SAN Security

9

Information security is a fundamental issue that must be dealt with while managing any data center. HP understands the importance and complexity of establishing and maintaining a secure information storage environment. HP storage products are designed to make it easy to protect the availability, integrity, and confidentiality of the customer data that they hold.

HP is working with other storage vendors in the Storage Networking Industry Association to develop enhanced SAN security technology. Refer to: http://www.snia.org/tech_activities/storage_security for additional information.

HP is also working with the Fibre Channel standards community to develop storage network security protocols. Refer to http://www.t11.org for information on the Fibre Channel Security Protocols (FC-SP) project.

This chapter describes storage aspects of information security in a StorageWorks SAN environment. Major topics covered in this chapter include:

- Basic Security Model
- Summary of SAN Security Practices
- Security Features of HP StorageWorks SAN Components
- Storage System
- Storage Security in an Enterprise Environment
- Storage Security in a Service Provider Environment
- Storage Security in a Secure Environment

Basic Security Model

The ideal mass storage system provides fast storage and retrieval of information for a number of servers.

This one line summary leaves unspoken a number of additional expectations: It is expected that data written to the storage system today will be available tomorrow. It is expected that the data will be the same when it's read as it was when it was written. And it's expected that the data is not available to any server or any person not specifically authorized to have access. These three possibilities are covered under the general headings of availability, integrity, and confidentiality.

These additional expectations form the basis for defining the availability and security of the data in the mass storage system. For example, the data should be available even if a hardware or software component in the storage system fails: RAID and remote mirroring technology are methods used to maximize data availability.

Three types of attacks, corresponding to the three aspects of information security, can be made on a computer system. Data can be made unavailable for access. Data can be deleted or modified without permission. Data can be examined without permission. Any computer security system must deal with these types of attacks.[1]

The security of a computer system is the responsibility of a Security Manager. This person defines the operational rules and procedures that are required to maintain the desired security level. To achieve the desired security level in an HP SAN system, the operational rules and procedures should incorporate the guidelines discussed in this chapter.

The basic approach to making a system secure is to define one or more security domains. A security domain is a logical grouping of related components in the storage system, along with a set of rules that specify the amount of communication that is allowed between the components. Devices such as servers and storage systems that are within a given security domain are allowed to communicate with each other. The security manager defines the communication–if any–that is allowed between domains. The security system works by controlling every possible communication path between the security domains, so that data cannot be moved between domains without authorization.

The boundaries of the security domains are barriers that control access to the components. The boundaries also control communication between domains through the network or storage bus connections. Any potential path between security domains must be reviewed to make sure that only approved access is permitted. This can be an extremely complex undertaking.

[1] An excellent introduction to computer security may be found in "Computer Security Basics", by Deborah Russell and G.T. Gangemi Sr, published by O'Reilly. A more detailed discussion of network security methods and protocols my be found in "Network Security Essentials," by William Stallings, published by Prentice-Hall.

Summary of SAN Security Practices

HP StorageWorks SAN hardware and software components incorporate features that can be used to implement a secure data storage system. The following table shows the appropriate use of these security features in various environments. The Enterprise Storage System environment is a typical mid-sized to large IT installation used in a business. The Service Provider Storage System environment is a large installation where several customers share a single IT infrastructure. These environments are discussed in more detail in later sections of this chapter.

Table 50: How to Use SAN Security Features

SAN Storage Security Feature	Enterprise Storage System	Service Provider Storage System
Physical security of SAN environment.	Suggested. All personnel are employees, but it is always better to keep sensitive systems away from informal access.	Essential. Personnel are competitors, so the systems must be kept in a secure environment.
Use of zones.	Optional. Use port or WWN zoning as required to manage Operating System conflicts.	Optional. Use port zoning as required to manage Operating System conflicts.
Use of Selective Storage Presentation (SSP.)	Essential. Use as required to manage access to data.	Essential. Use as required to manage access to data.
Controlled access to storage system management using serial line interface.	Suggested. Limit physical access to machine room.	Optional. Storage systems are physically secure in this environment.
Controlled access to storage system management using in-band interface.	Optional.	Optional.
Restricted use of multiple switches.	Optional. No additional risk is added.	Optional. No additional risk is added.
Restricted use of multiple storage systems.	Optional.	Essential. Each customer must be located on a different storage controller pair.
Restricted use of Storage Management Appliance.	Optional. Appliance applications are password protected.	Recommended. Appliance applications are password protected, but a shared infrastructure is sensitive to competing interests.
Use of logical unit visibility control on Modular Data Router tape controller.	Essential. Use as required to manage access to data.	Essential. Use as required to manage access to data.
Event logging enabled.	Essential. Needed to track possible intrusion attempts.	Essential. Needed to track possible intrusion attempts.

Data Path and Management Path Security

HP divides the responsibility for SAN security into two parts. Data Path Security refers to the protection of the communication path used to move user data through the SAN. Management Path Security refers to the protection of the communication path used to move management information through the SAN.

This is a functional distinction, because in some cases the same physical connection is used for both user data and for management information. For example, the Storage Management Appliance communicates with an HSV storage controller using the Fibre Channel connection that is also used to send user I/O traffic.

Table 51 shows the Data Path Security and the Management Path Security features available in HP SAN products.

Table 51: HP SAN Products Data Path and Management Path Security Features

Data Path Security	Management Path Security
Selective Storage Presentation	Passwords on user interfaces
Zoning by port and WWN	Security of sign-on to Element Manager
Port binding	Secure communication between storage management appliance and storage array
Fabric binding	Control of IP access to device management ports
Switch binding	
Communication packet encryption (future)	
Data encryption on storage media (future)	

The HP storage security model is implemented as three distinct areas. The overall security of the storage system is an integral part of the total solution security, and is deployed within the context of a comprehensive understanding of the system, developed and delivered by HP Professional Services. The software components of the storage system provide Management Path Security by controlling operator access rights and by securing the SAN management communication paths. The hardware components of the SAN provide Data Path Security by controlling storage array access and by governing the SAN fabric configuration control mechanisms.

Personnel and Operating Practises

The most important security feature in any environment is the attitude and operating practises of the personnel. The system managers and operators must have a positive view of security, and must be able to balance the need for data security with the need for reasonable user access.

Responsibility for maintaining SAN security should be assigned to a Security Manager, and this person should have the authority to enforce reasonable security guidelines. The Security Manager is responsible for making the trade-off between required user access capability and access restrictions required to maintain the required level of security.

HP professional services can assist in developing a suitable operating protocol for your SAN environment. The HP Security Services Portfolio includes a comprehensive end-to-end lifecycle range of services for designing, building, integrating, managing, and evolving sound solutions. The Security Healthcheck Services provide quick, comprehensive security vulnerability and risk assessments of your installation, including the storage systems and related storage network infrastructure. Refer to http://www.hp.com/hps/security for additional information on HP Security Services.

Professional Services for SAN Security

The establishment of a comprehensive security environment for a large computer system is a complex task. In addition, a failure or breach of the security system may result in the loss of important business information. For these reasons, HP requires that licensed security options must be installed as part of a professional services contract.

The HP SAN Security Services product includes a security review and planning feature and an ongoing security auditing process. The initial security review and planning steps are done before the security products are installed, and result in a report summarizing the security environment and requirements of the proposed installation. The security products are installed when required. The ongoing audit process includes a periodic review of the environment, management and operational practises, and any security logs or other data that is recorded by the system.

Risk of security problems is minimized by using the HP professional services for SAN security.

Security Features of HP StorageWorks SAN Components

The components of an HP StorageWorks SAN are shown in the figure below.

Hardware components include the Host Bus Adapter (HBA) residing in each Application Server, the Fibre Channel Switches that make up the SAN fabric (or fabrics in a multiple fabric SAN), the Disk Storage Systems (including their RAID controllers, cache memory, disks, and related management components), the Tape Storage Systems (including their Network Storage Router gateways), the SAN Management Server, the Storage Management Appliance, and various communication cables.

Software components include the server operating systems, the StorageWorks Command Console software, the SAN Management Software, Web Browser and Terminal Emulator interfaces to the Fibre Channel Switch and Storage System management tools, and the MDR management interface.

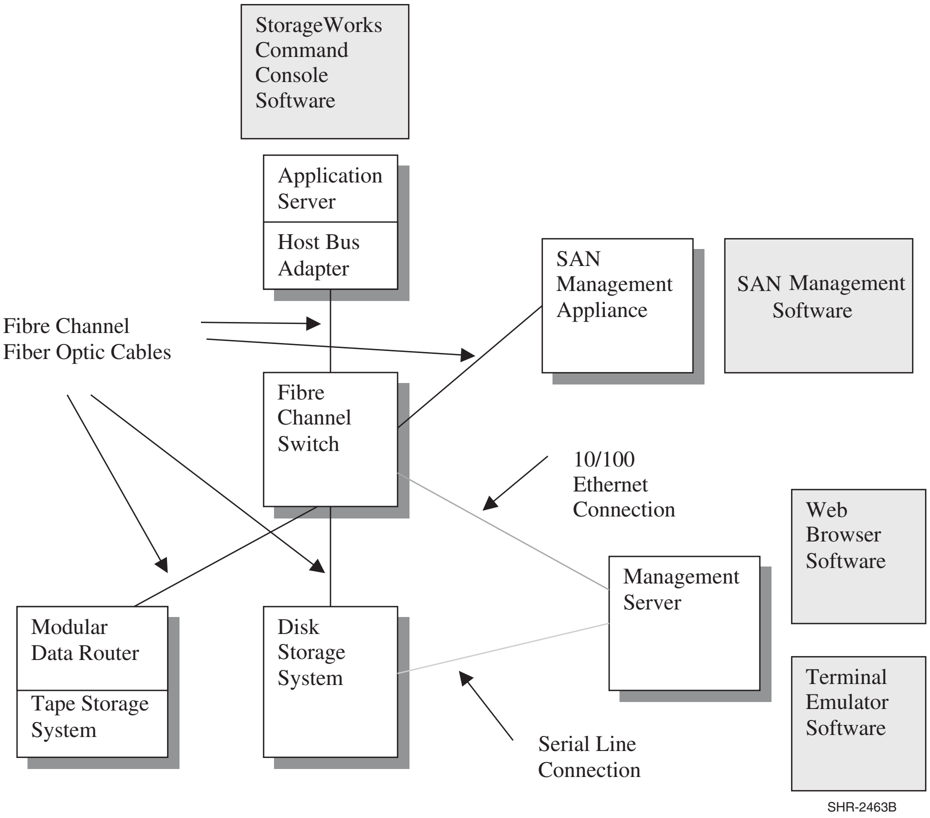

Figure 55: SAN Components

The current and future security features of each SAN component are listed below. SAN security is a rapidly developing technology, and the information in this chapter reflects the status of the technology as of the date of publication.

Fibre Channel Fiber Optic Cables

Fiber optic cables used for Fibre Channel communication do not emit electromagnetic radiation. This reduces the risk of security intrusion by means of remote sensing. However, it is not particularly difficult to make a physical tap into an active fiber optic cable. To maximize communication security, the cables should be kept within a secure area.

If a Fibre Channel cable is disconnected, the loss of signal is detected by the connecting devices and is logged in the devices' event logs. Verify that event logging is enabled on all connecting devices that have this feature.

10/100 Ethernet

Because of the difficulty of securing a distributed system, many IP LAN installations suffer from a low overall level of security. The storage security manager should verify that good passwords are in use on all the SAN components that are connected to a LAN, including the application servers, the Storage Management Appliance, the management server, and the Fibre Channel switches.

Serial Line

Serial line interfaces are used to connect a terminal (with its associated keyboard and display) to a server or other SAN component. Serial line connections are made using RS-232 physical interface. The EIA-423 protocol is used, and the connection runs at a low speed (typically 9600 baud). The serial line protocol itself does not have any provision for access security.

The security manager should verify that good passwords are in use on all the SAN components that have serial line connections, or that these connection points are in a secure area.

Host Bus Adapter

The host bus adapter (HBA) is the basic interface between the SAN and each server. The microcode in an HBA can be changed by using a utility program. In the case of Windows NT, a microcode load can be done on an active system, and the server does not need to be re-booted to resume normal I/O activity. A new host bus adapter may be installed in an operational server.

In Fibre Channel, there is no equivalent functionality to the "promiscuous" mode of operation that historically could be used on 10 Mbps CSMA/CD Ethernet networks. The security risk associated with HBAs in a Fibre Channel environment is low because the switches filter all traffic. Only traffic intended for a given server is communicated between the switch and that server's HBAs.

If the operating system driver is changed, then the system must be rebooted. This minimizes the likelihood of undetected changes to driver software.

Fibre Channel Switch

Fibre Channel switches are connected together to form a SAN fabric. The switches are the foundation of the SAN system. HP offers three families of switch products, the B-Series Fabric Line, the M-Series Line, and the C-Series Line, each with a unique set of features and capabilities. The security features differ between the three families, as described in the sections below. Refer to the product documentation for additional information that is specific to these products.

Standard Security Features of M-Series Product Line Switches

The following security features are included with all members of the M-Series product line family of Fibre Channel switches.

Switch Zones

The switches in a fabric cooperate to enforce data access zones. Servers are identified either by the switch port to which they are connected, or by their unique World Wide Names (WWN). These two methods are called "port zoning" and "WWN zoning", respectively.

The advantage of port zoning is that it is easy to configure, while the disadvantage is that if a server is moved from one port to another, the zone configuration must be changed to reflect the new connection topology. The advantage of WWN zoning is that it is independent of port, so servers may be moved from one port to another without changing the zone settings. The disadvantage is that an HBA in a server could, at least theoretically, take on the WWN of another HBA and thus gain unauthorized access to the wrong zone.

The purpose of zones is to manage the interaction of servers in a SAN, preventing interference between the operating system drivers. In heterogeneous configurations the drivers may interfere with each other, and in homogeneous operating system environments the capacity of certain driver data tables may be exceeded. Zoning is used to manage these operational factors. The security manager should verify that event logging is enabled to record unintended and unauthorized changes to the SAN configuration.

Passwords

All user interfaces to switches in the M-Series Line are protected by passwords. HP strongly recommends customers change the passwords on all switches.

Management System Communication

The Ethernet connection between the switch and the management station is protected by a secure protocol.

Optional Security Features of M-Series Product Line Switches

The following security features may be activated on all members of the M-Series product line family of Fibre Channel switches by the use of a license key. This key is supplied in the HP SANtegrity Binding product. Refer to the HP SANtegrity Binding product description for additional information on these features.

Fabric binding

When Fabric Binding is activated, only switches and directors that are identified in the Fabric Membership List are authorized to join the fabric.

Switch binding

When Switch Binding is enabled, only devices that are identified in the Switch Membership List are allowed to connect to the fabric.

Enterprise fabric mode

When Enterprise Fabric Mode is active, the security system automatically activates the following capabilities on all switches in the fabric and does not allow any to be deactivated:

- Fabric Binding (includes Insistent Domain ID)
- Switch Binding
- Domain RSCN's
- Rerouting Delay

Standard Security Features of B-Series Line Switches

The following security features are included with all members of the B-Series Line family of Fibre Channel switches.

Switch Zones

The switches in a fabric cooperate to enforce data access zones. Servers are identified either by the switch port to which they are connected, or by their WWN. These two methods are called "port zoning" and "WWN zoning", respectively.

The advantage of port zoning is that it is easy to configure, while the disadvantage is that if a server is moved from one port to another, the zone configuration must be changed to reflect the new connection topology. The advantage of WWN zoning is that it is independent of port, so servers may be moved from one port to another without changing the zone settings. The disadvantage is that an HBA in a server could, at least theoretically, take on the WWN of another HBA and thus gain unauthorized access to the wrong zone.

The purpose of zones is to manage the interaction of servers in a SAN, preventing interference between the operating system drivers. In heterogeneous configurations the drivers may interfere with each other, and in homogeneous operating system environments the capacity of certain driver data tables may be exceeded. Zoning is used to manage these operational factors. The security manager should verify that event logging is enabled to record unintended and unauthorized changes to the SAN configuration.

If more than 64 zones are defined in a single SAN, there may be cases where the port zoning table overflows. In this case the switches revert to WWN zoning. Refer to the user guide for the switch you're using for additional information on this topic.

Passwords

All user interfaces to switches in the B-Series product line are protected by passwords. The default passwords are available to the public, so it is extremely important to change them when the switches are installed.

Optional Security Features of B-Series Product Line Switches

Enhanced Brocade Fabric Manager 4.0

Brocade Fabric Manager provides a comprehensive SAN configuration control utility. Fabric Manager enables customers to configure and manage multiple B-Series product line switches from a single console. Features available with Fabric Manager 4.0 include SAN-at-a-Glance overviews with a topology map, call home support to send automatic notifications of system failure, enable remote support and isolate faults, and enhanced port management support, including port grouping.

Refer to www.brocade.com for additional information on Brocade Fabric Manager 4.0.

Secure Fabric OS

HP StorageWorks Secure Fabric OS protects your SAN by using the strongest, enterprise-class security methods available, including digital certificates and digital signatures, multiple levels of password protection, strong password encryption, and Public Key Infrastructure (PKI)-based authentication, and 128-bit encryption of the switch's private key used for digital signatures.

Features include Fabric Configuration Servers ("trusted" switches), Management Access Controls, Device Connection Controls (Access Control Lists), Switch Connection Controls, and Secure Management Communications. The trusted switches provide a central location for controlling SAN security. Device ACLs and Switch Connection Controls prevent unauthorized devices and switches from connecting to the secure fabric. All inter-switch management communication as well as communication to the management console is secured using encrypted passwords.

For additional information on configuring your HP StorageWorks SAN using the HP StorageWorks Secure Fabric OS, refer to

http://www.hp.com/country/us/eng/prodserv/storage.html

To access the technical documentation at this site:

- Locate the **Networked Storage** section of the web page.
- Under Networked Storage, go to the **by type** subsection.
- Click **SAN Infrastructure**. The SAN Infrastructure page displays.
- Locate the **fibre channel switches** section.
- Go to the **infrastructure** subsection.

Storage System

Products in the HP HSG80-based and Enterprise Virtual Array series of storage systems incorporate security controls on all the interfaces to the storage system.

Each storage system consists of a pair of HSG80 or HSV storage controllers, along with assorted supporting hardware.[2] The storage system is connected to one or more servers, and presents logical disks to those servers. Each logical disk has a logical unit number (LUN).

The Selective Storage Presentation (SSP) feature allows visibility of logical units to be restricted to a subset of the servers connected to the storage system.

Physical Access Control

The storage system is typically housed in a standard HP rack with locking front and rear doors. The locks for these cabinets all use the same key, so the security aspect of the locks is only sufficient to deter the most casual intrusion. The locks can be changed to provide additional physical security if desired.

Controller Management

Basic control of the storage system is performed using various buttons and lights on the front and rear panels of the RAID controller shelf. These controls allow the controllers to be halted or restarted. The HSG80 controller microcode is stored on PCMCIA cards that are inserted into these panels. Physical access controls to the controller shelf must be maintained to prevent unauthorized manipulation of these controls and to prevent unauthorized replacement of the controller microcode.

One option for initial setup of the storage system as well as for ongoing operation is to use a serial line connection to each HSG80 RAID controller. This connection is typically made between a controller and a terminal emulator program running on a nearby computer. All storage system management operations can be done using this interface. Physical access to the controller shelf must be maintained to avoid unauthorized use of this interface.

[2] Refer to the HSG80 and HSV controller documentation for a complete description of the features of the HP family of storage systems.

Another option for the initial setup and ongoing operation of the storage system is to use the in-band Fibre Channel management system. This system sends SCSI commands to logical units on the storage system to control the logical unit definitions and the SSP settings. A server may send these commands to any logical unit to which SSP allows it access.

Data Access Control

The Selective Storage Presentation feature of the storage system is the method used to control access to user data. Access is allowed to each logical unit by one or more servers.

The SSP settings may be controlled by any server having access to any logical unit on the storage system. This includes the SWCC agent, the SSSU tool, and the Storage Management Appliance, and could include a purpose-built intrusion application running on a server connected to the SAN. If a computing environment has multiple security domains then the domains must not coexist on a single storage system.

For example, consider the configuration shown in the following figure. Server A and Server B have access to logical unit D and logical unit E respectively. Server A and logical unit D are in one security domain, and Server B and logical unit E are in a separate security domain. Since both have access to Storage System C, then Server A may change the SSP settings to prevent Server B from accessing any logical units on the storage system.

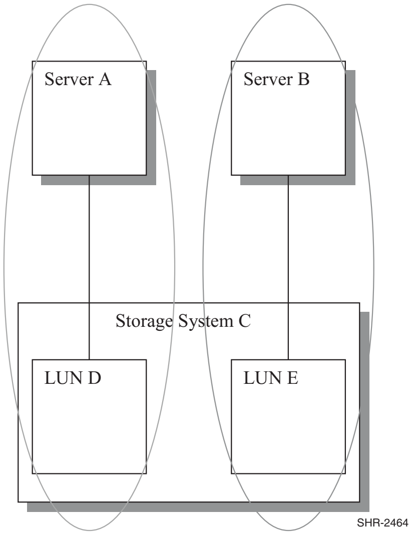

Figure 56: Multiple Security Domains on One Storage System

A future version of the HSG Array Controller Software will include a security enhancement that restricts management access to the controller. With this feature, the ability to make configuration changes to an HSG controller is restricted to those servers who are specifically authorized. This will allow multiple servers in multiple security domains to be connected to a single controller (or controller pair).

LUN security in the XP based Disk Storage Systems

Secure Manager XP provides security at LUN level, which is not available through switch zoning. LUN security can be enabled on a per port basis and allows permitted WWNs of hosts to be added to host group or groups on the selected ports.

LUN security in the VA-based Disk Storage Systems

Secure Manager VA is an optional software for the VA arrays that provides extra security at LUN level. This is accomplished by mapping LUNs against pre-configured host HBA WWNs thus creating a secure host table internally. The array will not permit access to the LUNs if the WWN of the host HBA is not present in the table. The total number of hosts or HBAs allowed per VA controller varies depending on the model. Refer to the respective user manuals for details.

EVA Management Access Control

A management agent can control many storage systems, and many management agents can control a storage system. Without password protection, any management agent on the fabric can access any storage system on the fabric. A password is used to increase the security within your storage subsystem. Specifically, password protection:

- Allows a management agent to control only certain storage systems.
- Allows only certain management agents to control a storage system.

All management functions for Enterprise Virtual Array storage subsystems are done via the Storage Management Appliance (sma). Two levels of security are implemented for the Enterprise Virtual Array to control unauthorized access to the storage subsystem.

> The first level controls access to the MA itself. User access to the MA is controlled by a username and password method that uses the WEBM security model. Without the correct username and password, an unauthorized user cannot access the MA.
>
> Secondly, the storage subsystem has an optional password protection to control which MA can manage which storage subsystems. The password is established by entering a password into the operator control panel (OCP) of one of the controllers. Use Command View for HSV Management Agent options to enter the password used by that MA to access particular Storage Subsystems.

In addition to the optional storage subsystem zoning on the fabric, this should prevent someone from putting an unauthorized MA on the fabric and attempting to manage a EVA storage subsystem.

StorageWorks Command Console Management Software

StorageWorks Command Console (SWCC) is a client-server storage management software product that supports in-band management of HP EVA and HSG80-based storage systems. An agent program runs on a server and communicates with any storage system attached to that server. The SWCC client program runs on a second, remote server to provide the GUI. The two servers communicate by using a TCP/IP connection between the two servers.

The Command Scripter tool also uses the SWCC agent to communicate with storage systems.

User access to the SWCC agent is controlled by a username and password. Any SWCC client accessing the agent to perform management tasks will be asked for this password. The communications between the management station and the host servers connected to the storage controllers is protected by single-use key encryption. In addition, remote configuration can be optionally disabled.

Communication between the agent and the controller is done by using SCSI commands on the Fibre Channel connection between the server and the controller. The agent communicates with a logical unit on the controller.

Storage System Scripting Utility

Storage System Scripting Utility (SSSU) is a character cell interface that allows a user to configure and control Storage Controllers generically on a Storage Area Network (SAN). Simple or initial configuration requests can be handled easily and expediently through this simple character cell interface, such as the initial creation of LUNs presented to the host. SSSU meets this requirement with an interface that allows the user to issue simple, terse commands.

SSSU uses the Storage Management Appliance (sma) to communicate with EVA storage systems. User access to the MA is controlled by the username and password method that uses the WEBM security model.

Storage Management Appliance

HP offers an optional integrated SAN management system that uses an appliance connected to the Fibre Channel fabric. The Storage Management Appliance hosts web-based Open SAN Storage Management software. This software provides a wide variety of management tools.

Access to the Open SAN Management applications is controlled by a username and password method that uses the WEBM security model.

Storage Security in an Enterprise Environment

In a business enterprise, computer systems may be shared between two or more departments. The systems are managed and operated by an Information Systems organization, which has enterprise-wide responsibility for the computing environment. All the people in the enterprise work towards a common business goal, but the day-to-day interests of the departments may vary widely depending on the business climate, time of year, or product development issues. Each department has specific computing requirements that must be met by the IS organization.

There may be wide differences in the need for data security. For example, a typical accounting department has strict security guidelines, while the marketing department may be willing to tolerate more risk.

The IS organization may try to achieve efficiency by placing the computer equipment in a single central location. A considerable amount of computer and storage hardware is required for an enterprise of moderate size. This discussion assumes that the storage for all the departments is located in a single SAN storage system. Servers are distributed throughout the facility.

The IS organization must implement a computing system that meets the security and capacity requirements of all the departments to which it provides service, and the IS security manager must implement a security plan that is suitable for the needs of the enterprise.

To meet the security requirements, many security managers specify a centralized machine room located in a secure area. This substantially reduces the security risk for the storage system, because the ordinary users of the system do not have physical access to the machines.

Security Expectations

This is an environment with a requirement for a high level of storage system security. Protection is needed against unauthorized accidental and malicious data access attempts. The required security level is set by the department with the most strict security needs.

SAN Component Security Attributes

The following features are used to provide security in this environment.

Traditional user account security is in effect in the servers. This protects each user account against accidental access by an unauthorized user. Disk quotas are enabled for each account. This prevents a user from consuming all of the storage capacity allocated to the server.

The HBAs pass user I/O requests to a Fibre Channel switch. Communication is done using Fibre Channel fiber optic cables. These cables pass from the servers into the secure area that holds the storage systems.

The SAN switches are shared by all the users and servers in all departments in the system, and are located in the secure area. Configuration management of the switches is done by the system manager using the web management interface. The interface is protected by password to prevent unauthorized changes to the switch configuration.

Data is stored in several StorageWorks storage systems. Access to each logical unit is controlled by the Selective Storage Presentation feature of the array controller.

Response to Attacks

Two attack scenarios are possible in this situation. Accidental inappropriate data access requests might be made by any user, and malicious attempts to make an inappropriate data access requests might be made by a user.[3]

Inappropriate read and write requests by system users are routinely handled by the operating system. Disk mounting requires a privileged account, and directories are protected by access control lists. The benign server environment puts little stress on the security capabilities of the storage system.

Since the storage systems are located in a secure area, the risk of inappropriate access to the array controllers is limited. There is some risk that the fiber optic cables might be tapped, but this requires a technical approach that is unlikely in this scenario.

Denial of service attacks initiated by system users, whether accidental or purposeful, are not fully protected against. A user could write a program that issues a useless but very high I/O load and consume most of the I/O operation capability of the storage system.

Checklist

For a SAN storage system that requires a moderate level of security, and where the storage systems and Fibre Channel switches are located in a secure area, the following steps are required.

- Good employment practices to minimize malicious attacks.
- Computer system security awareness training for all personnel.
- Routine user account management at the server.
- Disk quotas enabled for all users.
- Locate storage systems and Fibre Channel switches in a secure area.
- Passwords enabled on all switch configuration ports.
- Selective Storage Presentation for all logical units.
- Disable SES management interface to Fibre Channel switches.
- Routine periodic security audits.

The HP StorageWorks Secure Fabric OS is recommended for SANs based on B-Series product line switches.

[3] We've ruled out serious attempts to break into the storage system, but unsophisticated attempts to read someone else's data are possible in any computer system environment.

Storage Security in a Service Provider Environment

Some organizations provide computing services to their customers on a lease or contract basis. The services may include general-purpose office applications such as Microsoft Exchange or file and print services, or they may be specialized. One example of the latter is the Storage Service Provider, which provides storage capacity to some other organization. In all service provider situations, the service provider is the HP customer, and the service provider has second level customers of its own who purchase the service.

These second level customers are the users of the systems.

These users may be competitors of each other, and it is essential that they be protected against security breaches—accidental or intentional—by other users in the computer system. The security plan must take into account the possibility of aggressive attacks.[4] This is probably the most difficult environment for a storage system security manager.

Physical access to the storage system is controlled by placing it in a secure area. The servers are in separate secure areas, segregated by user so that each user has a unique secure server area.

Security Expectations

The requirement is for high security. Each user wants a separate security domain because there is no trust between competitors. Protection against accidental or intentional unauthorized access to data must be provided, and protection against unauthorized changes to the configuration of the storage system is also required. Sophisticated attacks are not expected, but intentional attacks may occur.

At the same time, services providers are very sensitive to cost. There is a desire to share equipment between users to minimize hardware and management cost. This must be balanced against the security requirements.

SAN Component Security Attributes

The following features are used to provide security in this environment.

Traditional account security is in effect in the servers. This protects each user from accidental unauthorized access. Disk quotas are enabled for each account. This prevents I/O from one account from consuming all of the storage capacity allocated to the server.

If one user attempts an intentional attack on another user’s data, it may be expected that this would be done from a privileged account on a server. Account security does not protect against this sort of attack, but the exposure from a privileged account is to the data of other accounts on that system, not other users—because they are on their own servers.

The HBAs pass I/O requests to a Fibre Channel SAN switch. Communication is done using fiber optic cables. These cables pass from the servers into the secure area that holds the storage systems.

The Fibre Channel switches are shared by all of the service provider’s customers, and are located in the secure area. Configuration management of the switches is done by the service provider’s system manager using the serial line interface.

Data is stored in several StorageWorks storage systems. Access to each logical unit is controlled by the Selective Storage Presentation feature of the array controller.

[4] Denial of Service attacks are not considered to be a problem, because the comparatively small number of users on a SAN makes it easy to identify and eliminate this sort of aggressor.

A user may attempt to access a competitor's data. To protect against this possibility, it is important to provide a separate storage system for each of the service provider's customers. While the risk associated with sharing a single storage controller between customers is small,[5] distributing them onto private storage controllers eliminates the risk.

Response to Attacks

Two attack scenarios are possible in this situation. Accidental inappropriate data access requests might be made by any user, and malicious attempts to make an inappropriate data access requests might be made by a user.

Inappropriate read and write requests by system users are routinely handled by the operating system. Disk mounting requires a privileged account, and directories are protected by access control lists.

The storage systems are located in a secure area, but there is some risk of intentional attacks. This is prevented by providing a separate storage controller for each user.

There is some risk that the fiber optic cables might be tapped. While this risk is minimal, the Fibre Channel switch logs must be examined regularly and the configuration change alarms on the switches enabled. These will notify the security manager if this sort of activity occurs.

Depending on the service provider environment, it may be possible for a sophisticated attack on the SAN to take place. This could involve equipment such as frame grabbers or phantom switches. It is extremely difficult to protect against a sophisticated attack against any network system, and Fibre Channel is inherently exposed because the data is sent as clear text. If this level of risk is expected, refer to the following section.

Denial of service attacks initiated by system users, whether accidental or purposeful, are not fully protected against. A user could write a program that issues a useless but very high I/O load and consume most of the I/O operation capability of the storage system.

Checklist

For a SAN storage system that requires a high level of security, and where the storage systems and Fibre Channel switches are located in a secure area, the following steps are required.

- Good employment practices to minimize malicious attacks.
- Computer system security awareness training for all personnel.
- Routine user account management at the server.
- Disk quotas enabled for all users.
- Locate storage systems and Fibre Channel switches in a secure area.
- Passwords enabled on all switch configuration ports.
- Selective Storage Presentation for all logical units.
- Disable SES management interface to Fibre Channel switches.
- Disable SNMP management interface to Fibre Channel switches.
- Disable web browser management interface to Fibre Channel switches.
- Each user (that is, each customer of the service provider) must have a separate array controller.
- Routine periodic security audits.

[5] It requires special knowledge and equipment to successfully complete an unauthorized access to data on an array controller.

The HP StorageWorks Secure Fabric OS is strongly recommended in B-Series product line SANs used in service provider environments. The enhanced security provided by this product eliminates the risk associated with having ports from a single SAN exposed to multiple second level customers.

Storage Security in a Secure Environment

Some system environments require extremely high levels of security. These are cases of national security or where the data is so sensitive that the owner is willing to make substantial functionality trade-offs to maintain the desired security level. These systems are safe in the face of the worst cases of overt attempts to break into the system by any means possible.

Security Expectations

It is expected that the system will have no exposure to security intrusions. This corresponds to the highest levels of information security.[6] Network systems generally are not able to be audited for compliance with the highest levels of security, because network software is too complex for a comprehensive evaluation. To obtain the highest possible levels of information security, the entire system must be enclosed in a secure environment.

SAN Component Security Attributes

To provide security in this environment, the system is enclosed in a secure area.

Checklist

For a SAN storage system that requires the highest level of security, enclose the entire system in a secure area.

- Perform routine periodic security audits.
- Follow other appropriate actions based on the required system security level.
- Place machines in a secure area.

[6] Computer system security ratings are set by NIST/NSA in the US and ITSEC in Europe, and “Common Criteria” is a newly-adopted US standard. Within these classifying bodies, a product can be evaluated at various security levels. Currently, most operating systems are classified at ITSEC's E3 rating or Common Criteria's CAPP protection profile EAL4. The OpenVMS SEVMS product has a E3/B1 rating. Tru64 UNIX has an E2/C2 rating. See http://csrc.nist.gov/cc/.