require high-performance and large capacity storage to provide efficient delivery of large files. As outlined above, a SAN can assist in meeting these success criteria while improving the ease of sharing ideas, concepts and work.

Today, for the typical workgroup, such as those found in Content Creation environments, users who collaborate on projects must switch workspaces or physically move media. Various states of a production process are accomplished separated by time or space, thus stifling teamwork and creativity with each individual working on their own island of information.

Many professionals in workgroup environments face the challenge of using their digital resources more effectively. In the future, success may be defined by how well existing equipment is leveraged into evolving environments to improve workflow, raise productivity and heighten creativity. Workgroup SAN solutions allow a team to work on separate parts of a project concurrently – changes can be made at any stage of the production process.

The benefits of a SAN are many and growing in workgroup environments. A SAN allows for the consolidation of storage, reduces storage management overhead and increases the efficiency of workflow.

SECTION 5 *Is Security Needed?*

With SANs being able to offer any user to "gain" access to any storage device it is obvious that security is needed. Not only from the individual who is looking to illegally access data but also so that a valid user does not write to a file that another is using. With the promise of users gaining access to all information comes the threat of unauthorized users corrupting, stealing or viewing data they shouldn't.

The possible cases of intentional and accidental abuse are obvious, but nonetheless need to be stated. There is the blatantly unauthorized – someone trying to see or steal data they shouldn't, and the inadvertent mishap – the chance corruption of data by overwriting a file. Data is an important business asset and should be protected as such. Data must be secured from both inside and outside threats; competition accessing product roadmaps can be as abhorrent and corrosive as an employee viewing payroll.

A file being overwritten may be innocent but it is nonetheless disruptive. For instance, an employee opens a file and starts to make changes to it while another worker opens the same file to edit it. Satisfied her work is done, the first employee saves the document and exits. Finally, the second employee saves and closes the file causing the initial requestor's changes to be overwritten. In this scenario a chaotic environment has been born.

Whatever the reason, corrupted and mismanaged data costs time, customers and money. So while a SAN may promise access to all information, it may be a promise that an administrator doesn't want to keep. As outlined earlier, the advantages of a SAN are truly revolutionary; while security is an important consideration, methods of ensuring data integrity do exist.

SECTION 6 *SAN Security*

The need for security is apparent; how it is implemented is not as clear cut. There are ways of limiting the any-to-any user access to data. One way that data can be protected from unauthorized host access is using hardware to secure Logical Unit Numbers (LUNs). A LUN is a 2nd level of device identification / addressing. Another way to maintain data integrity is to manage access to the data via software.

While hardware-based LUN security offers advantages there are drawbacks that must be acknowledged before moving forward. Primarily, there is no security in the sense of user authorization and authentication. Currently there are three points at which hardware LUN security can be handled: at the host bus adapter, through a Fibre Channel switch or within a storage controller. While hardware LUN masking techniques work well in controlled environments, they can be bypassed. A more flexible security approach is to limit access to the actual data.

Host Adapter-based Security

Security measures can be implemented through drivers for certain Fibre Channel Host Bus Adapters. These drivers initialize all LUNs they discover on the network. Additionally, LUNs are reported for each of the Fibre Channel nodes, identified by a unique World Wide Name (WWN) on the loop or fabric. The drivers provide a masking utility that allows an administrator to determine authorization. An administrator must visit each workstation to set masks. While this may be feasible for smaller SANs, consider the challenge of ensuring LUNs are partitioned correctly for large or growing installations. Additionally, hackers may be able to override masks.

Switch Zoning

Switch zoning can be utilized to provide security by masking to the node port level for all nodes that are known to the switch. All LUNs attached to a port node can be masked from hosts that do not access that port via switch

zoning. It is important to note that switch zoning cannot mask individual LUNs that sit behind a port. Switches require that any node that attaches itself must register its WWN. Therefore a switch can be zoned either by hardware port or by WWN. The drawback to WWN zoning is that if someone knows the WWN it opens the door to unauthorized access to data. So while hardware port zoning is less flexible, WWN zoning is not as secure.

Storage Controller Mapping

Certain storage subsystems can accomplish LUN masking within their storage controllers. This is generally accomplished by mapping all host adapters against the LUNs contained in the storage subsystem. Access is independent of any intervening SAN infrastructure and allows multiple host adapters to access different LUNs through the same port. While using the storage controller for LUN masking allows more hosts to be attached, storage controllers with this functionality are not readily available at this time and this method of security can be hacked.

Software Measures

SAN security can be accomplished by utilizing software applications that manage data access and therefore, integrity. While there are many software tools available today to manage different aspects of a SAN, the only one that is truly necessary in a multiple workstation configuration is an application that manages user access to data. By using software to administer data privileges the authorization is based upon the user and not their physical location.

With networked attached storage, each server is connected to its own bank of storage. This storage can be shared with other workstations or servers over a LAN or WAN. It is each server's responsibility to manage access to its storage. With a SAN, any connected server or workstation has direct access to all of the available storage. There is no dedicated server available to manage the data. As outlined earlier, this generates a few basic concerns.

Software can be implemented to control access to either the file or folder level or to the volume. File or folder level programs are more expansive to implement and manage than volume level security. Since most workgroups are relatively small and cost conscience entities, they tend to favor the flexibility of volume level security and can easily cost justify its advantages.

Software that controls access to data volumes is an effective tool that manages potential data corrupting issues. Each user can be assigned different access privileges for every storage volume detected. Only one user will have write access to a particular volume at any one point in time. All others can have read access or no access at all. This assures integrity of volume content and avoids costly fix-it time. Read and write privileges to specified volumes are set-up by an administrator allowing workgroups to easily collaborate on projects.

Software control certainly allows for a level of flexibility that is unavailable to hardware-based LUN security. Host software provides a centrally managed way to handle security beyond the LUN level. By controlling an individual's access and the type of access they have to data is not only beneficial to an administrator concerned with righteous access, but to entire workgroups trying to collaborate on projects.

Implementing a structured environment where access to data is controlled not by physical location, but by who is accessing the data leads to better security. In turn, tighter security leads to a saving in time, productivity and money by reducing corrupted and mismanaged data. While hardware SAN security measures have their place, volume level software security allows for the flexibility and ease-of-management that most working in SAN workgroup environments will find favorable.

SECTION 7 *Summary*

As Storage Area Networks are being implemented to help manage the explosion of data that most workgroups are currently experiencing, the need for security has become a concern. It is clear that there are benefits to centrally managed storage resources and a significant value to the any-to-any user access a SAN offers. However, any-to-all user access to data is not always beneficial.

No doubt, there are security challenges faced by workgroup SANs. The workgroup is often where files are shared and worked on by several users; therefore, security for the workgroup must be tight. Maintaining data integrity is of utmost importance to the adoption, acceptance and emergence of SANs.

There are several ways of limiting the any-to-any user access to data in a workgroup SAN environment. Data can be protected from unauthorized host access by securing LUNs based upon hardware or by managing access to specific data volumes with software. While each offers advantages, it is evident that software security permits the flexibility and manageability SAN administrators and workgroup users find essential.