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.

Securing Networked Storage using Defense in Depth

In this paper, I will discuss security vulnerabilities in networked storage solutions and methods to identify and mitigate risk associated with the vulnerabilities. I will begin with an overview of the evolution of storage from Direct Attached Storage (DAS) to two dominant networked storage solutions - file-based Networked Attached Storage (NAS) and block-based Storage Area Networks (SAN). I will discuss security exposures within each solution and the applicability of "defense in depth" techniques to address security i...

Copyright SANS Institute
Author Retains Full Rights

AD

Securing Networked Storage using Defense in Depth

Anilkumar Pochiraju
June 15, 2003

GIAC Security Essentials Certification (GSEC)
Practical Assignment: Version 1.4b – Option 1

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Abstract

In this paper, I will discuss security vulnerabilities in networked storage solutions and methods to identify and mitigate risk associated with the vulnerabilities.

I will begin with an overview of the evolution of storage from Direct Attached Storage (DAS) to two dominant networked storage solutions – file-based Networked Attached Storage (NAS) and block-based Storage Area Networks (SAN). I will discuss security exposures within each solution and the applicability of "defense in depth" techniques to address security issues in networked storage. Since networked storage is in constant evolution, I will conclude with an overview of emerging trends in storage security.

2. Evolution of Networked Storage

Enterprise information is created, stored and used by various users that depend on its accuracy and instant availability. Information stored can range from financial, legal, and technical to customer-related data. The need to ensure secure access, usage and storage of information is of critical importance since business downtimes or compromised information can cripple a business.

Direct Attached Storage (DAS) consisted of data stored directly on servers, and marked the first generation of enterprise storage. Information stored directly on the servers posed limitations such as provisioning, maintenance and scalability. The sheer size of storage requirements and the need for constant uptime exposed key limitations of DAS solutions. Further, as businesses became more loosely coupled in their operations and moved towards distributed access, centralized data storage became a key challenge.

A second generation of networked storage evolved to solve DAS limitations. The ability to distribute storage across a network led to cheaper and more reliable storage systems in the form of Network Attached Storage (NAS) and Storage Area Network (SAN) solutions. NAS and SAN storage solutions provided additional benefits such as leveraging network-administrative resources to help manage the distributed storage more efficiently. Networked storage led to reducing operational costs and higher productivity.

The rate of migration from DAS to NAS/SAN solutions varies across businesses, but the trend is a dominant one. Research firms like IDC indicate that more than 70% of the businesses will adopt networked storage in the next few years. As with any evolution, there is one critical challenge while adopting NAS/SAN solutions – given the porous network with its incessant vulnerability to network layer attacks, are the second generation storage solutions secure enough?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. The Need for Storage Security

While the benefits of storage networks have been widely acknowledged,[1] consolidation of enterprise data on networked storage poses significant security risks. Hackers adept at exploiting network-layer vulnerabilities can now explore deeper strata of corporate information.

Key drivers to implementing security for networked storage include:

- Perimeter defense strategies focus on protection from external threats. With the number of security attacks on the rise [2], relying on perimeter defense alone is not sufficient to protect enterprise data, and a single security breach can cripple a business [3]
- The number of internal attacks is on the rise thereby threatening NAS/SAN deployments that are part of the "trusted" corporate networks. Reports such as the CSI/FBI's annual Computer Crime & Security Survey[4] help quantify the significant threat caused by data theft
- Certain industry verticals in the USA such as Healthcare and Finance are mandated to conform to regulations such as HIPAA [5] and GLBA [6] respectively. Globalization of markets demands that corporations and their partners meet the security directives in all parts of the world – implying that all distributed storage needs to be secure

Risks due to compromised storage range from tangible loss such as business discontinuity in the form of information downtime, to intangibles such as the loss of stature as a secure business partner. With the number of reported security attacks on the rise**,** a firm understanding of networked storage solutions is a precursor to determining and mitigating security risks.

4. Overview of Networked Storage Technologies and Security

An important observation in a recent Storage Networking Industry Association (SNIA) SNIA report [7] was that "Storage Security issues often fall through the cracks because very few IT professionals understand both security and storage".

An effective networked storage security policy can be built only with a clear understanding of networked storage technologies, the associated security risks and using defense in depth techniques to mitigate known risks. This section provides a primer to NAS and SAN solutions and a brief overview of security to help evaluate a good networked storage security policy.

4.1 Network Attached Storage (NAS)

SNIA defines NAS as "A term used to refer to storage elements that connect to a network and provide file access services to computer systems. A NAS storage

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

element consists of an engine, which implements the file services, and one or more devices, on which data is stored".[8]

The storage elements referred to are typically called NAS filers which provide file-based access to data. NAS filers are a class of IP-based systems or storage appliances that are shared over the network. They use common file sharing protocols like CIFS/SMB, NFS and HTTP to share the file systems that they host. NAS filers typically run an embedded OS hardened against attacks, and support fault- tolerance features such as RAID and data replication.[9]

A NAS implementation using Cisco switches and Network Appliance's NetApp NAS Filers in a high availability environment is shown in Figure 1 below.

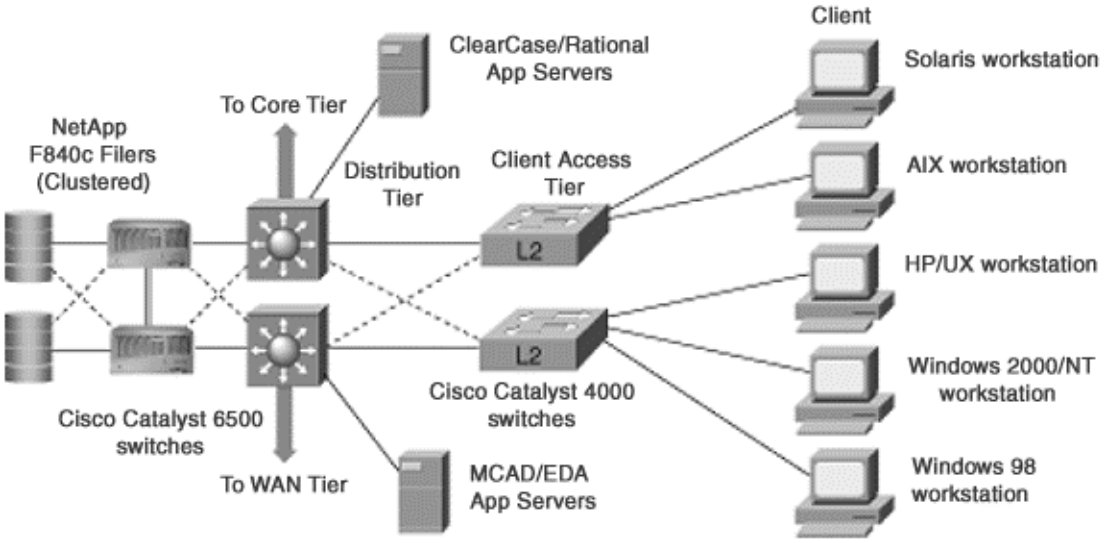

Figure 1: A typical enterprise NAS deployment [10]

4.2 Storage Area Network (SAN)

SNIA defines SAN as "A network whose primary purpose is the transfer of data between computer systems and storage elements and among storage elements. A SAN consists of communication infrastructure, which provides physical connections and a management layer, which organizes the connections, storage elements and computer systems so that data transfer is secure and robust".[11]

SAN is a high speed network of storage devices and hosts that enables sharing data hosted by the storage devices. SANs provide block-based access and include many types of devices such as Host Bus Adapters (HBA), hubs, switches, servers and disk storage. Most SANs currently implemented are Fibre Channel based. Data stored on SANs can be accessed by any hosts connected directly to the SAN and can be shared by using any file-sharing protocol

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

supported by the underlying host-OS. SANs also support data–replication and most SAN storage devices support fault-tolerance features like RAID. Storage on an SAN is advertised to multiple hosts capable of accessing the same storage.[12]

Apart from Fibre Channel, there are also other emerging technologies that leverage existing investments in Ethernet technologies. These technologies include iSCSI (Internet SCSI), FCIP (Fibre Channel over IP) and iFCP (Internet Fibre Channel Protocol). iSCSI allows SAN over IP and allows the use of inexpensive Ethernet technologies like Gigabit Ethernet over copper. FCIP is a proposed standard that will allow SANs to connect over IP and communicate over long distances. iFCP allows SAN devices to be linked to existing IP infrastructures.[12]

A Fibre Channel SAN implementation at the Center of Excellence in Bioinformatics at the University of Buffalo using Dell PowerEdge servers, Dell-EMC storage arrays, Dell PowerVault Tape libraries and Dell PowerVault Fibre Channel switches. is shown in Figure 2 below.

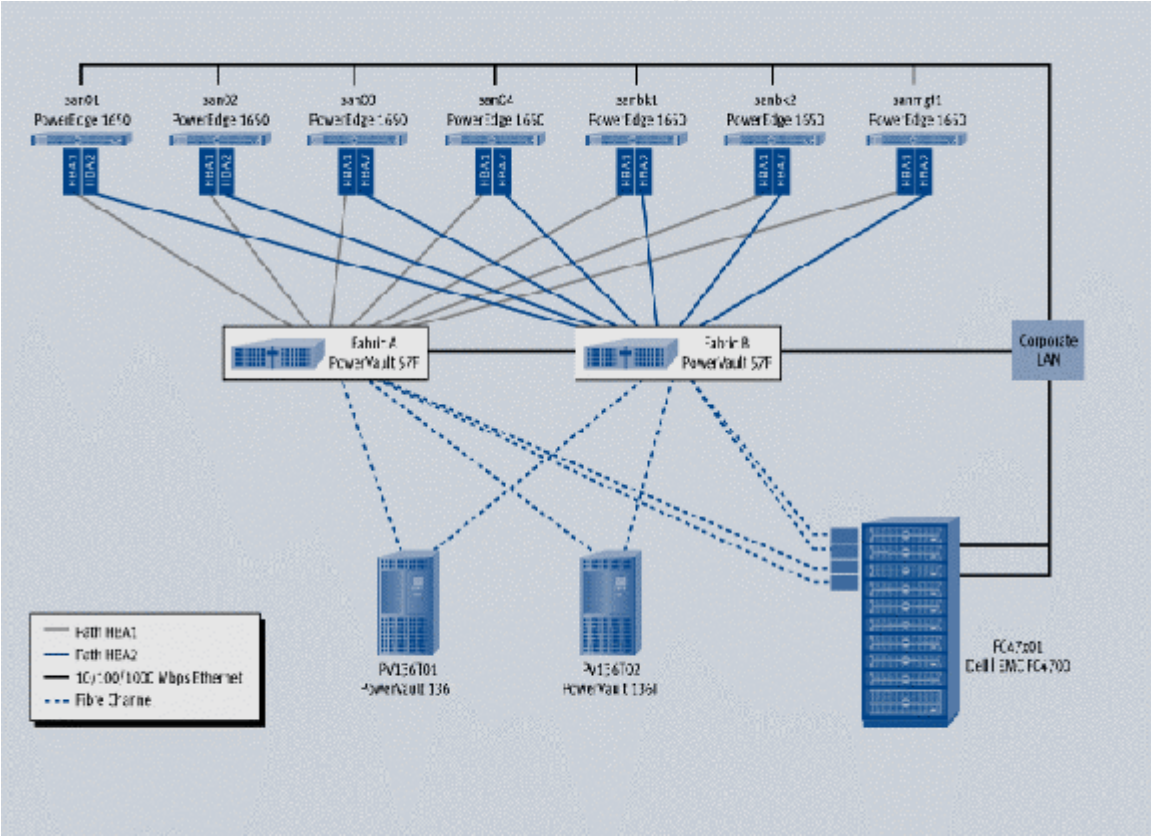

Figure 2: A typical Fibre Channel SAN environment [13]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.3 Security Overview

The fundamental goal of information security is to protect the confidentiality, integrity and availability of information assets, and activities that adversely impact these information attributes are referred to as threats. Threats occur because of system vulnerabilities associated with the information and risk is directly proportional to the level of threat to an information asset.[14]

Defense in Depth (referred to as DID in this paper) is an excellent framework advocating a layered approach to defending against attacks, thereby mitigating risks.[14] A key principle in implementing DID is to use a distributed security model for two reasons:

- There is no single device built for networked storage that can comprehensively secure networked storage
- Leveraging the existing security functions on all the NAS/SAN devices provides a distributed, resilient and stronger level of protection vis-à-vis a centralized single-device security model with a concentrated point of vulnerability

This section concludes an overview of NAS, SAN and Security technologies. We will now take a look at the vulnerabilities in networked storage deployments.[34,35,36]

5. Vulnerabilities in Networked Storage Technologies

NAS and SAN implementations can get to be very complex. A DID-based methodical approach to mitigate risks begins by segmenting the networked storage into layers and analyzing each layer for vulnerabilities.

Using this approach, typical NAS/SAN deployments can be segmented into four layers:

1. Devices on the storage network
2. Data access
3. Network connectivity
4. Management access

Vulnerabilities in NAS and SAN deployments [19,20] are discussed separately in the following subsections.

5.1 NAS Vulnerabilities

<u>Layer 1 – Devices on the storage network</u>

Devices in this layer consist of NAS filers or NAS servers that share the file systems with the entire network. Vulnerabilities in this layer are rooted in the OS on the filer/server and include:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Unauthorized access due to weak authentication and authorization mechanisms. Usage of default username and passwords that are preconfigured on the NAS appliances, weak passwords and the reliance of just username and password for authentication are some examples
- Security breaches based on published vulnerabilities in the OS and services provided by the OS. For example, a CERT advisory (CA-2002-19) regarding "buffer overflow in DNS resolver libraries" that could let an attacker execute arbitrary code or cause a denial of service on a vulnerable system, affected NetApp NAS filers which run Network Appliance's proprietary OS called Data ONTAP, and needed patches to the OS to resolve the issue [15]

Layer 2 – Data access

Data stored on NAS is shared using file systems such as CIFS/SMB (Common Internet File System / Server Message Block) and NFS (Network File System). Commonly known vulnerabilities using these protocols, include unauthorized access due to:

- CIFS share-level authentication. Share-level authentication uses only a single password per share and the passwords are transmitted in plain text which are vulnerable in transit [16]
- CIFS user-level authentication based on LanMan which is highly insecure [16]
- NFS transactions in clear text. Sniffing of NFS transactions can lead to unauthorized access to NFS shares, by using the UID and the NFS file handle within the NFS transaction to mount NFS shares [17]
- Limited authentication of NFS for mounting NFS shares - based solely on host-name authentication [18]
- Loss of data integrity and availability of due to viruses, worms and Denial of Service (DoS) attacks

Layer 3 – Network connectivity

Since NAS appliances are IP-based, they are subject to well known attacks such as DoS attacks, session hijacking, IP-spoofing that take advantage of IP-based vulnerabilities.

Layer 4 – Management access

Management of NAS appliances includes the administration of the device, the file systems and the stored data. Vulnerabilities include

- Unauthorized access by sniffing of passwords due to the use of clear-text communication protocols like Telnet and HTTP for access
- Unauthorized access due to weak authentication and authorization mechanisms. Weak passwords, use of default usernames and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

passwords and single-factor authentication using just a username/password combination contribute to the weakness

- Lack of access control and auditing measures. Sharing of administrator access, unrestricted user access, and inability to determine the actions of a user are some common examples

5.2 SAN Vulnerabilities

Layer 1 – Devices on the storage network

All hosts and servers connected to a SAN have access to the data stored on the SAN storage devices, and thus pose vulnerabilities such as:

- Unauthorized access due to weak authentication and authorization schemes of the OS on the servers and hosts connected to the SAN
- Security breaches based on published vulnerabilities in the OS and services provided by the OS on the servers and hosts. Servers and hosts on a SAN can be powered either by Linux, Windows, Solaris or any other OS and the weakest host can act as an attack gateway
- Security breaches based on published vulnerabilities in widely used applications such as Oracle, Exchange and SAP running on hosts accessing SAN storage

Layer 2 – Data Access

Data stored on a SAN can be shared using servers configured similar to NAS appliances, i.e. using NFS and CIFS/ SMB. The data can also be directly accessed by applications such as mail servers and database servers. Vulnerabilities include:

- Unauthorized access due to weaknesses in CIFS share-level and certain user-level authentication implementations [16]
- Unauthorized access due to weaknesses in NFS as discussed in the NAS Data Access section [17,18]
- Loss of data integrity and availability due to viruses, worms and DoS attacks
- Data theft based on unfettered access to storage devices by all hosts on the SAN

Layer 3 – Network connectivity

SAN devices are connected using HBAs, hubs, switches and mostly use Fibre Channel protocol. SANs were presumed to be more secure based on its isolated network characteristics. However, Fibre Channel is not a secure protocol in itself, and some of the vulnerabilities include:

- Unauthorized access to data using Fibre Channel protocol weaknesses. Spoofing World Wide Names to assume identity of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

legitimate devices, rouge switches added to the SAN taking advantage of weak authentication between FC entities, snooping and data-hijacking because of the lack of data encryption capabilities are some examples of the protocol vulnerabilities

- Lack of access control and auditing measures on the network devices such as the switches make it an easy target
- Unauthorized access using man in the middle attacks, spoofing and data hijacking because of the use of in-band management access – using the data network for management activities
- Security breaches based on improperly configured devices and use of default configurations

Layer 4 – Management access

Management of all SAN devices includes overcoming vulnerabilities such as:

- Unauthorized access by sniffing of passwords due to the use of insecure access protocols like Telnet and HTTP
- Unauthorized access due to weak authentication and authorization mechanisms. Weak passwords, use of default usernames and passwords and single-factor authentication using just a username/password combination can lead to breaches resulting in unauthorized modifications of configurations, Name Server records, routing tables, and so on
- Lack of access control and auditing measures. Sharing of administrator access, unrestricted user access, and inability to determine the actions of a user are some common examples

With this overview of vulnerabilities in each NAS and SAN layer, the next section discusses ways to mitigate risk at each layer.[34,35,36]

6. Risk Mitigation for Networked Storage

Having identified vulnerabilities at each layer, we will now discuss steps to mitigate the risks, [19,20] with an emphasis on distributed and layered security measures for Defense in Depth.

6.1 Defense in Depth for NAS

Layer 1 – Devices on the Storage Network

The following risk-mitigation measures are recommended:

- Authentication schemes provided by the OS should be evaluated. Schemes utilizing public- private key based authentication such as SSH or Kerberos, which also encrypt authentication communications on the network, should be used

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Two-factor authentication mechanisms, like Biometrics, Tokens or SSL User Authentication can enhance security. [21] Decru, a storage security appliance manufacturer, supports two-factor authentication using Smart Cards on their DataFort storage security appliance [22]
- Authorization using Access Control Lists (ACL) to setup role-based access and appropriate permissions will enhance security
- Strong password schemes like minimum length passwords and periodic change of passwords should be enforced. The default username and passwords that are configured on the device should be changed
- Constant monitoring of published OS-vulnerabilities using CVE database, Bugtraq, SANS Security Alert Consensus newsletter and the NAS vendor's support site, is a necessity to prepare for possible attacks
- Regular patch maintenance including recommended security patches for the OS should be strictly enforced, since most attacks exploit well-known vulnerabilities in the OS itself
- Periodic use of vulnerability scanners like Nessus, Saint and others help discover hidden vulnerabilities and provide an audit of the systems
- Though most NAS devices use embedded and hardened OS, all services running on the devices should be reevaluated using tools like nmap. Unused or unnecessary services and ports should be disabled
- Logging and auditing controls should be implemented to prevent unauthorized use, track usage and for incident response

<u>Layer 2 – Data access</u>

Risks can be mitigated by enforcing policies based on the methods below

- A data classification policy, based on the importance and sensitivity of the data, must be created and enforced. The classification should also identify the users allowed to access the appropriate class of information and their respective permissions. A sound methodology for achieving this objective is outlined in Susan Flower's paper "Information Classification – Who, Why and How" in the SANS Reading Room. [23] A data classification policy helps segregate data and allows for strong data access controls to be enforced using ACLs on the OS
- Encryption based on data classification should be implemented to safeguard data, both during transit and while at rest. Decru's DataFort storage security appliance supports data encryption on NAS [22]
- Enforce CIFS NTLMv2 user-level authentication mechanism only. User-level authentication uses per-user authentication and is more secure than share-level authentication. Furthermore, the use of NTLMv2 encrypts the username/password combinations and is recommended over LanMan [24]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Use IP Address for hostnames for host-based authenticated mounting of NFS shares and audit all NFS share configurations [25]
- Encrypting NFS traffic using SSH port-forwarding reduces the risk associated with the clear-text communications inherent to NFS [26]
- Enforce logging and auditing for tracking usage and for incident response
- Real-time protection of data on NAS filers against viruses and malicious code enhance the integrity of data. Anti-virus software vendors like Symantec and Trend Micro offer products for NAS data protection

Layer 3 – Network connectivity

NAS appliances face similar vulnerabilities as IP based network devices. Common techniques used to protect IP networks are also applicable to NAS:

- Extending network perimeter defense strategies like using a Firewall and IDS device to filter traffic reaching the NAS appliance will increase protection
- Use VLANs for segregating traffic to the NAS appliances
- Separate and isolate management interface from data interfaces on the NAS, thus enforcing out-of-band management which is more secure
- Monitor traffic patterns on the data interfaces of the NAS devices for unusual activity

Layer 4 – Management access

Management access is a significant source of attack. To address the vulnerabilities, the following guidelines provide help

- Disable the use of telnet and HTTP and enforce management access through SSH and HTTPS for encrypted communication
- Create separate user accounts based on the management tasks assigned to the users
- Implement strong authentication mechanisms like two-factor authentication using tokens, biometrics, etc
- Strong password schemes like minimum length passwords and periodic change of passwords should be enforced
- Implement authorization using Access Control Lists to setup role-based access and appropriate permissions
- Enforce logging and auditing to prevent unauthorized use, track usage and for incident response
- Restrict the management of the storage network devices from specific hosts

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

6.2 Defense in Depth for SAN

Layer 1 – Devices on the storage network

Since all hosts and servers on SAN have access to the data on the SAN, the weakest host can become a gateway providing unauthorized access to the data. Hence each host and server vulnerability such as the following needs attention:

- Authentication schemes provided by the OS and applications should be evaluated. Schemes utilizing public- private key based authentication such as SSH or Kerberos, which also encrypt authentication over the network, should be used
- Two-factor authentication mechanisms, like Biometrics, Tokens or SSL User Authentication can enhance security.[21] Decru, a storage security appliance manufacturer, supports two-factor authentication using Smart Cards on their DataFort storage security appliance [22]
- Authorization using Access Control Lists (ACL) to setup role-based access and appropriate permissions will enhance security
- Strong password schemes like minimum length passwords and periodic change of passwords should be enforced. The default username and passwords that are configured on the device should be changed
- Constant monitoring of published OS and application vulnerabilities using CVE database, Bugtraq, SANS Security Alert Consensus newsletter and the vendor's support site, is a necessity to prepare for possible attacks
- Regular patch maintenance including recommended security patches for the OS and applications should be strictly enforced
- Periodic use of vulnerability scanners like Nessus, Saint, and others help discover hidden vulnerabilities and provide an audit of the systems
- Services running on the hosts, servers and devices should be reevaluated using tools like nmap. Unused or unnecessary services and ports should be disabled
- Use of Host-based IDS software like Tripwire on the hosts and servers will enhance security
- Logging and auditing controls should be implemented to prevent unauthorized use, track usage and for incident response

Layer 2 – Data access

Unauthorized access to data affects the confidentiality, integrity and availability of the data due to theft, modification, corruption or destruction of data. Vulnerabilities can be prevented by following the practices mentioned below:

- A data classification policy, based on the importance and sensitivity of the data, must be created and enforced. The classification should also identify the users allowed to access the appropriate class of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

information and their respective permissions. A sound methodology for achieving this objective is outlined in Susan Flower's paper "Information Classification – Who, Why and How" in the SANS Reading Room.[23] A data classification policy helps segregate data and provides guidelines for data access controls

- Encryption based on data classification should be implemented to safeguard data, both during transit and while at rest. Decru's DataFort and NeoScale's CryptoStor FC storage security appliance support encryption of data on the SAN [22]
- Enforce CIFS NTLMv2 user-level authentication mechanism only. User-level authentication uses per-user authentication and is more secure than share-level authentication. Furthermore, the use of NTLMv2 encrypts the username/password combinations and is recommended over LanMan [24]
- Use IP Address for hostnames for host-based authenticated mounting of NFS shares and audit all NFS share configurations [25]
- Encrypting NFS traffic using SSH port-forwarding reduces the risk associated with the clear-text communications inherent to NFS [26]
- Implement partitioning based on the data classification policy and on the application access requirements using LUN masking. Logical Unit Numbers (LUNs) represent storage media such as disks and tapes and are advertised to hosts. The ability to assign specific LUNs to hosts thereby limiting the visibility of the hosts to only the LUNs assigned to them is called LUN masking [27]
- Enforce logging and auditing for tracking usage and for incident response
- Monitor the hosts, servers and applications for unusual and abnormal activity that might indicate an infected host
- Implement anti-virus applications on the hosts and servers to prevent data corruption due to viruses

<u>Layer 3 – Network connectivity</u>

Vulnerabilities on the storage network can be overcome using a combination of security features currently present, which include

- Implement zoning to segregate traffic from the hosts to storage resources and restrict communication between the SAN devices. Zoning allows devices to be segmented into logical groups called zones. A zone consists of servers, switches, host Bus Adapters, Storage disks and other elements. Hard zoning implements zones on the switch and is based on switch ports. A hard zone implemented in the switch's circuitry allows communication only between ports in the zone based on the switch's port routing table. Soft zoning is based on a unique identifier assigned to each Fibre Channel device called World Wide Name (WWN). Software on the switch maintains a table of WWNs assigned to a zone ensures that communication between

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

WWNs in different zones is dropped. While soft zoning is flexible, hard zoning is more secure [28]

- Implement port binding on switches to prevent WWN spoofing. Port binding binds a WWN to a specific switch port allowing connections of that device only through the predefined port thereby preventing other devices to assume the WWN's identity [29]
- Implement vendor specific security techniques. For example, Brocade's Secure Fabric OS provides for additional security by enforcing switch authentication [30]
- Create a separate management network which is isolated from the data network, thus preventing insecure in-band management activities
- Extend network perimeter defense strategies like using a Firewall and IDS device to filter traffic reaching the SAN
- Monitor traffic patterns on the data network for unusual or increased activity indicating DOS attacks

<u>Layer 4 – Management access</u>

Management access poses significant risk to data and the following guidelines help address the vulnerabilities.

- Disable the use of telnet and HTTP for management access and implement SSH and HTPS for encrypted access
- Create separate user accounts based on the management tasks assigned to the users
- Implement strong authentication mechanisms using biometrics or tokens for two factor authentication
- Strict password policy enforcements with strong passwords and periodic change of passwords are essential
- Implement authorization using Access Control Lists (ACL) to setup role-based access and appropriate permissions
- Restrict management of the SAN devices from specific hosts
- Centralized management of the entire SAN provides greater visibility of the entire topology, effective administration with enhanced security. Vendors like Veritas, IBM, Computer Associates, BMC Software, McData and others now support functions like zoning and LUN masking as part of their storage management software
- Enforce logging and auditing to prevent unauthorized use, track usage and for incident response

7. Trends in Storage Security

There has been considerable effort by the storage industry to deliver standards and technologies for securing storage networks. Key drivers to adopting these standards within the industry have been the need for compatibility of the storage

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

offering with the current enterprise infrastructure, and interoperability with each other.

Some of the groups driving security standards within storage are:

1. IETF IP Storage Working Group [31]
    - IPSEC encapsulating ISECI

2. ANSI TII Fibre Channel Security Protocols Working Group [32]
    - FCSec: encapsulating and authentication of FC SCSI packets using IPSEC
    - FC-AP using CHAP for switch authentication

3. IEEE Storage System Standards Working Group [33]
    - Proposals to standardize encryption in storage systems

While standards are still being developed, industry consortiums have formed forums to promote storage security and to accelerate the development of storage security standards like SNIA's Storage Security Industry Forum.

8. Conclusion

Corporate information continues to remain the blood line of any business. First generation server attached storage systems (DAS) ran into size, scalability and manageability limitations, and an unexpected challenge of an increasingly networked world. Second generation networked storage solutions (NAS/SAN) leveraged IP-based investments and were created to primarily overcome DAS limitations of manageability and accessibility. However security on these systems was overlooked, opening them up to increased security risks. Current security measures do not provide effective defense to the new security challenges posed by networked storage and require businesses to reevaluate their security strategy.

This paper suggests a methodical application of "defense in depth" security techniques that can help allay security risks in networked storage. More importantly, a defense in depth based networked storage security policy provides a comprehensive framework to thwart future attacks as the current technologies are more clearly understood. The emerging standards in storage security in conjunction with defense in depth will help in making storage much more resilient to future threats.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

9. References

[1] Brocade Communication Systems, Inc. "Comparing Storage Area Networks and Network Attached Storage". URL: http://www.brocade.com/san/white_papers/pdf/SANvsNASWPFINAL3_01_01.pdf

[2] CERT Coordination Center. "CERT/CC Statistics 1998-2003". URL: http://www.cert.org/stats/cert_stats.html

[3] Washington Post. "8 Million Credit Card Accounts Exposed". February 19, 2003. URL: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A27334-2003Feb18&notFound=true

[4] Computer Security Institute. "The 2003 CSI/FBI Computer Crime and Security Survey". URL: http://www.gocsi.com/press/20030528.html

[5] HHS – Office for Civil Rights – HIPPA. URL: http://www.hhs.gov/ocr/hipaa/

[6] Federal Trade Commission. "In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act". URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

[7] Computerworld. "Enterprise Storage Security: Context, Challenges and Solutions". February 17, 2003. URL: http://www.computerworld.com/computerworld/records/whitepapers/storagewpfeb17.pdf

[8] Storage Networking Industry Association. "A Dictionary of Storage Networking Terminology". URL: http://www.snia.org/education/dictionary/n/#network_attached_storage

[9] John Chirillo and Scott Blaul. "Storage Security: Protecting, SANs, NAS and DAS". Wiley Publishing, Inc. 2003. 51 – 58.

[10] Iftikhar Ahmed, Rajesh Godbole and Shiva Vishwanathan. "An Open Standards Approach to Network-Centric Storage". Network Appliance, Inc. URL: http://www.netapp.com/tech_library/3121.html

[11] Storage Networking Industry Association. "A Dictionary of Storage Networking Terminology". URL: http://www.snia.org/education/dictionary/s#storage_area_network

[12] John Chirillo and Scott Blaul. "Storage Security: Protecting, SANs, NAS and DAS". Wiley Publishing, Inc. 2003. 87 – 100.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[13] Geoff Mattie. “Dell HPC Cluster Enhances Bioinformatics Research at the University at Buffalo”. Dell Power Solutions, Dell Computer Corp. November 2002. URL: http://www.dell.com/us/en/esg/topics/power_ps4q02-mattie.htm

[14] SANS Security Essentials. “SANS Security Essentials II: Network Security Overview”

[15] CERT Coordination Centre. “CERT® Advisory CA-2002-19 Buffer Overflows in Multiple DNS Resolver Libraries”. June 28, 2002. Last revised September 9, 2002. URL: http://www.cert.org/advisories/CA-2002-19.html

[16] Bridget Allison. “CIFS Authentication and Security”. NetApp Library, Network Appliance, Inc. URL: http://www.netapp.com/tech_library/3020.html

[17] Redhat Linux. “Red Hat Linux 9: Red Hat Linux Security Guide”. Redhat Linux Manuals, Redhat Inc. URL: http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-server-nfs.html

[18] Redhat Linux. “Red Hat Linux 9: Red Hat Linux Reference Guide”. Redhat Linux Manuals, Redhat Inc. URL: http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-nfs-security.html

[19] John Chirillo and Scott Blaul. “Storage Security: Protecting, SANs, NAS and DAS”. Wiley Publishing, Inc. 2003. 59 – 86.

[20] John Chirillo and Scott Blaul. “Storage Security: Protecting, SANs, NAS and DAS”. Wiley Publishing, Inc. 2003. 97 – 116.

[21] Rainbow Technologies. ”Two-Factor Authentication – Making Sense of all the Options”. The Encyclopedia of Computer Security. 2 February, 2002. URL: http://www.itsecurity.com/papers/rainbow2.htm

[22] Decru Inc. “Decru DataFort ™ Security Appliances”. URL: http://www.decru.com/products/datafort0.htm

[23] Susan Fowler. “Information Classification – Who, Why and How”. SANS InfoSec Reading Room. February 28, 2003. URL: http://www.sans.org/rr/paper.php?id=846

[24] Randy Franklin Smith. “Inside SP4 NTLMv2 Security Enhancements”. Windows & .Net Magazine. September 1999. URL: http://www.win2000mag.com/Articles/Index.cfm?ArticleID=7072&pg=1&show=1234

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[25] Redhat Linux. "Red Hat Linux 9: Red Hat Linux Reference Guide". Redhat Linux Manuals, Redhat Inc. URL: http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-nfs-security.html

[26] Tavis Barr, Nicolai Langfeldt, Seth Vidal and Tom McNeal. "Linux NFS-HowTo". August 25, 2002. URL: http://nfs.sourceforge.net/nfs-howto/security.html#NFS-SSH

[27] Bill King. "LUN Masking in a SAN". QLogic Corporation. October 8, 2001. URL: http://www.qlogic.com/documents/datasheets/knowledge_data/whitepapers/whitepaper.lunmasking.pdf

[28] Mike O'Donnell. "An Introduction to Zoning". McData Corporation. April 2002. URL: http://www.mcdata.com/downloads/whitepapers/zoning.pdf

[29] Michael O'Donnell. "Security in Switched Fibre Channel SANs". McData Corporation. April 2001. URL: http://www.mcdata.com/downloads/whitepapers/SecurityInSANs.pdf

[30] Brocade White Paper Library. "Advancing Security in Storage Area Networks". Brocade Communication Systems, Inc. URL: http://www.brocade.com/san/white_papers/pdf/Adv_Security_WP_03.pdf

[31] IETF IP Storage Working Group. URL: http://www.ietf.org/html.charters/ips-charter.html

[32] ANSI TII Fibre Channel Security Protocols Working Group. URL: http://www.t11.org

[33] IEEE Storage System Standards Working Group. URL: http://www.ssswg.org

[34] W. Curtis Preston, Himanshu Dwivedi and Michel Kabay. "Storage Security Handbook". Neoscale Systems Inc. January 2003. URL: http://www.itstorageonline.com/content/news/article.asp?docid={abd4eb35-bf9e-427f-a138-2ad3223231d4}

[35] Elizabeth Clark. "Fibre Channel SAN Security". NetworkMagazine.com. September 2002. URL: http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleID=8703406

[36] Dr. Vijay Ahuja, Hugo Fruehauf and Roger Cummings. "SNIA Security Tutorial". Storage Networking Industry Association. URL: http://www.snia.org/education/tutorials/Security.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced