Global Information Assurance Certification Paper

Network Backup Security:
Francisco Londono
March 5, 2002; GSEC v1.3

Introduction

This paper analyzes the security issues involved in the backup of information. It takes a practical overview of two protocols used for this purpose, a Fibre Channel Storage Area Network and the Network Attached Storage backup protocol - NDMP.
We will review the basic terminology for each and analyze what are the issues to keep in mind from a security perspective while using these technologies. We will first start discussing fiber channel in the context of data backup only. Then we will explain the Network Management Protocol and it authentication mechanisms.

Terminology

Before any further explanation of the Fibre Channel Protocol, let us review some basic terminology. (The terminology provided by the Storage Network Industry Association is as follows and can be found in [1]):

SAN
Context [Fibre Channel] [Network]

1. Acronym for Storage Area Network.
2. Acronym for Server Area Network, which connects one or more servers.

Fibre Channel
Context [Fibre Channel]
A set of standards for a serial I/O bus capable of transferring data between two ports at up to 100 MBytes/second, with standards proposals to go to higher speeds. Fibre Channel supports point to point, arbitrated loop and switched topologies

Fabric
Context [Fibre Channel]
A Fibre Channel switch or two or more Fibre Channel switches interconnected in such a way that data can be physically transmitted between any two N_Ports on any of the switches.

With the ever increase of disk space and the need for more data storage IT organizations have a variety of hardware choices to store this information on. With system capacity in the terabytes range the IT administrators have to scale accordingly their backup implementations. Doing backups over the LAN proved to decrease performance of the network. Fiber Channel provides a method by which storage Administrators can do system wide backups over dedicated high-speed fiber optic connections without incurring in the expensive performance overhead that they would incur if they used the local area network [2]. Below is a diagram that shows the basic components of a SAN and the corresponding potential vulnerable access points:

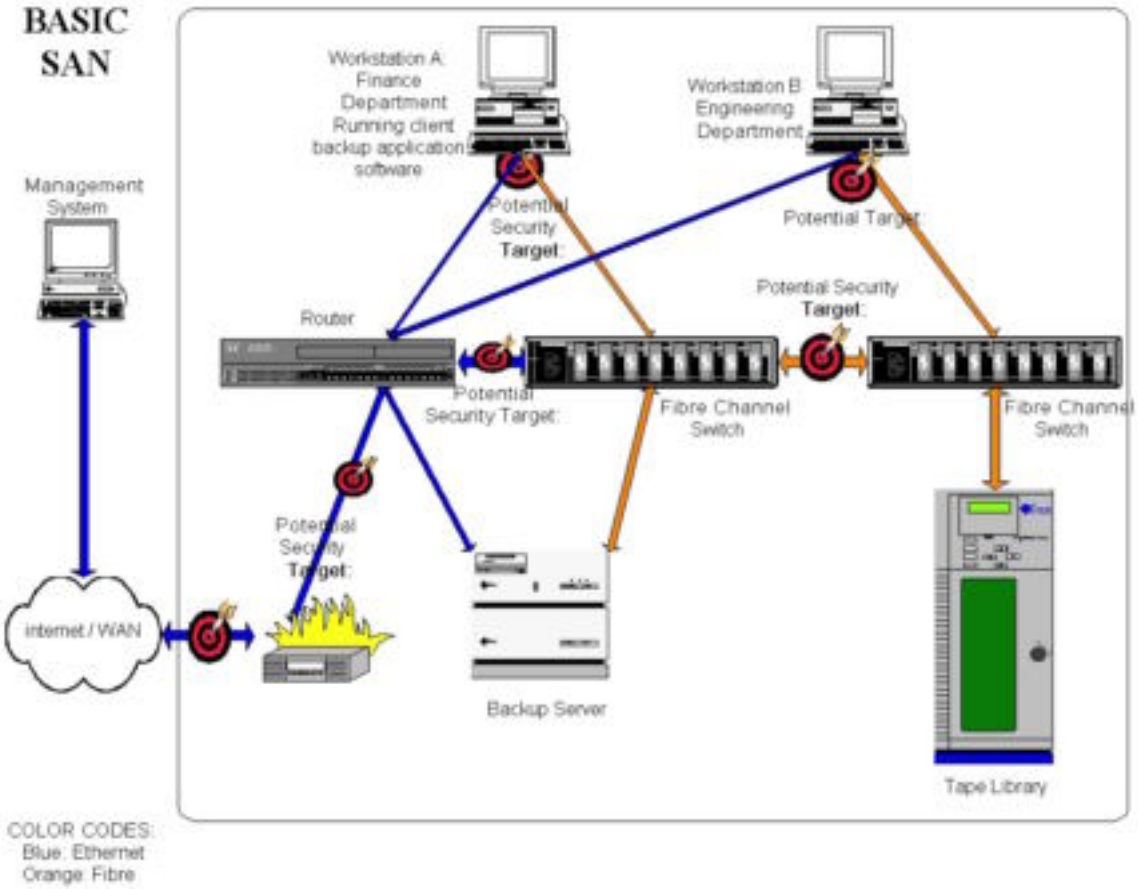

Figure 1

SAN Overview

In order to look at the security aspects we will analyze the elements of a SAN from Figure 1. Some minimum hardware requirements for a SAN would be:

- Host Bus Adapter (physical Fibre Channel card in the server)
- Network Interface Card (or a port dedicated for backup)
- Fiber Optic cables
- Fabric Switch
- Network Router
- Tape Library
- Backup Application Software
- Operating System

Out of the previous list, data needs to be secured at various levels, especially at the Fabric switch, networks router and client operating system.

Fabric Switch
The fabric switch usually has front panel configuration capabilities. Physical security or access to the switch must be enforced. Some Fibre Channel switch vendors have a choice of preloading the switches with what they call a "secure" fabric operating system. Unfortunately, this is usually an item that must be requested before buying the switch, as they generally tend to come with their default OS. For switch management purposes vendors usually include the following services:

- telnet : no encryption of data between Management console and switch
- SNMP: follows the same vulnerabilities as other SNMP devices
- web server access through a 10/100 Ethernet port.

One of the inherent security methods used in the switches is ZONING, defined as [3]:
"A feature in fabric switches or hubs that allows segmentation of a node by physical port, name, or address."

The switch operating system has to address vulnerabilities by supporting authentication methods at the following access points:

- User Access to the management interface
- Management console access to the fabric
- Server access to the fabric
- Switch access to an existing fabric (switch to switch)

To prevent the above-mentioned vulnerabilities the fabric switch needs to have the following capabilities:

- Multilevel passwords
- Access Control Lists
- Centralization of "trusted" switch for configuration purposes
- Prevention of World Wide Name spoofing
  (A World Wide Name is a unique identifier assigned to each manufacturer by IEEE)

Network Switch:
The network switch provides remote configuration for the fabric switches in addition to Client-server connectivity. The standard security measures must be taken at this level including password authentication, ACL, VLAN, subnets, etc. For a more detail overview on router security look at [4].
Even though the data is going to be sent over the Fibre Channel link most backup software vendors require the use of a network interface card for passing metadata and establishing Inter-process Network Communications for the backup application software. This creates a client and a server network link in which both systems can potentially compromise each other.

Backup Application Software
The backup management software can be considered as one of the biggest security risks in a secure network environment. Once the data leaves a secure server the information is flowing through the networks without any protection. While selecting commercial backup application software the system administrator has to keep in mind security features such as [5]:

1. **Authentication**:
What type is the application using?
For Veritas NetBackup for example, the standard is a one-time password (challenge/response) mechanism. Based on the US Navy OPIE protocol.

2. **Authorization**:
   - Protection of data from unauthorized access through the use of secure client hosts to restrict client-server communications, and administrator imposed restrictions on restore operations.
   - Prohibit user from viewing or restoring other people's files (from the client side). The software should allow viewing of data that has been backup up only from that particular client. In case of different user needs, only the administrator can override those restrictions. It is recommended for the administrator not to relax file access restrictions by giving the clients the capability to access the archived images created on other files.
   - At the backup server level, creation of appropriate user privileges so that the backup is not run as root is recommended.

3. **Encryption**:
Does the backup software have this capability?
The backup application software must provide at least a mechanism to perform data encryption on the client, transfer it through the network encrypted and store on tape in the same format. For restores, the data must be read from media encrypted and sent to the client before decrypting it.

4. **Backup Software Port configuration**:
The storage administrator has to know how the backup application software communicates between computer systems. NetBackup for example, has a combination of registered and dynamically allocated ports. Registered ports are assigned to specific services such as:

(daemon name) (reserved port number)
   - bpcd: 13782
   - bpdbm: 13721
   - bprd: 13720
   - vmd: 13701
   - vopied: 13783

Dynamically allocated ports are assigned as needed from ranges that are configurable. In the cases were there is a firewall between the client and the server the software needs to be

configured so that clients that are outside of the internal network can indeed connect through a firewall. The network administrator must know what other features to enable in the software like whether the application will select a port number at random from the allowed range or if it will start at the top of the port range and then use the first available port number.

The basic recommendation is to limit the external connections to the server in the private network by allowing the backup application to accept reserved connections on a subset port range. (The default is any port from 512 to 1023). The same applies to connections out of the private network so the server can select only a subset of ports in which to communicate to the clients. The main factor to consider when selecting the minimum port ranges is the number of clients to backup.

Fibre Channel Protocol Analyzer:

The tools required to look at the port traffic on the switch requires the use of specialized hardware, which is currently expensive. This can only be done on site and by physically connecting to the fabric port. Tools from companies like Finisar Systems provide this capability at a premium.

Host Bus Adapter:

It is important for the storage administrator to keep a tracking mechanism or logs of which Host Bust Adapter- World Wide Names are installed on each individual server. This can then be verified at the switch configuration interface. For organizations with multiple nodes this can be an expensive proposition and the appropriate analysis needs to be conducted for acceptable risks.

In summary, the question that the storage network administrator and network security specialists have to look at is [6]:

Where to secure data storage?
Secure data storage at all access points within the network:

1) Data network
2) Management Interfaces
3) User and application access
4) Application software
5) Operating System

NDMP: Security Overview

What is NDMP?

Is an acronym for Network Data Management Protocol and is an evolving standard for enterprise wide backup of network-attached storage.
The NDMP protocol defines the communication between a client (or Data Management Application) and one or multiple ndmp servers.

The following diagram illustrates a simple NDMP configuration:

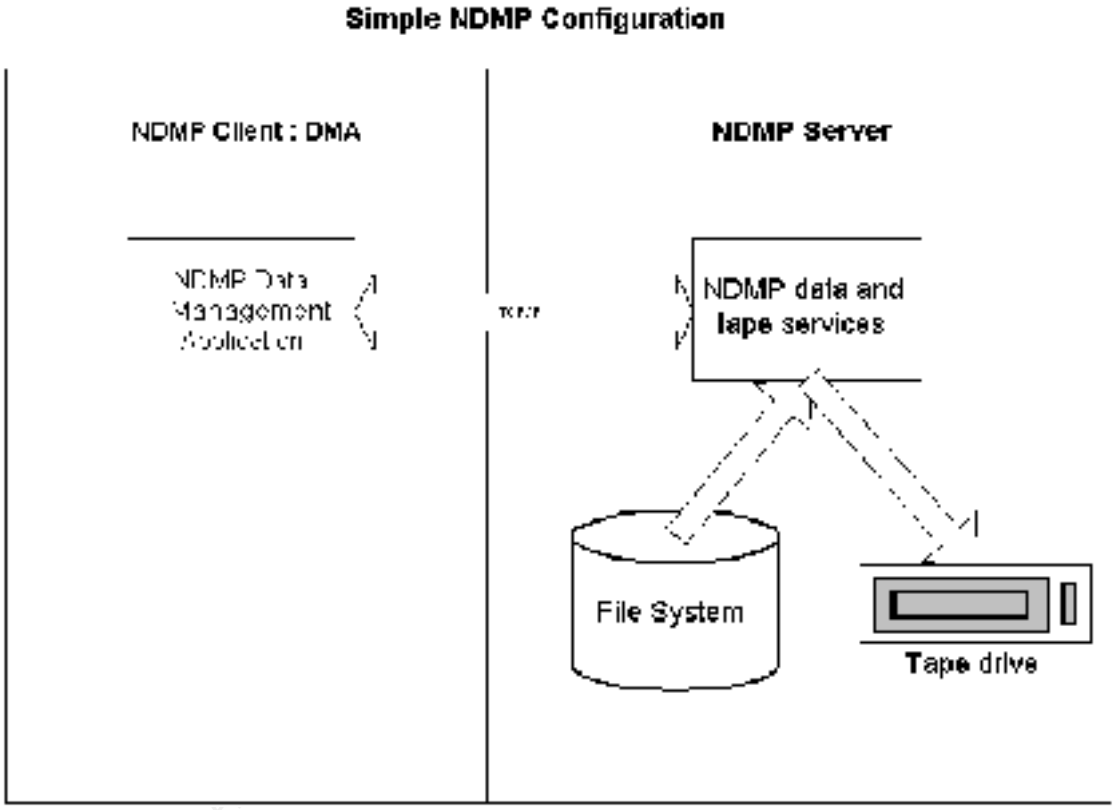

Figure 2

Common backup architecture components:

1) The file server (running a ndmp server daemon). Commercial vendors like Network Appliance and Auspex Systems file servers provide this capability.
2) The backup device (tape library or jukebox)
3) Third party backup software (DMA). Commercial vendor applications include Legato and Veritas to name a few.

The NDMP client is running in a workstation were the backup software application (DMA) initiates connections to a NDMP server.

Connection:
The Data Management Application initiates a TCP/IP connection on Port 10,000. This is the default port and the standard calls for configurable port assignment for both NDMP client and server in case of port conflicts.

Authentication:

Using the NDMP_CONNECT_CLIENT_AUTH request message the Data Management Application is authenticated. Only then it will be allowed to use most of the other NDMP request messages.

The NDMP standard calls for supporting at least one of the following authentication methods:

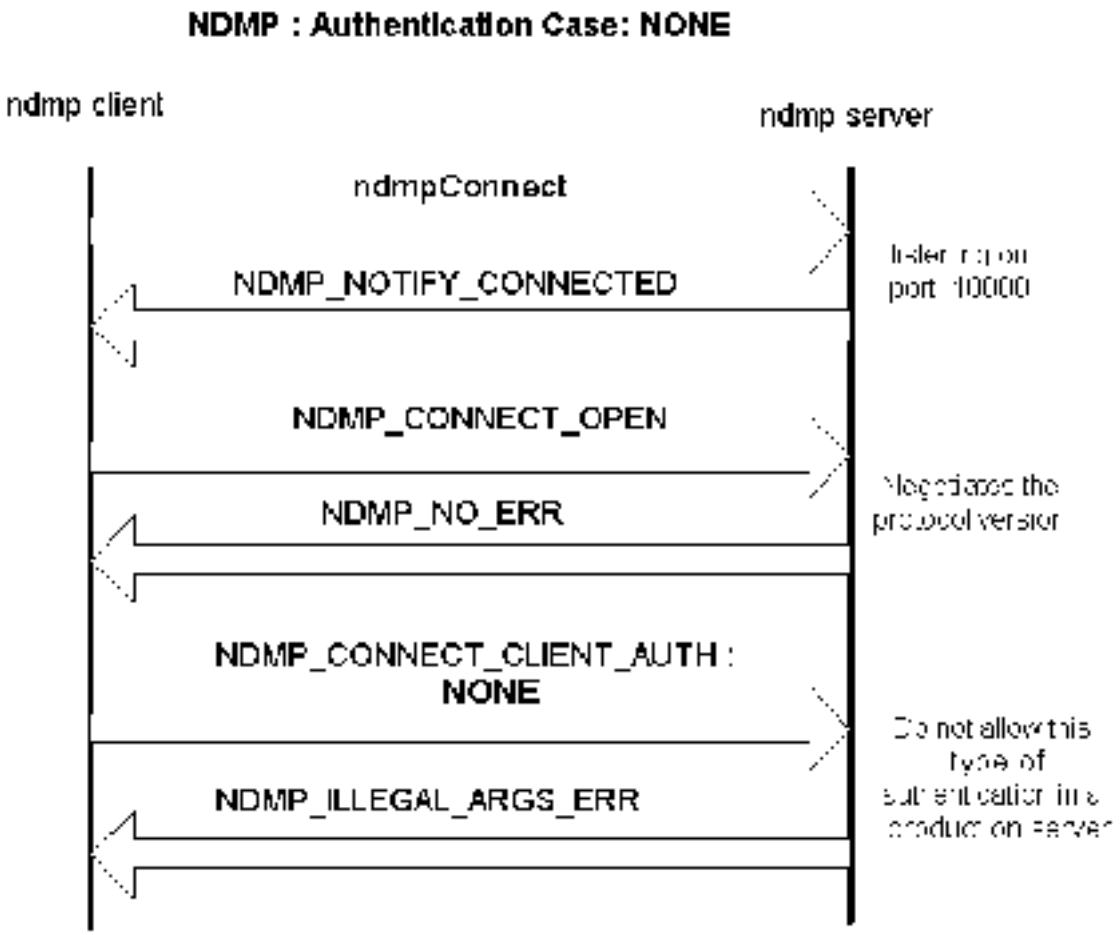

Figure 3

Check with your file server documentation to make sure this type of authentication is not enabled on a production server.

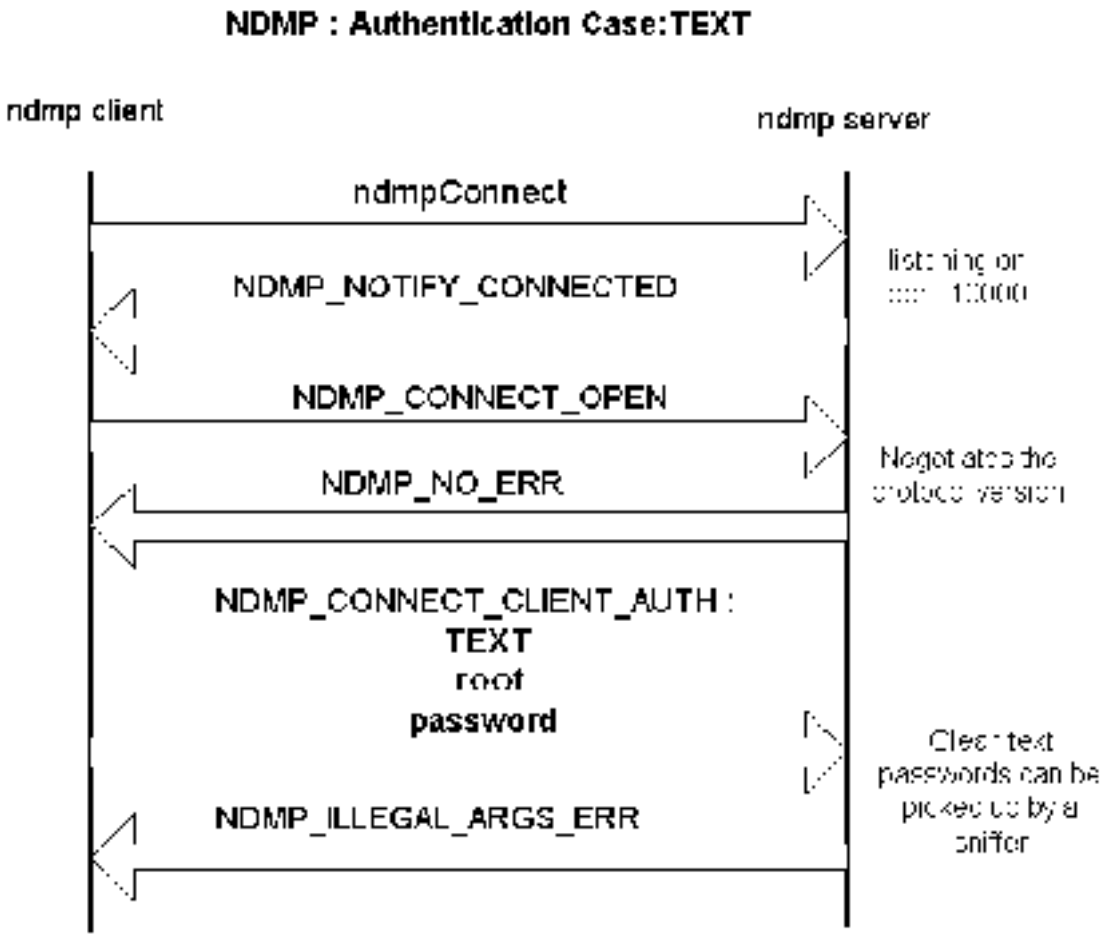

Figure 4

The ndmp client connects to the server on port 10000. The server notifies the client that it accepted the connection by way of a NDMP_NOTIFY_CONNECTED reply message. There is a message to establish which version of the protocol each daemon is running. To date there are multiple versions of the protocol including version 1, version 2, version 3, version 4 and version 5 in the pipeline. The protocol calls for the applications to start with their latest version of the protocol and decrement the number each time if they are not at the same level. This guarantees that the least common denominator that any given application will 'talk' to is protocol version 1. The client will then send the appropriate authentication message as TEXT with two parameters. Those parameters are user-id and password. The user-id unfortunately has to be root. The standard does not allow including other type of user-ids. It would be appropriate if the protocol was less restrictive and allow another type of user-id. The password is not encrypted and is sent as clear text. Again, this is not a secure method of authentication.

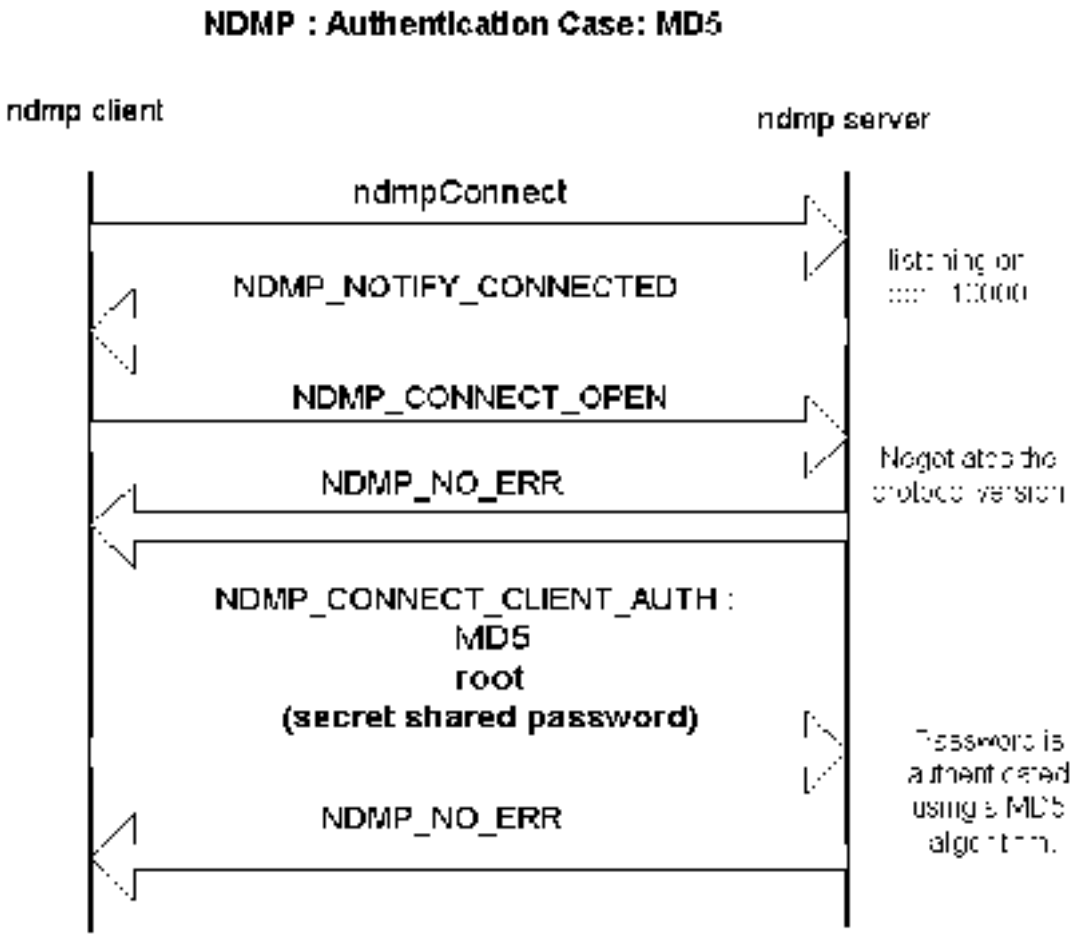

Figure 5

The message exchange is similar to the Figure xxx, but now the authentication type is MD5 (Message Digest 5). The user-id is still root, no other type of user-id are allowed in the protocol but this time the password is encrypted at the client side and decrypted at the server side. During the exchange of communications the password can still be picked up by a network sniffer but at least there will be more work to do on the hacker side to steal the root password of the systems. This is the most secure out of the three authentication mechanism used in NDMP so it should be the default method that a production server ought to be running.

The ndmp.org web site has a software development kit which illustrates how the protocol should behave. You can run this on a single solaris or linux system and look at the transactions with tcpdump. Below is an example of a simple authentication handshake with three basic authentication commands from client to server:

a) Connect Open (ndmp version 3)
b) Connect_Client_Auth NONE
c) Connect Close

(**Begin establish connection**)
13:36:20.078333 localhost.localdomain.**1038** > localhost.localdomain.**10000: S** 683554265:683554265(0) win 31072 <mss 3884,sackOK,timestamp 2370905 0,nop,wscale 0> (DF)

13:36:20.078409 localhost.localdomain.**10000** > localhost.localdomain.**1038: S** 672918606:672918606(0) **ack** 683554266 win 31072 <mss 3884,sackOK,timestamp 2370905 2370905,nop,wscale 0> (DF)

13:36:20.078445 localhost.localdomain.**1038** > localhost.localdomain.**10000**: **. ack** 1 win 31072 <nop,nop,timestamp 2370905 2370905> (DF)

(End establish connection)
13:36:20.080409 localhost.localdomain.10000 > localhost.localdomain.1038: P 1:41(40) ack 1 win 31072 <nop,nop,timestamp 2370905 2370905> (DF)

13:36:20.080451 localhost.localdomain.1038 > localhost.localdomain.10000: . ack 41 win 31032 <nop,nop,timestamp 2370905 2370905> (DF)

13:36:20.211034 localhost.localdomain.1038 > localhost.localdomain.10000: P 1:33(32) ack 41 win 31072 <nop,nop,timestamp 2370918 2370905> (DF)

13:36:20.211093 localhost.localdomain.10000 > localhost.localdomain.1038: . ack 33 win 31040 <nop,nop,timestamp 2370918 2370918> (DF)

13:36:20.211439 localhost.localdomain.10000 > localhost.localdomain.1038: P 41:73(32) ack 33 win31072 <nop,nop,timestamp 2370918 2370918> (DF)

13:36:20.224683 localhost.localdomain.1038 > localhost.localdomain.10000: . ack 73 win 31072 <nop,nop,timestamp 2370920 2370918> (DF)

13:36:20.229285 localhost.localdomain.1038 >localhost.localdomain.10000: P 33:65(32) ack 73 win 31072 <nop,nop,timestamp 2370920 2370918> (DF)

13:36:20.229500 localhost.localdomain.10000 > localhost.localdomain.1038: P 73:105(32) ack 65 win 31072 <nop,nop,timestamp 2370920 2370920> (DF)

13:36:20.244681 localhost.localdomain.1038 > localhost.localdomain.10000: . ack 105 win 31072 <nop,nop,timestamp 2370922 2370920> (DF)

13:36:20.275102 localhost.localdomain.1038 > localhost.localdomain.10000: P 65:93(28) ack 105 win 31072 <nop,nop,timestamp 2370925 2370920> (DF)

(Begin TCP connection close)
13:36:20.275309 localhost.localdomain.**10000** > localhost.localdomain.**1038: F** 105:105(0) ack 93 win 31072 <nop,nop,timestamp 2370925 2370925> (DF)

13:36:20.275349 localhost.localdomain.**1038** >localhost.localdomain.**10000**: **. ack** 106 win 31072 <nop,nop,timestamp 2370925 2370925> (DF)

13:36:20.276763 localhost.localdomain.**1038** >localhost.localdomain.**10000: F** 93:93(0) **ack** 106 win 31072 <nop,nop,timestamp 2370925 2370925> (DF)

13:36:20.276849 localhost.localdomain.**10000** > localhost.localdomain.**1038**: . **ack** 94 win 31072 <nop,nop,timestamp 2370925 2370925> (DF)

For a real case scenario, let's look at how a network attached storage company implements the NDMP protocol.

Before we discuss the details of the protocol we need to show an overview of the hardware and software configuration for these file servers. For this example we will look at the Auspex Systems NS2000 Network Attached Storage Server [7]:

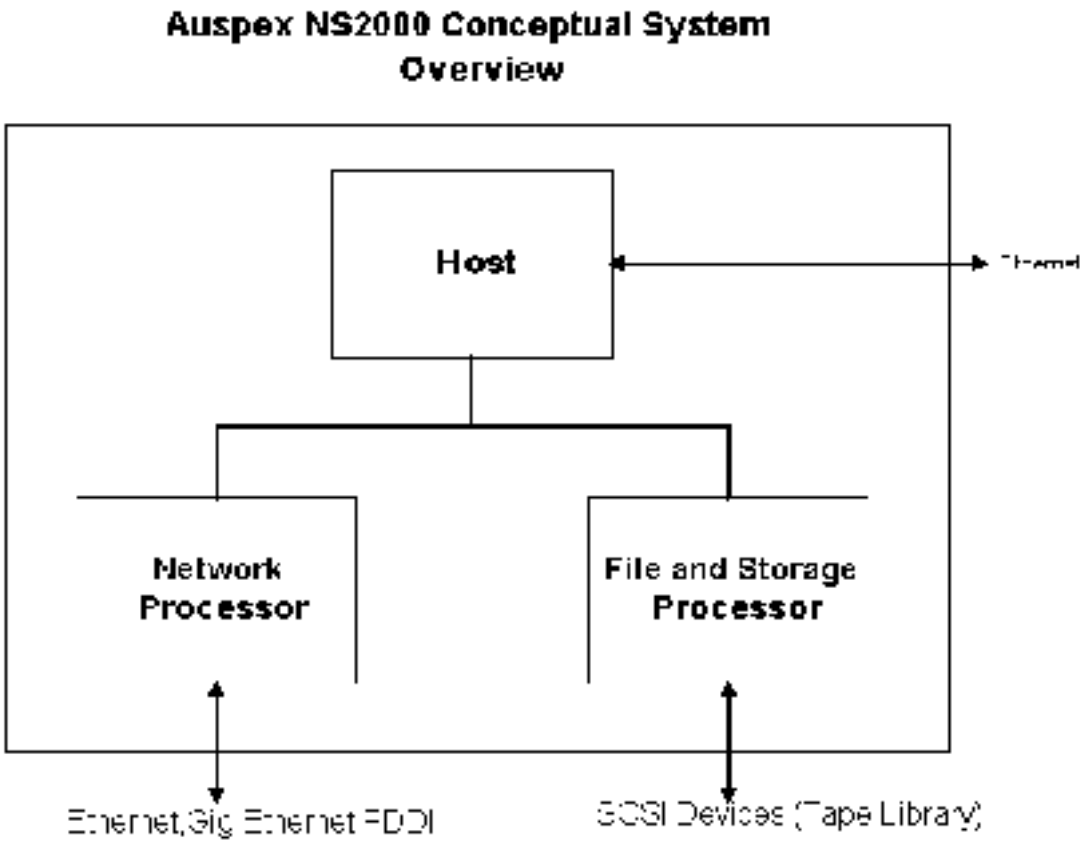

Figure 6

2.1 **Host**

The host processor is a SPARC system running Solaris 2.6 (as of 2000).
It provides most of the Unix services and as such it has most of the security vulnerabilities that a regular Unix system would. The host board main purpose is to provide:

- System startup and shutdown
- Software licensing
- SNMP
- **NDMP** (running as **ax_ndmpd**)
- Web based server management tool (http://servername:8081)
- System error and report logging

2.2 **Network Processor**

The network protocol stack is implemented on the protocol processing CPU.
The network processor provides:

a) Transport layer protocols UDP and TCP.
b) IP routing, ICMP and ARP.
c) Network applications: NFS, FTP

Packets which the protocol processing CPU is not design to handle will be forwarded to the Host.

2.3 **File and Storage Processor**

It implements the standard Unix BSD 4.3 FFFS. The file storage processor provides a file-oriented view of storage. It also implements hierarchical directory support. It is out of the scope of this document to discuss the file system security mechanisms.

NS2000 NDMP Server

The NDMP server is implemented as a daemon process (ax_ndmpd) running on the Host Processor. When a NDMP client requests a connection to the Host, a thread is spawned off the NDMP server. Upon authentication, that threads then interfaces with the appropriate transfer engines (file or block)

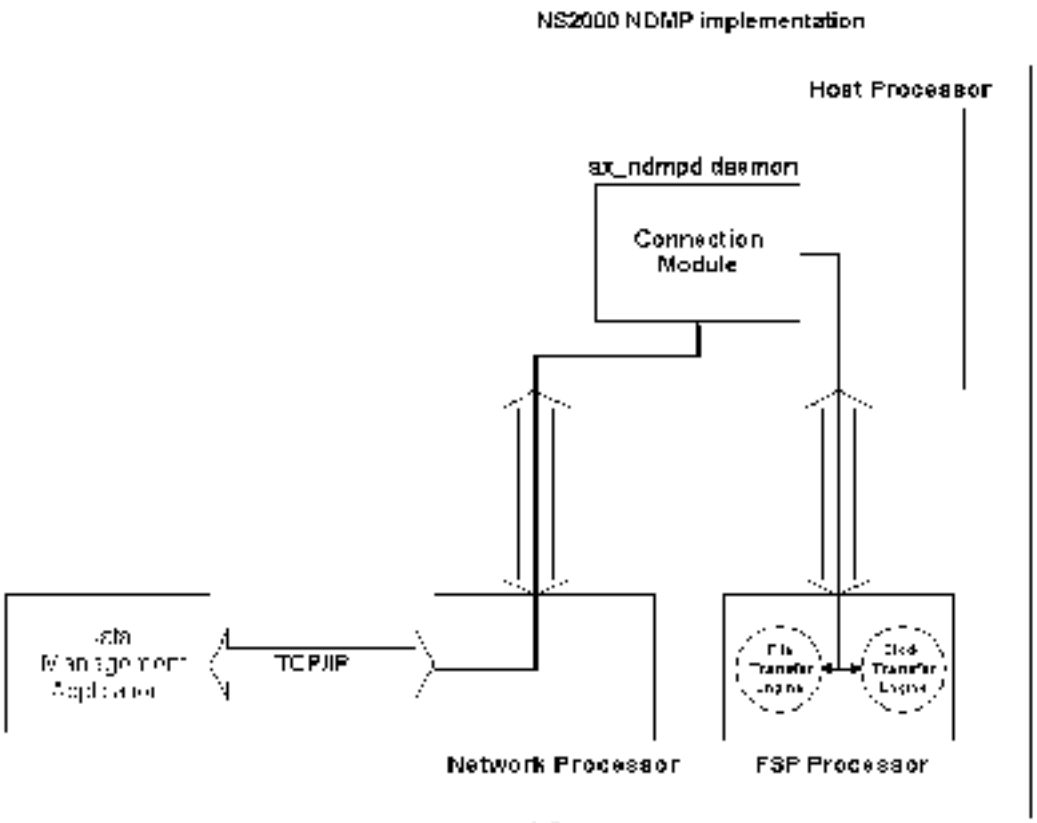

Figure 7

The Data Management Application will initiate the request to the server. Special considerations need to be taken into account if there is a firewall between the DMA and the file server. If the firewall is configured in such a way that it only allows for outbound connections then the initial connection must be established from the file server that has the tape services.
If the firewall administrator opens the firewall for inbound connections, the storage administrator must define the range of TCP ports to use, in case the default port assignment is not used.
Once the connection is established between client and server the NDMP protocol does not define any privileges to be set. The data will be exchanged between the two applications without restrictions, including file history.

Prior to initiating an authentication request, the NDMP server can be probed via a message to provide information about the server's vendor name and revision information. Make sure the NDMP server is implemented in such a way that this information is not given before a valid client authentication. This can be used as a reconnaissance method to plan an attack on the server.

There are other interfaces in the protocol, which allow for access to SCSI media changer devices at a low level. Special considerations need to be in place for the NDMP server not to allow access to disk SCSI devices that would bypass file system security. [8]

Conclusion

As we have seen there are a variety of issues to consider when implementing a secure backup strategy. The primary consideration for the IT team is to gain an understanding of the protocols, their strengths and weaknesses with respect to security. With this information then we can do a detailed risk analysis and implement security policies accordingly.

References

[1] Storage Networking Industry Association
(Products and Services→Resource Center→Dictionary)
URL http://www.snia.org/

[2] White paper
URL: http://data.fibrechannel-europe.com/technology/whitepapers/wp_030800.html

[3] University of Minnesota
URL: http://gfs.lcse.umn.edu/fc/fc_san.html

[4] Cisco Systems
URL: http://www.cisco.com/warp/public/707/21.html

[5] NetBackup Global Data Manger 3.4 System Administrator Guide
URL: http://seer.support.veritas.com/docs/233837.htm

[6] Hitachi Data Systems
URL: http://ieee-tcia.org/sisw2001/HDS_IEEE_sisw_12_4_2001.pdf

[7] Auspex Systems NS2000 System Administration

[8] NDMP Organization
URL: www.ndmp.org

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event