Layered Approach for Securing the Storage Infrastructure

Rajesh Ramachandran

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option 1
April 12, 2003

1. Abstract:

Network storage is changing the way business operates. This new evolving storage technology opens new avenues for handling the data, by individuals and companies. The remote storage over wide area network technology (internet SAN – iSAN, Fiber Channel over IP- FCIP, internet Fiber Channel Protocol - iFCP), which has evolved from locally connected storage (Direct Attached Storage – DAS), and storage network (Network Attached Storage – NAS and Storage Area Network – SAN) opens a plethora of vulnerabilities and threats. This paper will discuss the possible vulnerabilities and threats that may manifest at various layers of Shared Storage Model [1] and how applying the security principles such as Confidentiality, Integrity and Availability would mitigate these threats. At the end we will also cover the various research groups contributing for developing standards pertaining to storage and the solutions available in the market from various vendors.

2. Why do we need to secure our storage?

In the past, the data storage was de-centralized with each workstation or server had its own internal storage or Storage attached to the machine directly using Small Computer System Interface (SCSI). This was sufficient for relatively small storage needs and the dataset. The growing business needs, storage hungry applications, and the need for sharing data within and outside business entities led to the evolution of two types of Storage network—Storage Area Network (SAN) and Network Attached Storage (NAS). SAN [2] is a high-speed special-purpose network that interconnects different kinds of data storage devices with associated servers with a larger network of users and this system shares data on block level. The Network Attached Storage (NAS) [2], unlike SAN, takes the functionality of the data and application servers and shares them much more efficiently for multiple users. Generally, NAS devices have a network address (IP), support multiple protocols, and also emulate different file systems. The SAN and NAS are a big leap from direct attached storage, despite concerns about security of the data stored in these devices (data-at-rest) and data on wire when the data is accessed by users, applications and while being backed-up (data-in-motion).

In networks based on NAS and SAN data is stored centrally. There are advantages and disadvantages of this. Consolidating the data allows for better control and makes it more manageable and scalable. However, it also requires an increased attention to various threats like virus attacks, data theft, and disasters. Statistics show that chances of virus attacks and data theft are high from within the network. And, since the data is stored externally in order to perform a disaster recovery makes these kinds of network based storage systems more vulnerable. Given this storage security is of critical importance to most businesses and the government. Storage security, I believe, is important of having a robust security shield and it complements the efforts that many organizations make in securing their IP based network security including perimeter security (firewall, IDS, content management servers etc). Securing storage is securing ones Intellectual Property.

Neglecting storage security could mean:

- increased down time due to security related incidents,
- lack of stability in providing consistent data access for the users and application

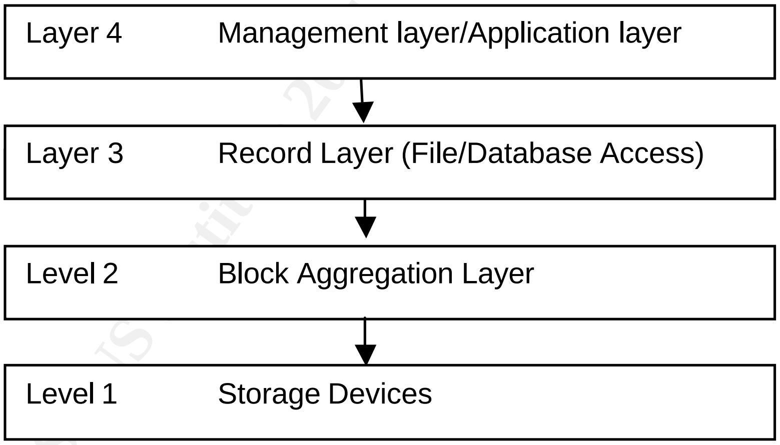
The result of the above would deteriorate business performance.

Governmental mandates, through various legislations and decrees like the ones listed under, to protect the sensitive data of consumers are a good start.

- **HIPAA** [20]: Ensures the confidentiality, integrity and availability of medical records of the patients.
- **Gramm-Leach-Bliley Act** [21]: Financial institutions have to disclose policies for protecting the non-public customer personal information.
- **Sarbanes –Oxley** [22]: Ensures the accuracy of corporate disclosures made under security laws.
- **California state law SB1386** [23]: Requires that all state agencies and businesses that collect information from individuals need to disclose the security breaches promptly.

3. Layered view of Shared storage model

The SNIA has defined *de facto* model for the storage network called as Shared Storage Model [1]. The model is very similar to the ISO model for networking the model separates the data access into layer as shown in exhibit bellow


Layer 4 Management layer/Application layer
Layer 3 Record Layer (File/Database Access)
Level 2 Block Aggregation Layer
Level 1 Storage Devices

This model forms the basis to identify various components that are required to build the storage network infrastructure. This model also depicts the complexity of the infrastructure and why security is important.

- Currently storage networks are comprised of multi-vendor and multi component structure integrated together without a standardized protocol of operation. There are working groups like T11 and others, setup and performing research at various area of storage networking.

- Many recommend using multi vendor solution for perimeter protection or anti-virus application, since this approach minimizes the possibility of compromising the entire network security if one vendor’s product fails. The same approach to storage security should be recommended allowing multiple vendors to provide solutions for different aspects of storage network security. This avoids single point of failure and also allows the customers to achieve more accurate solution to satisfy their business need. For example, using anti-virus product from multi vendor. Using products from Symantec for messaging infrastructure and McAfee anti-virus products on clients and servers. And probably a third vendor for managing and reporting all these products to a central location.
- Once we place the components for each layer we can apply the “Defense-in-depth” concept of security to each one of these four layers. We will analyze how the four major concepts of security, i.e., Confidentiality, Integrity, Authentication and Availability apply to each of these layers.

4. Components of Shared Security model and some identified threats

4.1 Application layer:

4.1.1 Components: This comprises of all the management applications that are used to manage and monitor the storage devices, operating system of the management station, backup software, the network management application and the network protocol security. This is the most crucial layer on storage security model since components on this layer interact closely with other layers on every aspect of storage security.

4.1.2 Data state: Mostly Data-in-motion

4.1.3 Threats: The major threats identified in this layer can be further classified into two types 1) IP Based threat [3], 2) threats initiated from Management application and workstation [4]

4.1.3.1 IP Based threats/Transport:

- IP port hacking could lead to DoS [6] (Denial of Service attacks)
- Data and management Hijacking [6]. Once the attacker get the relevant data including username, password and connection parameters. He/She can redirect the data going forward to his/her management workstation
- Port vulnerability would allow intruder to connect using known application like ftp or telnet
- Known operating system services which are not required for storage functionality may have some vulnerability which would lead compromise in security
- Spoofing [6] the management data including username and password
- Applying a Trojan or Virus through the weak port causes an availability threat.

4.1.3.2 Management application: [4]

Management application would the applications used for network device, storage device and data management application.

- There are many occasions where the installation is left with default password and username and if fact some cases multiple roles (backup and storage administrators) use the same login credentials.
- Passing the login credentials in clear text.
- Access to management or backup software allows anyone to install the client and start managing the storage or initiate a backup job from remote location
- Allowing remote access to the management workstation.
- Physical security plays a major role; this includes the fabric setup where the switches and storage is located. The management station left open for access allows any user to login and perform administrative tasks.

4.2 File/Record layer:

4.2.1 Components: This layer includes the file system and other database systems used to store the data in storage. Couple of the most commonly used Relational databases is MS SQL Server and Oracle. The two most commonly user files systems are Common Internet File System (CIFS) and Network File Systems (NFS).

4.2.2 Data state: Data-in-rest and Data-in-motion

4.2.3 Threats: The threats identified are also classified according to the components available in this layer

4.2.3.1 Database systems [7,8,9]: Two major aspects of database security are secure transmission and secure data storage

- Risk due to operating database installations with default system administrator password and without hardening the OS.
- The database server by default is installed to answer for multiple protocols. Some of these protocols like Named pipes are prone for multiple vulnerabilities.
- The catalog tables that house the user data are not secured in most of the installations.
-

4.2.3.2 File systems: CIFS is primarily used to support Windows based clients. This allows multi vendor client operating system to open the files shared from NAS device. This is the extension of Windows® open cross-platform Server Message Block (SMB), also available in UNIX, VMS and OS/2. NFS is primarily used in UNIX or Linux world. CIFS based threats are [5,10]:

- CIFS security is based on share-level. This share based authentication requires having only one password per share and there is no audit trail for multiple users.
- SMB extension of CIFS allows user authentication. This allows previous Windows authentication methodologies including NTLM (NT LanMan) and LM (LanMan). Both these have serious flaws in the way they hash the authentication parameters (username and password).
- The authentication data is passed as clear text.
- If CIFS is used without the SMB feature the server authenticates the client and the client does not. This exposes the system for threats like sniffing, Man-in-the-middle etc.

4.2.3.3 NFS based threats [5,11]:

- Uses clear text for passing authentication parameters
- NFS file system exported with root privilege allows users from remote workstations to with administrative access to view this Exports file system data, which can easily obtained by spoofing
- NFS clients have very limited options when it comes to authentication methodologies.
- inode number can be guessed very easily to gain file access if the generator does number is not randomized

4.3 Block Aggregation Layer

This layer renders the raw storage to all the upper layers. The aggregation part is done in one of the three components hosts, components of storage network or most commonly the storage itself. Any one of the following techniques may be used space management, striping or redundancy. This layer along with the other layers defines the data path and the storage architecture if it is DAS, NAS or SAN. To increase the performance there is cache involves in every layer or even a dedicated cache appliance. This improves the performance but it makes the setup more complex because you have to deal with tracking copies of metadata (data about data). There are multiple access paths to the storage device, this allows more threats manifest.

4.3.1 State of Data: Data-at-rest and Data-in-motion

4.3.2 Threats

- On the host level aggregation there are Host Bus Adapters (HBA) and device drivers involved in connecting the fabric or the storage directly to the hosts. Most HBA allow changing World Wide Name (WWN) allowing connecting to different zone.
- If the storage system is not protected using encryption, any wrong configuration in zoning could expose breach in the confidentiality of data.

4.4 Device layer:

This layer is comprised of the actual storage devices. Any of the threats in the layers above would affect the operation of these devices.

4.4.1 State of data: Data-at-rest

4.4.2 Threats

- Un-authorized user taking over the management stations because of lack of physical security, weak authentication or authorization.
- Spoofing of WWN or port configuration would allow the device to send valid data to invalid destination.
- Wrong zoning configuration would also render data to wrong destination.

5. Solutions to mitigate the threats identified through Shared Storage model:

5.1 Application layer:

This layer has been the primary target for intruders to take control of the storage system. When we say application layer we are addressing the management application, not the business application. The following are some recommended means of mitigating the threat

- First step to mitigate the threat is to get familiarized with every possible data path to the storage.
- The management application has to be installed preferable in only one workstation, the cabinet should be locked and there should be strong physical security (preferably two-factor authentication) to enter the premises.
- Login to the management station has to be preferably a two-factor authentication [12] and with strong password. This will reduce the chances of storage compromise if the password is lost or spoofed.
- Disable all connections that use clear text data transfer. Use encrypted data transfer like SSH, SSL or Kerberos technology for management. Most of the storage vendors support HTTPS (SSL) based connection to the management web interface.
- Storage management is very similar to network management. It is recommended that the storage management network segment is separated from rest of the network segment.
- Services available for each IP port have to be identified and check if they are configurable. If not they have to be disabled. IP ports have to be identified and hardened to handle various traffics.

- Use IPSec and DES to encrypt the data and the management traffic on both and in-band and out-of-band management. The transport layer has significant data exposure especially nowadays most of the businesses are moving into geographically disbursed storage architecture.
- Follow the standard hardening procedure for OS hardening (CERT and SANS).[13,14] . Disable the services not used and apply all the service packs and patches to address the vulnerabilities related to the applications such as telnet, ftp and other remote access applications.
- Turn on the available auditing in both OS and the management application. Use OS level authentication and ACL to set much granular permissions to management application access.
- Use the available security feature like encryption available with the any application. Veritas Netbackup™ [15] backup software allows encrypting the data while backing up.

5.2 File/Record Layer

Data stored in storage network is broadly classified into two categories files system and databases. Most of these file system and database installations are “out of the box” installations.

5.2.1 File systems

5.2.1.1 Common Internet File System (CIFS) [5,10]

- NAS devices that use CIFS operating system should not use Share level permission
- Always use user level authentication and do not use version less than NTLMv2
- Use SMB signing for CIFS. This allows both the server and client side authentication. SMB signing assigns a digital signature on each packet.

5.2.1.2 Network File System (NFS) [5, 11]

Use RSA/DES to encrypt any communication between NFS client and server. This avoids the spoofing attack from capturing clear text password transfer.

- Use Kerberos v5 based authentication.
- Use IP address with the host name for NFS authentication.

5.2.1.3 Database systems [9]

Most of the databases are installed on SAN. SAN segments the data on the block level. There could be multiple databases using the striped same physical device aggregated based on the database size and performance requirement.

- Databases should rely on internal security to lock the data in the catalogs.
- Enforce strong password structure for system administrative privilege.
- Define clearly using permissions who can read, write or modify data in the table
- Avoid user’s direct access to data. Use middle tier applications to query the database and cache the information the users need.
- Separate the security catalogs (contains username and password) from application catalogs (holds application specific data) and encryption them.

5.3 Block Layer: (Block Aggregation Layer + Device)

Device: Performs data aggregation, LUN configuration, caching (with non-volatile write-behind data), and simple access control

Block Aggregation Layer: This layer performs functionality that is done either by hosts (HBA, device drivers, logical volume managers, caching and RAID controllers), network components (SN appliances, caching appliance) or the storage devices (RAID Controllers and caching device) themselves.

- The hosts are involved in block aggregation, the driver and firmware for the HBA and RAID controllers has to be checked periodically against manufacturer's website list for vulnerabilities or enroll for email notification.
- The block data in the storage has to be encrypted to prevent data compromise due to faulty zoning configuration.
- If there are caching device involved make sure that data in these devices are encrypted as well. Wherever configurable set values for cache aging.
- Used the RAID techniques to increase the availability if there is a compromise. Different RAID levels allow improvement in performance (striping RAID 0) and availability (mirroring RAID 1 and data striping with striped parity RAID5).
- Implement anti-virus in hosts and servers connecting to storage to increase the availability
- Update the vulnerability patches on workstations, servers and storage as soon as they are available.
- For crucial systems install HIDS (Host Intrusion Detection System) to prevent, track and monitor both internal and external intruders.

5.4 Device layer

Storage security is still in the process of evolutions. There are no clear standards on security. There are very limited products available in the marketplace to address all or most of the storage network components. This layer depends on the vendor solutions offered by various components.

- Access to storage device due to lack of security in management interface. Two-factor authentication is required for all management station. Disable all applications that uses clear-text authentication and use SSH or SSL for connectivity.
- Use LUN masking to prevent the hosts reading the drives they are not authorized to read.
- Use device encryption to prevent accidental configuration error from rendering data to wrong host.
- Use zoning to alleviate the threats caused by weak communication (IPv4/ Fibre Channel) medium. Soft zoning allows WWN spoofing. Wherever possible (small installations or segmented for higher security), use hard zoning.
- To avoid WWN or IP spoofing use port binding [17] feature. This binds a specific port to a HBA/WWN. Use key based authentication between the host (HBA) and the switches (ports).
- Use virtualization of storage network using features like Virtual SAN [16] in fibre (VSAN) and Virtual LAN (VLAN) in Ethernet based network.
- Apply authentication procedures especially for the switches in fabric. The new implementation of Cisco and Brocade switches support Fibre Channel-Security

Protocol (FC-SP). Configure switches to use PKI and authenticate against a RADIUS or TACACS. This prevents any un-authorized client, server or the switch to join the fabric.
- Separate the storage network from the rest of the network infrastructure.

6 Present and future standards that define storage security

The following are some of the major working groups which are involved in arriving at various standards for storage networks.

- American National Standard Institute (ANSI, http://www.ansi.org): governing body for the working group T11. The list of projects T11 working group and the projected date is listed under the following link http://www.t11.org/index.htm .
- IEEE Storage Systems Standards Committee (IEEE-SSSC, http://www.ieee-sssc.org): New working group created by IEEE (Institute Of Electrical and Electronics Engineers). The primary focus of this group is to work on storage. The other group which work on storage security is Security In Storage Working Group (SISWG, http://siswg.org)
- Internet Engineering Task Force (IETF, http://www.ietf.org): Most of the TCP/IP and Internet architecture based standards were derived by this organization. This organization also governs the working group developing standards for IP Storage (http://www.ietf.org/html.charters/ips-charter.html).
- Fibre Channel Industry Association (FCIA, http://www.fibrechannel.org): This organization established SANMark ™ (http://www.sanmark.org/) qualified program to provide a baseline in quality of fibre channel products.
- Storage Networking Industry Association (SNIA http://www.snia.org): Works towards establishing new standards in storage networking. Have multiple work groups working in the following area backup, fibre channel, IP storage, NAS, Object-based storage devices (OSD), policy, security and Storage Media Library.
- Storage Management Initiative (SMI-S http://www.snia.org/smi/home): The primarily provides the following a common interoperable management interface, unified model to control the LUN and Zones for SAN infrastructure, automated discovery and a Common Information Model (CIM) with Distributed Management Task Force (DMTF).
- Storage Security Industry Forum (SSIF http://www.snia.org/ssif): Consortium to increase the availability and perform research with the vendor in increasing the storage security awareness, developing storage security products and solutions.

7 What vendors have in the market to secure the storage network?

Neoscale [18]: Offers family of wire-speed, policy based storage security appliance. The product CryptoStor ™ has two flavors 1) for fabric and 2) for tapes. Offers support for both Fibre channel and SCSI. The product is policy based and encrypts data when it is at transport. Uses 3DES/AES encryption and 2-factor smart card authenticated access and key export. Allows management through SSL/SSH. There is no solution available for NAS. CryptoStor ™ Tape is the new product NeoScale introduced for tape devices. This device on the fly compresses, digitally signs and encrypts the that is written and read from the tape devices. These products are certified with McData, Brocade, QLogic, ADIC, ATK, Quantum and Overland.

Decru [19]: Has partnership with industries major vendors including McData, Brocade, Veritas, HP, SUN and many more. Offers support for SAN, NAS, DAS and tape systems. The product provides support for two-factor authentication to control access to management application. The company is certified with FIPS 140-2 level 3. The encryption AES-256, SHA-1 and SHA-256 are certified by NIST for the Datafort product. The product supports LDAP, NIS and other directory based authentication. The product also offers life-time key management and protection. Data disposal is a snap by deleting the CryptoShred ™.

Vormetric: CoreGaurd consist two components, 1) software that is installed on hosts that needs to be protected 2) appliance that connects to these protected hosts via dedication connection. Each of this appliance supports multiple protected hosts. Uses 3DES and AES for data encryption. Only encrypts application data and does not encrypt metadata using proprietary technology called MetaClear™ .

McData [24]: SANTegrity suite of security products from McData offers a wide range of security solutions we have discussed in this paper. They provide solution for Zone management, role-based management and centralized management for fabric management. The software offers multiple levels of binding zone level, port level and technology. No storage vendor partnership. This is placed as more data and application security. The new version supports host intrusion.

Brocade [25]: Unlike McData, Brocade is new to the market for large enterprise fabric installation. The Secure Fabric OS offers wide range of security features such Public key based authentication between switches, user 1024 bit encryption for private key storage. Access control list for both management level and the host connectivity through WWN.

8 Conclusion

Securing storage is an essential element in protecting the intellectual property. In order to achieve this objective each organization needs a well defined security policy covering various aspects of storage. As we had seen in this discussion, threats exist in DAS, NAS and SAN setup. The existing storage product ideas, the emerging standards, vendor partnership and the layered approach to the storage model would provide better solutions to protect the storage. Vendor should follow the layer approach to tailor the products to better address the threats in each level. The market research [4] shows that the vendor concentration is going to on "data-at-rest". One way of protecting the data-at-rest is to encrypt the data on the drive.

Storage security is very much relative to the value and requirement of what business needs. As long as there is data with a value attached to it, there is always going to be vulnerabilities and threats in systems protecting them. What can we do to mitigate these threats?

- Be aware of company policy about the data retention. The policies main goal should be arriving at data identification. Clear identification of data gives a structured approach of recovering if there is an incident. Procedures must be documented clearly, tested and also updated from learned lessons.
- Wherever required use physical security, perimeter security, storage device configuration, access to management station and even physically isolate the storage systems.
- Once the data identified use extreme caution handling the sensitive data. If it is required encrypt data on drives. Use port mapping, LUN mapping and hard zoning.
- Have the procedures ready for business continuity. This will get the organization in better shape in terms of security implementation, updating the policies and gives better understanding on how we protect the data at remote data center.

This paper explains the application of security principles to different layers of storage model. This would also help the IT professionals to better understand the components of storage and identify the right solution for security they are looking for.

References

[1] Storage Networking Industry Association, “Shared Storage Model - A framework for describing the storage architectures” URL: http://www.snia.org/tech_activities/shared_storage_model/SNIA-SSM-text-2003-04-13.pdf

[2] Storage Networking Industry Association, “A Dictionary of Storage Networking Terminology” URL: http://www.snia.org/education/dictionary/s/#storage_area_network

[3] Storage Networking Industry Association, “Minimum Security Requirement and Best Practices for IP Management” URL: http://www.snia.org/apps/group_public/download.php/5525/SSIF_SANS_Sec.v1.1.pdf

[4] Yankee Research Group, “The Emerging Storage Security Challenge” URL: http://www.neoscale.com/English/Collaterals/Documents/EmergingChallenge_YankeeGroup_20030901.pdf

[5] Himanshu Dwivedi and Andy Hubbard, “Securing Storage Networks”, URL: http://www.atstake.com/research/reports/acrobat/atstake_storage_networks.pdf

[6] Hitachi Data Systems, “Towards Securing Information End-to-End-Network Storage Security Update and Best Practices“ URL: http://www.hds.com/pdf/wp_129_security.pdf

[7] Jingmin He and Min Wang, “Cryptography and Relational Database Management” URL: http://www.cs.duke.edu/~minw/Publication/ideas01.pdf

[8] Blake Wiedman, “Database security (Common-sense principles)” URL: http://www.governmentsecurity.org/articles/DatabaseSecurityCommon-sensePrinciples.php

[9] Dan Rahmel, “Database security”, URL: http://www.governmentsecurity.org/articles/DatabaseSecurityPart1.php

[10] Paul Leach and Dan Perry, Microsoft Internet Developer, “CIFS: A Common Internet File System”, URL: http://www.microsoft.com/mind/1196/cifs.asp

[11] Computer Security Resource Center, “Network File System (NFS) Threats”, URL: http://csrc.nist.gov/publications/nistpubs/800-7/node132.html#SECTION08128100000000000000

[12] RSA Security, “RSA SecureID Hardware Tokens”, URL: http://www.rsasecurity.com/products/securid/hardware_token.html

[13] Carnegie Mellon Software Engineering Institute, CERT® Incident Response Center. “Tech Tips”, URL: http://www.cert.org/tech_tips/

[14] Chet Duncan, “Using Security Template and Group Policy to Secure Windows Server”, URL: http://www.sans.org/rr/catindex.php?cat_id=67

[15] Veritas, “Veritas NetBackup ™ Encryption Option”, URL: http://www.veritas.com/Products/van?c=option&refId=195

[16] Cisco, “Using VSAN and Zoning with the CISCO MDS 9000 Switches”, URL: http://www.cisco.com/en/US/products/hw/ps4159/ps4358/products_white_paper09186a0080114c21.shtml

[17] Cisco, “Configuring Port Security”, URL: http://www.cisco.com/en/US/products/hw/ps4159/ps4358/products_configuration_guide_chapter09186a00801dd8f8.html

[18] NeoScale, “CryptoStor™ FC”, URL: http://www.neoscale.com/English/Collaterals/Documents/CryptoStorFC_datasheet.pdf

[19] Decru, “DECRU DataFort ™,”FC-Series Storage Security Appliance” URL: http://www.decru.com/products/dsFCseries.htm

[20] United States Department of Health and Human Services, “Summary of HIPAA Privacy Rule”, URL: http://www.hhs.gov/ocr/privacysummary.pdf

[21] Federal Trade Commission, “In Brief: The Financial Privacy Requirement of the Gramm-Leach-Bliley Act”, URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

[22] One Hundred Seven Congress of America, “Sarbanes-Oxley Act of 2002”, USR: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf

[23] California Senate, “California State Law SB1386”, URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[24] McData SANTegrity ™, “SANTegrity security suite software”, URL: http://www.mcdata.com/products/network/security/santegrity.html

[25] Brocade - Secure Fabric OS, “A comprehensive security Architecture for SAN Fabrics”, URL: http://www.brocade.com/products/pdf/data_sheets/SecureFabOS_DS_0226.pdf

[26] Vormetric, “CoreGaurd - Data Security System”, URL: http://www.vormetric.com/solutions/