LAHDEN AMMATTIKORKEAKOULU
*Lahti University of Applied Sciences*

# HACKING A FIBRE CHANNEL NETWORK

Sniffing valuable data, undetected

LAHTI UNIVERSITY OF APPLIED SCIENCES
Information Technology
Software engineering
Bachelor's Thesis
Autumn 2013
Harri Hänninen

Lahti University of Applied Sciences
Degree Programme in Information Technology

HÄNNINEN, HARRI:

Hacking fibre channel network
Sniffing valuable data, undetected

Bachelor's Thesis in software engineering, 38 pages

Autumn 2013

ABSTRACT

---

This thesis provides a general introduction to storage area networking, the Fibre Channel protocol and SCSI, as well as why enterprises use SAN attached storage array subsystems today. The focus is on the security of storage area networking.

The objective of the thesis was to study and test in practice the possibility to eavesdrop a Fibre Channel Storage Area Network. The tests were conducted by sniffering the fiber optic cables by breaking the optical link and placing an optical splitter in between to establish connectivity for the sniffering device to capture data frames from the link. Also, there were tests to actually sniffer data frames without breaking the optical link, by using clip-on couplers, which are available from the internet for less than USD 1000. Also stealing data was tested by WWN spoofing.

Another topic of study and testing in the thesis was Brocade Encryption Switch, which is a Fibre Channel switch with encryption engines to provide data-at-rest encryption. The management of data encryption key was also studied. It was tested whether data is actually encrypted after being redirected through the encryption engine and whether the encrypted logical disk device is really ciphertext and includes the metadata that is documented by Brocade Encryption Switch documentation.

The thesis proved that it is possible for an attacker to sniffer data payload from a Fibre Channel link and for example steal a hashed root password for the linux server booting from SAN. Sniffering without breaking the circuit was not successful in this thesis, but is definitely possible. Also stealing data with WWN spoofing is possible, but it seems to require good luck or other attack vectors to force original WWN to logout from the SAN fabric.

Key words: Fibre Channel, SAN, BES, encryption, hacking, storage

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

HÄNNINEN, HARRI:

Fibre Channel verkon hakkerointi arvokkaan datan varastaminen huomaamatta

Ohjelmistotekniikan opinnäytetyö, 38 sivua

Syksy 2013

TIIVISTELMÄ

---

Opinnäytetyö antaa yleiskuvauksen tallennusverkoista, FibreChannel- ja SCSI-protokollista sekä siitä miksi suuret ja keskisuuret yritykset käyttävät SAN-tallennusjärjestelmiä tänä päivänä.

Tavoitteena oli tutkia ja testata, kuinka helppoa on varastaa dataa salakuuntelemalla FibreChannel-verkkoa katkaisemalla optinen kuitulinkki ja jakaa valosignaali prismalla laitteelle, jolla optista linkkiä voidaan kuunnella ja analysoida. Lisäksi testattiin käytännössä varastaa data samasta kuitulinkistä katkaisematta linkkiä missään vaiheessa käyttäen kaapelin vaipan päälle naksautettavia signaalin jakajia, joita voi löytää internetistä alle USD 1000. Lopuksi testattiin vielä datan varastamista väärentämällä palvelintietokoneen kuitukortin WWN-osoite.

Opinnäytetyössä tutustuttiin Brocade Encryption Switch Fibre Channel-kytkimeen ja testattiin sitä. Kytkin pystyy kryptaamaan sen läpi kulkevan liikenteen levyjärjestelmään. Tämän lisäksi tutkitaan kryptauksen kanssa käytettävää salausavainten hallintajärjestelmää. Opinnäytetyön lopussa testattiin, että data on todella salattua sen jälkeen kun Fibre Channel-kehykset on reititetty salausmoottorin lävitse levyjärjestelmään, sekä tarkasteltiin salatun levyn metadataosiota ja verrattiin sitä Brocaden dokumentaatioon aiheesta.

Opinnäytetyössä todistetaan, että hyökkääjän on mahdollista tallentaa data FibreChannel -linkistä ja esimerkiksi varastaa tätä kautta tiivistetty pääkäyttäjän salasana Linux-palvelimelle, jonka käyttöjärjestelmä on SAN-verkossa olevalla levyllä. Datan varastamisessa ilman että kuitulinkkiä katkaistaan ei onnistuttu, mutta on selvää, että se on mahdollista. Lisäksi todetaan, että datan varastaminen WWN-osoitetta väärentämällä on mahdollista, mutta ilmeisesti tarvitaan hyvää onnea tai muiden hyökkäysvektoreiden käyttöä, jotta alkuperäisen WWN-osoitteen käyttäjän saa poistettua SAN-verkon osasta.

Asiasanat: Fibre Channel, SAN, BES, kryptaus, tietomurto, tallennus

ABBREVIATIONS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| BES | Brocade Encryption Switch |
| CTC | Crypto Target Container |
| DEK | Data Encryption Key |
| FC | Fibre Channel |
| FCID | Fibre Channel Identifier |
| FCP | Fibre Channel Protocol |
| FDISC | Fabric Disconnect, FCP Primitive |
| FLOGI | Fabric Login, FCP primitive |
| HBA | Host Bus Adapter. In this context, it is practically FC I/O adapter. |
| KEK | Key Encryption Key |
| LBA | Logical Block Address. In this context, always 512 Byte block address. |
| LU | Logical Unit |
| LUN | Logical Unit Number |
| MK | Master Key |
| NAS | Network Attached Storage |
| SAN | Storage Area Network, network dedicated for storage traffic |
| WWN | World Wide Name |
| WWNN | World Wide Node Name |
| WWPN | World Wide Port Name |

| | |
|---|---|
| KMS | Key Management System |
| SFP | Small Form Pluggable |

TABLE OF CONTENTS

# 1 INTRODUCTION

How much money is there in one's bank account? That information is stored in the bank's datacenter, in a server, in a database. The bank's web site forces the use of strong authentication, as well as the HTTPS protocol, to access the bank's web server to make bank transactions. Therefore there is no need to worry about someone eavesdropping traffic in between? But what is the encryption between the web server and the database? Does it matter if they are located in the same datacenter, and can one assume its physical security is implemented properly?

There are things to worry about. To keep banking account information highly available to users, banks obviously need to be prepared for a disaster in one datacenter. Therefore it is likely that the databases are being replicated to another location. So if one datacenter experiences for example a power supplying failure, servers in the other location can carry on providing the banking information service. Naturally the methods how this replication is being done are not public. IT hosting companies for example tend to use enterprise storage array subsystems and related technologies to mirror data to another storage array on another site. The protocol commonly used for that traffic is Fibre Channel inside optical fiber cable.

So, maybe there is dedicated optical fiber cable installed between the bank's two datacenters. No matter if you run the Ethernet or Fibre Channel protocol in it, it seems to be considered a private physical link layer that no one else can access. The risk in such an assumption could be that encryption is forgotten. Another dangerous assumption could be related to intrusion detection, as there must be interruption to the data traffic when a traffic monitoring device is inserted to the cable. Optical fiber cables are coated, so the light inside cannot be monitored, except by cutting the cable, inserting a monitoring device in between and then reconnecting the link.

Let us make the hypothesis that there is a Storage Area Network (SAN) based on Fibre Channel (FC), which is not encrypted and data is sent across two locations as plain text. Then somehow an attacker is able to capture data flow without

disrupting the data traffic. Is secret data stolen? This sounds simple to prove, so such hacking will be tested later in this thesis.

If the data is encrypted in our hypothetical situation, does it make it more difficult, maybe even impossible, to steal data? However, it must be understood that if the data was stored to a database, it is obvious that someone wants to read that encrypted data later. Therefore it must be decrypted some day and there is going to be a key or algorithm to do it.

Another hypothesis is that the attacker is able to breach physical security and steals everything from the datacenter, including fibre channel switches, disk storage array, and servers or appliances that may contain encryption key store. Can secret data be stolen?

This thesis will study the possibility to eavesdrop a Fibre Channel Storage Area Network. The possibility to eavesdrop such a network without being noticed will be also studied. After studying these topics in theory, the goal of the thesis is to build a sample environment with storage and servers attached together with Fibre Channel. The sample environment allows eavesdropping tests in practice. The thesis will also study the Brocade Encryption Switch (BES) solution together with encryption key management, and implement it as proof of concept to the sample environment.

# 2 WHAT IS STORAGE AREA NETWORK?

The acronym SAN stands for Storage Area Network, which is a high performance network whose primary purpose is to enable storage resources to communicate with computer systems. Storage resource can be for example diskdrive, disk subsystem or tapedrive. The definition of SAN does not take into account whether physical cabling is made by using twisted pair wire or optical cable, neither it does not take into accout what data transfer protocol is being used. It can be TCP/IP or FCP or something else. (Barker, Massiglia 2002, 3-6.)

An example SAN is represented in Figure 1, where SAN is formed by two Fibre Channel (FC) switches using Fibre Channel Protocol (FCP) to communicate. The SAN in Figure 1 also has one Local Area Network (LAN) switch that communicates by Ethernet. The physical layer for both technologies can be fiber optic cables, but for Ethernet it can be twisted pair cables also. Some protocols above Ethernet are sometimes referred to with acronym NAS, which stands for Network Attached Storage. The term is used mainly for NFS and CIFS protocols operating above the TCP/IP layer (Farley 2001, 24). The SAN term is commonly used for block-access storage, which is often storage subsystems providing logical units of storage, which behave as local disk drive from the client's point of view (Barker, Massiglia 2002, 18). Enterprise backup software commonly uses tape drives that can also be connected through Fibre Channel SAN, like in Figure 1.

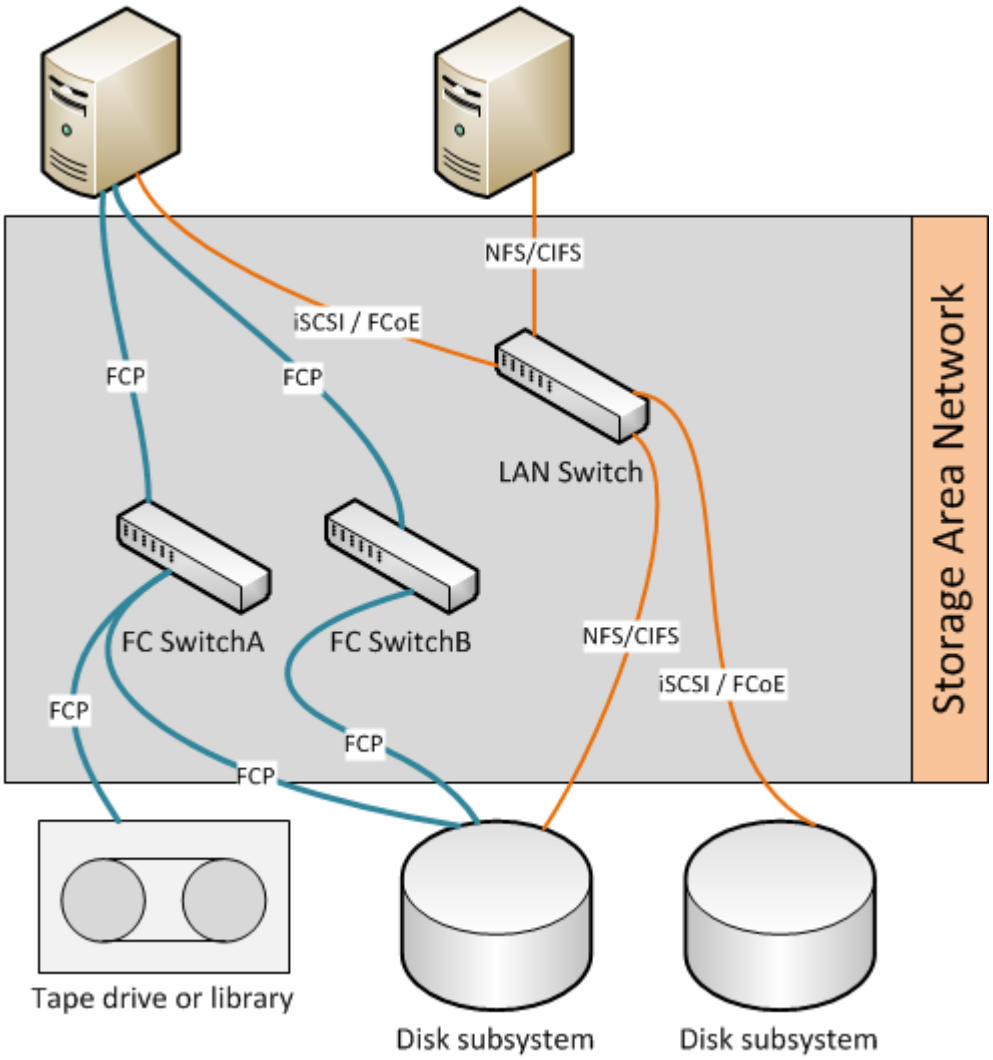


FIGURE 1. Abstraction of typical SAN

SCSI was developed initially already in 1981 for disk drive interface called SASI. It was renamed as SCSI (small computer system interface) in 1986, when it became an official ANSI standard (Farley 2001, 14-15). SCSI is still widely used in server computers, though physical wiring has changed from the 1980s.

## 2.1 Rationale for SAN attached storage

Why do companies choose SAN? Barker and Massiglia (Barker, Massiglia 2002, 4) state it simply saying “it is universal storage connectivity” and that computers are indeed connected to storage nowadays, but are all computers connected to all of its storage. SAN allows sharing disk storage with several servers

simultaneously, making it possible to quickly move business workload from one server computer to another without moving a large amount of data. Also, backups can be taken directly from disk-storage to disk-storage or from disk-storage to tape, so the server resources are not wasted to back up the valuable data.

### 2.1.1 Deduplication and data compression for efficiency

Today's storage subsystems are capable of finding duplicate data blocks and removing duplicate blocks to save space. This method is called deduplication. As an example, two server computers are installed to SAN storage and have the same operating system. Both servers will have 20 GB of storage space assigned. That would make a total of 40 GB of storage assigned. However, as it can be expected, the two server computers cannot differ from each other too much. Only the hostname, IP address and other small configuration parameters are different. If the storage array is capable of finding the duplicate blocks of storage, the other one can be replaced by a pointer. Such space saving mechanism is called deduplication. In this case deduplication would gain 99% space saving for the two installed servers. (Wollnik 2013.)

Data compression is based on different algorithms to reduce used space, and methods vary between storage vendors.

### 2.1.2 Thin provisioning

By the thin provisioning technique, it is possible to allocate more storage space to server computers than actually available inside the storage array. For example two server computers are installed to SAN storage and the operating system is the same. Both servers will have 20 GB of storage space assigned; total amount of allocated storage would be 40 GB. Very often after installing the operating system, it only consumes about 5 GB of disk space. For the two servers it would be 10 GB of used storage. If the storage array does not have more than 40 GB of storage space that can be allocated, it would be full by now. However, if thin provisioning is used, it would still leave 30 GB available for other server computers. Combining this with the deduplication technique, it would actually

leave the server computers with nearly 35 GB available for futher allocation to server computers.

# 3 FIBRE CHANNEL STORAGE AREA NETWORKS

Very often a server computer, as well as a personal computer has a local disk drive attached to it, like on the left-hand side in Figure 2. Three servers in Figure 2 have local disks connected by an SCSI, SATA or SAS cable. One of the servers cabled by SATA is also using a RAID controller to mirror two disks and presenting the mirrored logical unit to the server as a single device.

On the right-hand side in Figure 2, there are two servers that do not have local disks in the same case with the CPU and motherboard, but through a storage area network. Disks presented through SAN are similar local disks as for the three servers on the left hand side in Figure 2, but the cable is just extended over a distance. Logical devices are configured from a RAID array, which is called storage subsystem or storage array.

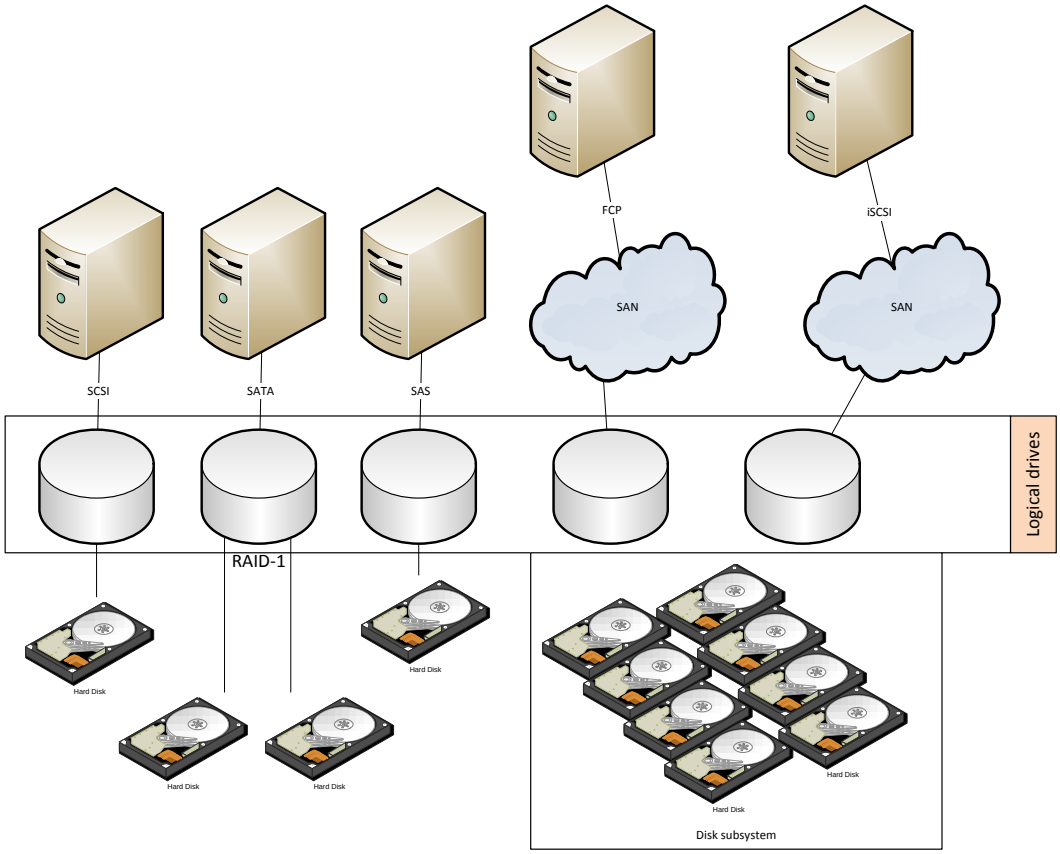


FIGURE 2. Comparison to local disks

## 3.1 RAID controller

In a single computer there can be two disk drives, but they are used via a RAID controller. The controller can mirror or stripe data to two or more disks, providing either fault tolerance or high performance or both. A server computer with two 100 GB disk drives and with a mirroring RAID controller distinguishes two disks into one single 100 GB disk to the operating system. The array continues to operate as long as there is at least one functional drive. The RAID controller is a kind of a volume manager. (Barker, Massiglia 2002, 92-93; Donald 2003.)

Commonly used RAID levels are 0, 1, 5 and 6. However, there are also proprietary RAID levels such as RAID-DP developed by NetApp or Intel's Matrix RAID. RAID-0 stands for block level striping, without parity or mirroring. RAID-0 with multiple disks provides performance over several disks, but does not offer protection from disk failure. RAID-1 stands for block level mirroring, and offers protection, while the performance is as fast as with one disk. RAID-5 stands for block level striping with distributed parity. RAID-5 requires at least 3 disks, providing performance over multiple disks, and is protected from a single disk failure. RAID-6 stands for block level striping with dual distributed parity. RAID-6 is formed from minimum of 4 disks, providing performance, and is protected from two disk failures.

## 3.2 Storage array subsystem

Storage array subsystem is a complicated volume manager. One system can have hundreds of physical harddisk drives, often configured with different RAID levels. Logical units (LU) are sliced from the configured RAID groups and allocated to server computers. Figure 3 illustrates key points from a filesystem to a SAN attached storage subsystem with a bunch of disks. Logical unit (LU) is called virtual disk in Figure 3. Four physical disk drives in storage array can be configured as RAID-5 or RAID-1 or something else. Then, a chunk of the logical space is allocated as logical unit, also known as virtual disk. Virtual disks are then mapped to the server computer where the device driver makes it visible to the

operating system as a local disk drive. The filesystem can then be created to the local disk that is actually not local, at least not physically.

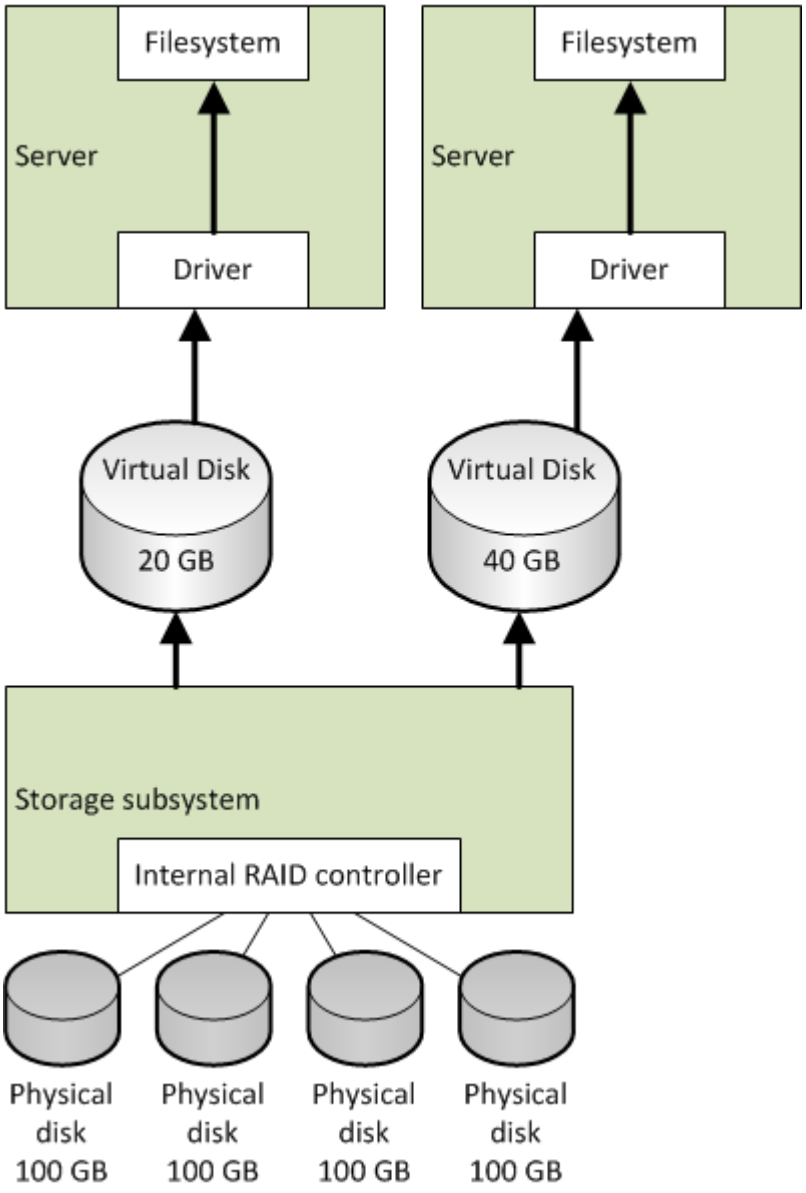


FIGURE 3. Logical view of disk storage subsystem

## 3.3 Logical Block Address (LBA)

Each physical disk or logical unit is sliced into multiple blocks and each block is referred through block addresses. Block size, however, may vary depending on the filesystem, device driver and storage subsystem. For example, there is one logical unit allocated to a server computer with size of 1 MB, as illustrated with

virtual disks in Figure 3. One megabyte is 1048576 bytes. If the filesystem is formatted with 64 KB block size, the logical unit can be addressed throughout with 16 different LBAs. 64 KB multiplied by 16 equals 1 MB, and its LBA numbers are referred to as LBA0 … LBA15.

However, the device driver under the filesystem (see figure 3) may not be using the same block size, so it actually accesses the virtual disk from the storage array with block size of 512 bytes. So the device driver sees 2048 logical block addresses for the virtual disk. That is LBA0 … LBA2047.

Now, if the operating system needs to read data from the filesystem LBA0, the device driver will actually read data from its LBA0…LBA127 and pass the information to the filesystem.

Classical Master Boot Record is generally written to the LBA0 of 512 bytes. Later in this document LBA size is always referred to as 512 bytes.

### 3.4 Server connection to a storage array in FC SAN

Basically, there are two kinds of objects in SAN connectivity: SCSI initiators and SCSI targets. Initiators are called Host Bus Adapters (HBA) on the computer or server side, while targets are storage subsystem adapters. Initiators and targets must be connected together in order to form connectivity. If a single physical harddisk drive is installed to a server or personal computer, it is connected by an SATA, SAS or SCSI cable to the computer's motherboard. On FC SAN cabling is done by fibre optic cables and connection between server and storage is commonly performed with a technique called zoning. It can be done without zoning as well, meaning that all initiators in the SAN can see all the targets and initiators in the network.

One more key thing is to understand the meaning of the SAN fabric before we go deeper into how servers and storage connect. The SAN fabric is similar to a network segment in a local area network. SAN can have one or more fabrics. Very often there are two fabrics within a single SAN to provide fault tolerancy. Fabrics

do not interact together so they are isolated segments of their own. Very often fabrics are physically separated from each other.

### 3.4.1 Host Bus Adapter (HBA)

Host bus adapters are a kind of a network adapter that has a unique world-wide name, called World Wide Name (WWN). It has two portions. World Wide Node Name (WWNN) is unique for the adapter or server or storage device itself. World Wide Port Name (WWPN) is unique for a single physical port within the adapter or storage device. When HBA logs in to SAN, it will have FibreChannel ID (FCID) that is unique within the SAN fabric. This process is called FLOGI and happens only once when HBA logs in to the fabric. When HBA is moved to another port in the SAN switch or when the server is rebooted, FCID may or may not change in the FLOGI process. If there are no restrictions in the SAN as to what storage targets HBA can connect, it will log in to every SCSI target there is in the fabric. This process is called PLOGI and happens when a new storage target is about to be scanned for the HBA.

### 3.4.2 World Wide Names

Every node and port in the Fibre Channel fabric has a globally unique world-wide name. For nodes this is called World Wide Node Name (WWNN). For ports it is World Wide Port Name (WWPN). Globally unique WWNs are maintained by the IEEE organization together with hardware vendors. For example in Figure 4 there is one HBA with two ports. The HBA itself has a unique node name and both ports have a unique port name. WWN can be either 8 bytes or 16 bytes in size. Physical ports, such as server HBA, are using an 8-byte WWN identifier while logical units are using 16-byte WWN. (Butler 2007, 1-3).

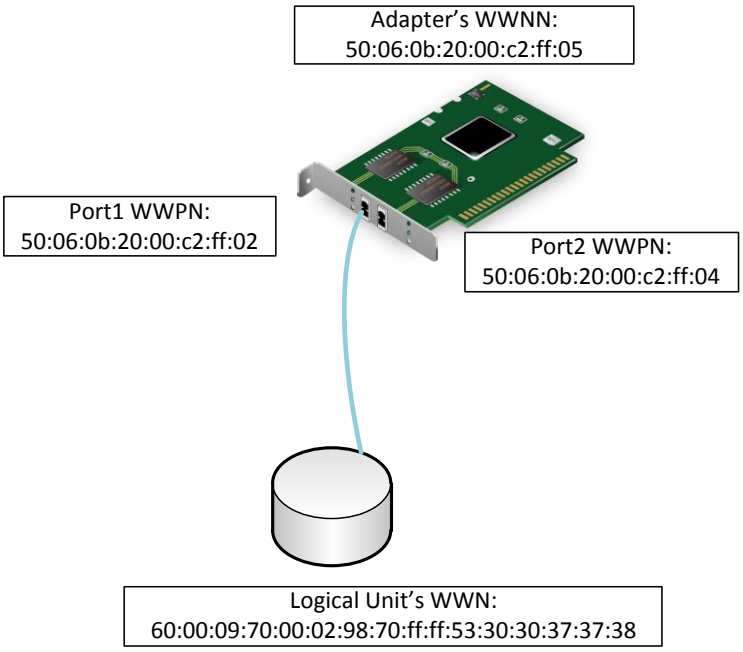


FIGURE 4. WWN example

### 3.4.3 Zoning

Zoning is a technique that can be used to isolate initiators and targets from communicating to every node in the SAN. As stated in the previous chapter, there are several unique identifiers for devices in the SAN: WWPN, WWNN and FCID. These identifiers can be put as members of a zone. Each zone has members that can interact together, but not with members outside their zone. There are no restrictions as to what members can be within a zone, meaning that a single WWPN or FCID can be in all zones within the fabric if that is preferred. From those two, WWPN is a more flexible option to be used in zoning, because it does not depend on anything else than the HBA. If a server is moved to another location or SAN switch port, WWPN remains the same and zoning is valid after the change. If the server is moved to another location or SAN switch port, its FCID may change, and thus it requires modification to zone configuration.

If server HBA fails and must be replaced, WWN is changed in HBA. If zoning was done with WWPN or WWNN, zoning must be reconfigured while FCID-based zoning may not require such modifications. Zoning does not provide a security feature, it provides separation. (Tate, Lucchese, Moore 2006, 188-193.)

### 3.4.4 Masking logical disk device to a zoned initiator

In most storage array subsystems it is not enough that a server computer is zoned to the array, masking to a logical disk device must also be defined. So far, HBA initiators and logical devices have been described, but one more object must be defined before the logical disk is available to the server operating system: Logical Unit Number (LUN). For each logical device to be mapped, a LUN number must be given. The LUN number should be unique for each initiator and per SCSI target, also known as storage array. Some storage arrays use the term host group or initiator group, which consist of initiator ID and LUN numbers for mapped logical devices.

## 3.5 Multipath Input / Output

An example of single point of failure is the SATA cable between a personal computer's motherboard and harddisk drive. If the cable is cut, connection will fail. SAN is often designed to provide fault tolerance by having at least two fabrics that are separated from each other and designed so that a crash or failure of a single fabric does not affect input and output operations on the other fabric. So if two cables are placed in a personal computer to connect a single harddisk drive and motherboard, the operating system is likely to see two disks, while there is actually only one disk behind the cables. A similar issue is common on storage attached through SAN. However there are multipath IO drivers, which detect how many paths there are to a single logical device and the driver presents the multipath device as a single disk to the operating system.

# 4 BUSINESS CONTINUITY

Some years ago when one visited a doctor, medical records were stored by using media called paper. The medical center or customer took care of storing this data in a secure way. It could mean storing the paper in a safe that is not vulnerable to fire or stealing. It could also mean that the paper was copied and stored in two different locations to make sure the medical record would not be lost, even if it was stolen and destroyed in another location. Business or public healthcare just has to work even after a disaster. This is called business continuity.

Nowadays several government agencies and the banking sector are required to follow certain requlation on business continuity. The Finnish government sector follows the national security auditing criteria defined by NCSA-FI and the banking sector follows standards defined by the national financial supervisory authority, also known as Finanssivalvonta. (Basel Committee on Banking Supervision 2011; Finanssivalvonta 2010; Ficora 2013.)

## 4.1 Backup and disaster recovery

By the nature of computer systems, data may get lost on several scenarios, for example human error, software error, hardware error and malware. Very often backup and disaster recovery are referred to as the same thing and in a way they are, but still are not. For example, the doctor needs to access a client's medical record from the archive, but the single file is missing. The single file would be restored from the backup. It could be in another office or in another safe somewhere. But if the whole archive is lost, burnt for example, then restoring would be called disaster recovery and the method may be different.

Methods to recover a single file or a whole archive may be the same, or may not. If a single file in the archive is 1 MB of size and the archive contains 500 files, it would not make a big difference to restore it from backup media that can perform the restore operation at the speed of 50 MB/s. Restoring a single file would take 0.2 seconds while recovering the full archive would take 10 seconds. If the archive contains 8 million files, restoring the whole archive would take over 44 hours at the speed of 50 MB/s.

The law or customer may define the recovery time objective less than 4 hours, abbreviated as RTO 4h. Recovering 8 million of 1 MB files from traditional backup media is not an option in such a scenario. Mirroring or synchronizing data to another storage array could be the solution, as well as some disaster recovery products, depending on the technology used to store the original archive.

## 4.2 High availability and eavesdropping of SAN

The Finnish financial supervisory authority has stated explicitly that those under supervision must minimize service interruptions even in the case of fire, flood, hardware failure or electricity outage (Finanssivalvonta 2010, 28). Fire, flood and electricity outage are the hard challenges to overcome; basically it means separating computer services to at least two different locations and failure domains. Then data must be continuously synchronized to another location several kilometers or hundreds of kilometers away from the primary location. When data is moved over distance, the physical security that was in place in the server room or within company facilities does not exist anymore. Optical cables are buried to the ground or installed to pipes or sewers. Anyone with enough interest can go to sewers or take a shovel to dig up the cable from its ducts.

# 5 PHOTONS OF INFORMATION

## 5.1 Fibre Channel Protocol (FCP)

Fibre channel is a transmission protocol just like Ethernet. Fiber channel is broken up into five layers, three physical layers and two upper layers. Layers are described in Figure 5.

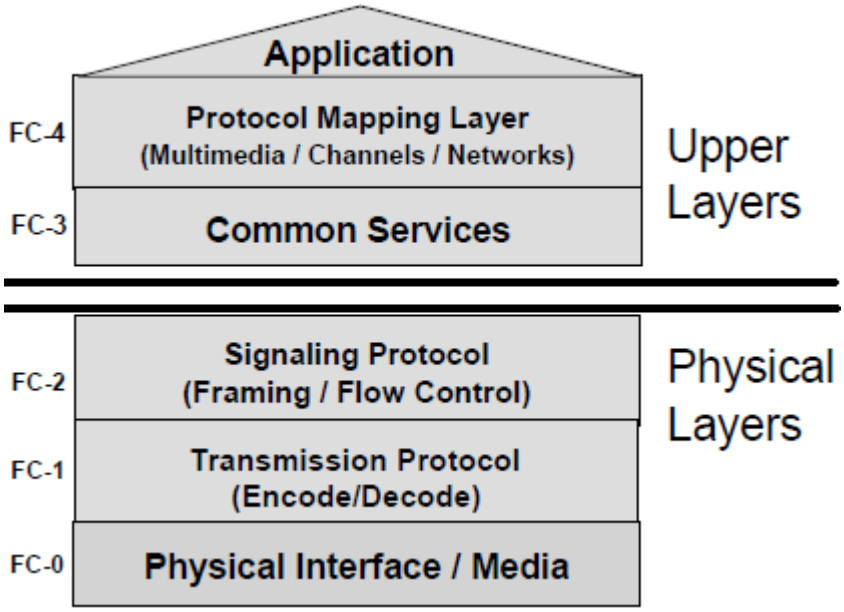


FIGURE 5. FCP layers (IBM redbook)

The FC-0 layer in Figure 5 is commonly connected by fiber optic cables, which are divided into two different categories: single-mode and multi-mode. The difference between these two cable modes is how the light signal travels in the cable. Single-mode is used for long distances and is more expensive, because of laser sources. Multi-mode is used for short distances and the signal source can be made with cheaper electronics, such as light-emitting diodes (LED). Figure 6 describes how the light signal travels in single-mode and multi-mode cables. Due to modal dispersion, multi-mode has higher pulse spreading rates than single mode fiber, limiting multi-mode's information transmission capacity. (ARC Electronics 2007.)

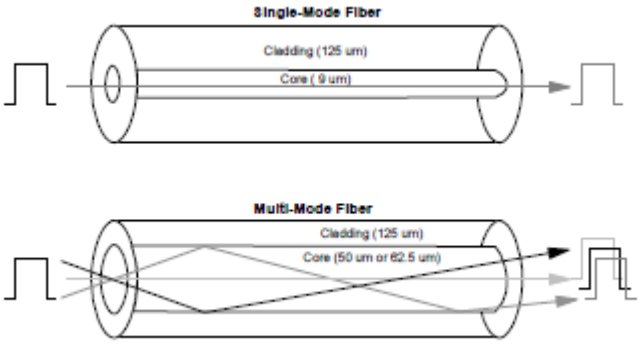


FIGURE 6. Two modes of optical cables (Tate et al 2006, 42)

## 5.2 FC Frame and SCSI payload

The size of the Fibre Channel frame may vary from 9 to 537 transmission words, where the size of each transmission word is of 40 bits. Transmission word is the smallest transmission unit defined in Fibre Channel. Transmission word consists of four transmission characters, each 10 bits. (Tate et al 2006, 46-57).

Other rules that apply to the framing protocol are:

- A frame is the smallest unit of information transfer.
- A sequence has at least one frame.
- An exchange has at least one sequence.

| | | **Byte 0** | **Byte 1** | **Byte 2** | **Byte 3** |
|---|---|---|---|---|---|
| **SOF** | **TW 0** | SOF | | | |
| **Header** | **TW 0** | R_CTL | Destination_ID (D_ID) | | |
| | **TW 1** | Reserved | Source_ID (S_ID) | | |
| | **TW 2** | Type | Frame Control (F_CTL) | | |
| | **TW 3** | SEQ_ID | DF_CTL | SEQ_CNT | |
| | **TW 4** | Originator X_ID (OX_ID) | | Responder X_ID (RX_ID) | |
| | **TW 5** | Parameter | | | |
| **Payload** | **TW0** | | | | |
| | **…** | 0… 2112 Bytes | | | |
| | **TW527** | | | | |
| **CRC** | **TW0** | CRC | | | |
| **EOF** | **TW0** | EOF | | | |

FIGURE 7. Fibre Channel frame structure

In Figure 7, all data fields are referred to as bytes, as in 8 bits. As each transmission word (e.g TW0 in Figure 6) is 40 bits, while four bytes is only 32 bits, the framing protocol will need to add fill bits. Fill bits are required to make 8b/10b and 10b/8b encoding that will reveal possible parity and other errors. The fill bits are removed at the destination. (Tate et al 2006, 46-57).

FC Payload in storage environments contains SCSI protocol commands and data. Commands often fit in just a few bytes, containing information about Logical Unit Number (LUN), whether it is going to be write- or read -I/O operation, Logical Block Address (LBA), priority and other information. SCSI data is just the data that is written to or read from the LUN LBA that was defined by the SCSI command.

## 5.3 Stealing photons by placing a splitter in between

There are devices called fibre optic splitters, sometimes referred to as couplers. These devices take in a light beam and split it into two or more light beams. In Figure 8, there is a splitter device with one input terminal and two output terminals. Both outputs are receiving the same light beam from the input terminal, but with a certain loss ratio.


FIGURE 8. Fibre Optic splitter

So if one would like to steal data from an active optical link, the link must be broken and reassembled with a splitter in between. Once the splitter is in between, one can attach a sniffer or analyzer device to the splitter and eavesdrop the traffic that goes through the link. This metod is also called man-in-the-middle attack.

However, this method is likely to cause an alarm event for the party responsible for the link, for example a link down or link up event.

## 5.4 Stealing photons, undetected

To do eavesdropping with a splitter device without breaking the original link, there are devices called fibre optic clip-on couplers or splitters. The Clip-on coupler method rely on bending the fibre optic cable just enough beyond a particular radius, so that a small amount of light leaks from the outer corner. A Clip-on device also attaches a glass prism through the cable coating to the optical cable core, allowing the attacker to steal the data traffic that flows through the optical link.

Unlike a normal splitter, this method is likely to trigger no alarms, as proven in the Infosecurity show in London, 2007. This method did not make noise or errors to the line while data capturing was in progress (Leyden 2007). There are a few publicly known cases when such optic monitoring has been done. The security forces of the US found an illegal clip on splitter attached to Verizon’s network in 2003 (BlackHat federal briefing 2003). Former intelligence officers in the US confirmed that NSA is able to monitor underwater fibre optics with a submarine that is placed over the cable (Zorpette 2001; BlackHat federal briefing 2003; The New York Times 2005).

# 6 ENCRYPTING DISK STORAGE IN SAN

If encryption of disk data is made on the SAN layer, encryption is transparent for the host systems as well as for the storage arrays. The SAN Network layer in between makes the encryption, thus an encryption key is not required to be exposed to the host system and host accesses its data as plaintext. Meanwhile, the storage array does not need to know the encryption key, it can see data from the host system only as ciphertext.

## 6.1 Advanced Encryption Standard (AES)

Advanced Encryption Standard defines the FIPS-approved data encryption method implemented by Rijndael algorithm. AES is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. Rijndael was designed to handle additional block sizes and key lengths, such as 512 bits, but those are not in the standard. AES has survived numerous cryptanalytic tests and for ten years it has been the most popular cryptographic primitive. It is recognized as a very strong encryption algorithm. Recovering an AES cipher key requires a lot of computing power and it is considered nearly impossible nowadays. In 2011 a new algorithm was found, making it four times easier to recover the cipher key for AES, but it is still a long process to recover it. After these findings Andrey Bogdanov, crypto researcher from Leuven University, has given a practical example for how long it actually takes to recover the AES cipher key. If a trillion computer machines, which each could test a billion keys per second, would be used to recover the key, it would still take more than two billion years to recover an AES-128 key. (Federal Information Processing Standards Publication 2001; Neal 2011; Bogdanov, Khovratovich, Rechberger 2013.)

## 6.2 Encryption Key life cycle management

Disk data is encrypted and decrypted using the same Data Encryption Key (DEK), meaning that the key is symmetric. A practical synonym for symmetric key is password. The DEK must be preserved as long as there is a need to decrypt the

ciphertext that the DEK created. In some applications key management is complicated and multilayered and for such cases there are a number of key management systems provided by third-party vendors, such as Thales, RSA and Netapp for example (Wikipedia 2013). Key management then stores DEKs and can revoke, delete or backup the keys. If an encryption key is compromised or expired, a new key must be generated and data must be re-encrypted with the new key. This process is later referred to as re-key operation. If data must be stored for years or decades before it is accessed, and if several re-key operations have been issued in between, not only the DEKs must be available, but also identification of which backup copy was encrypted with a specific DEK. This identification can be made by giving an ID for each DEK. Some systems create this ID, by using Secure Hash Algorithm (SHA) and if ID is documented with each backup, proper DEK can be recovered according to this ID. (Brocade 2011, 7-10.)

## 6.3 Data-at-rest encryption with multipath I/O

Earlier in this thesis, multipathed input/ouput was described, where a server computer can access its logical unit through multiple paths, where different paths go through isolated fabrics. Fabrics are not connected together, resulting in highly available SAN connectivity where failure in one fabric does not affect the other fabrics.

Multipath I/O makes it difficult for data-at-rest SAN encryption, because a host must encrypt and decrypt data traffic with the same data encryption key (DEK) on both fabrics. Failure to do so will result in data corruption because the same logical block address may be accessed in plaintext and ciphertext.

# 7 BROCADE ENCRYPTION SWITCH

Brocade Encryption Switch, referred to as BES, is a network-based solution that secures data-at-rest for disk array LUNs and tape drives, using Advanced Encryption Standard (AES) 256-bit algorithms (AES-256). Encryption and decryption engines provide in-line encryption with up to 96 Gbps throughput for disk I/O. Disk I/O is a mix of ciphertext and cleartext traffic.

As in a normal SAN network, connectivity between the server computer and storage array is made from physical initiator to physical target. BES hides physical end points from each other and replaces them with virtual initiator and virtual target (see Figure 9). Internal re-routing zoning makes sure physical initiator is able to communicate only with a virtual target. The encryption engine then encrypts the payload of the Fibre Channel frame and passes it to the physical target.

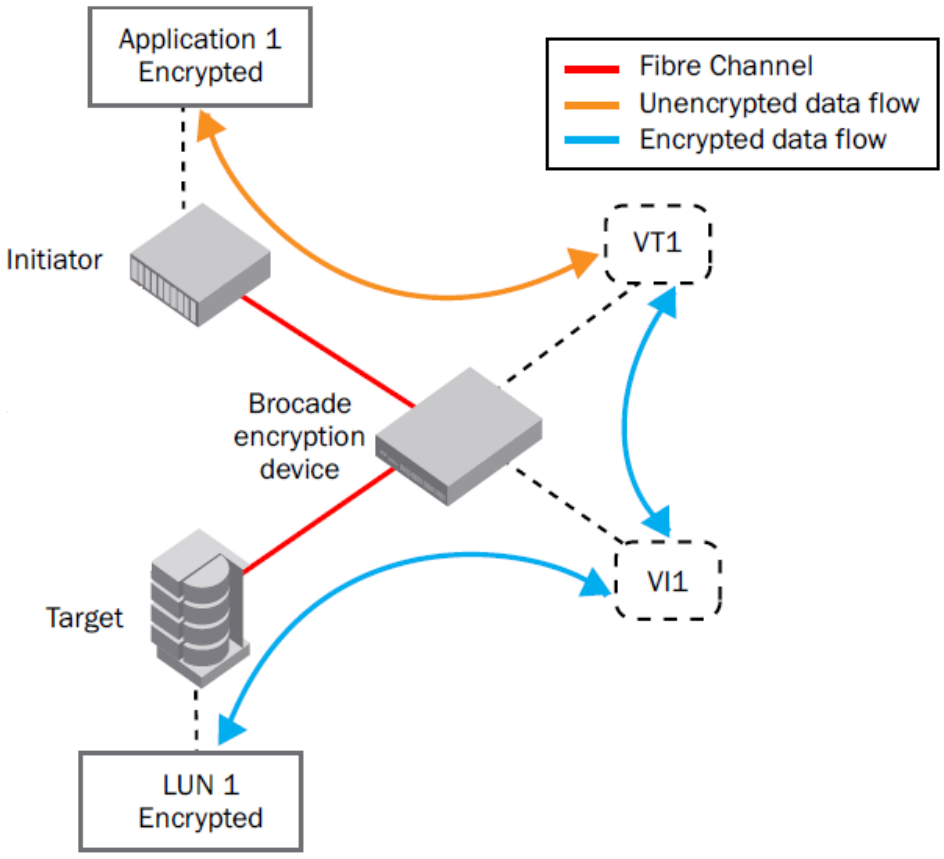


FIGURE 9. Encryption engine's logical data flow (Brocade 2011, 8)

For each target used in encryption configuration, BES requires a configuration object called Crypto Target Container to be created, referred to as CTC. One CTC can contain only one target but multiple initiators and LUNs. When an initiator is added to a CTC, it will loose connectivity to its LUNs in the target, if the LUNs are not also added to the CTC. For each LUN added to a CTC, it must be defined whether this LUN is going to be encrypted, kept in plaint text or if it was already encrypted.

When an initial encryption is performed to the LUN, BES writes its metadata to the LUN LBA range 1-16, including Data Encryption key ID, but not the key itself. LBA 0 is always cleartext, even for an encrypted LUN. Metadata is not visible to the host itself, but LBA range 1-16 of cource is. However, BES will handle I/O request to this region in the encryption software and the host will not know that physical LBA actually contain different data than the host is able to see from this LBA range. Metadata on the LUN is useful if the LUN is later cloned to another environment or data has to be restored from backup. (Brocade 2011, 185.)

## 7.1 Data Encryption Key group (DEK-group)

Data encryption key, referred to as DEK is a symmetric key that is used to encrypt and decrypt data. When a LUN is encrypted, BES will generate a data encryption key (DEK) for the LUN. DEK itself will be encrypted by key a encryption key (KEK). Brocade Encryption Switch may implement DEK encryption by KEK in two different ways, which are described more in later chapters of this thesis.

When deploying a highly available SAN solution, multiple SAN fabrics are required to provide fault tolerance, as described earlier in this document. If a server computer had two paths to the storage like in Figure 10, but only one of these paths used a data encryption key to encrypt the data, it would result in read operations through Fabric 2 to seem like an I/O error or data corruption. It would be even worse if the data is later written back through Fabric 2 as plain text, while the other path decrypts this plain text with DEK. This would definitely result in a data corruption scenario.

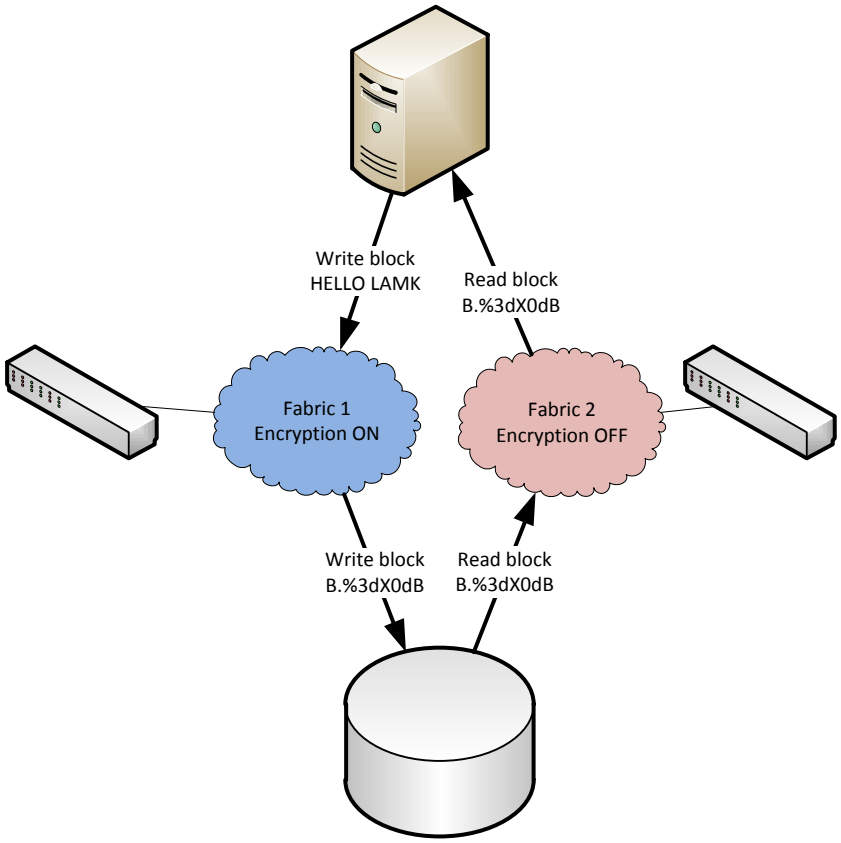


FIGURE 10. Multiple paths with only one path configured for encryption

To avoid data corruption and still provide multiple fabric solution, Brocade encryption switches can be configured to share data encryption keys within a group called an encryption group. An encryption group, also known as DEK group, is formed by two or more encryption engines that are connected to each other through a dedicated cluster I/O sync link, which uses the TCP/IP protocol. In order for encryption group members to communicate with each other, members must trust each other in the group. Trust relation is created by first configuring a single member as the group leader and importing certificate files from other members to it. Trust is then formed by configuring members for the group leader by defining a certificate file, world-wide-name for the member, as well as its I/O sync link IP address. The management network for the switches is physically separated from the I/O sync link, as seen in Figure 11. Once an encryption group is formed, encryption switches can share data encryption keys for a single LUN, allowing multipath I/O without data corruption.

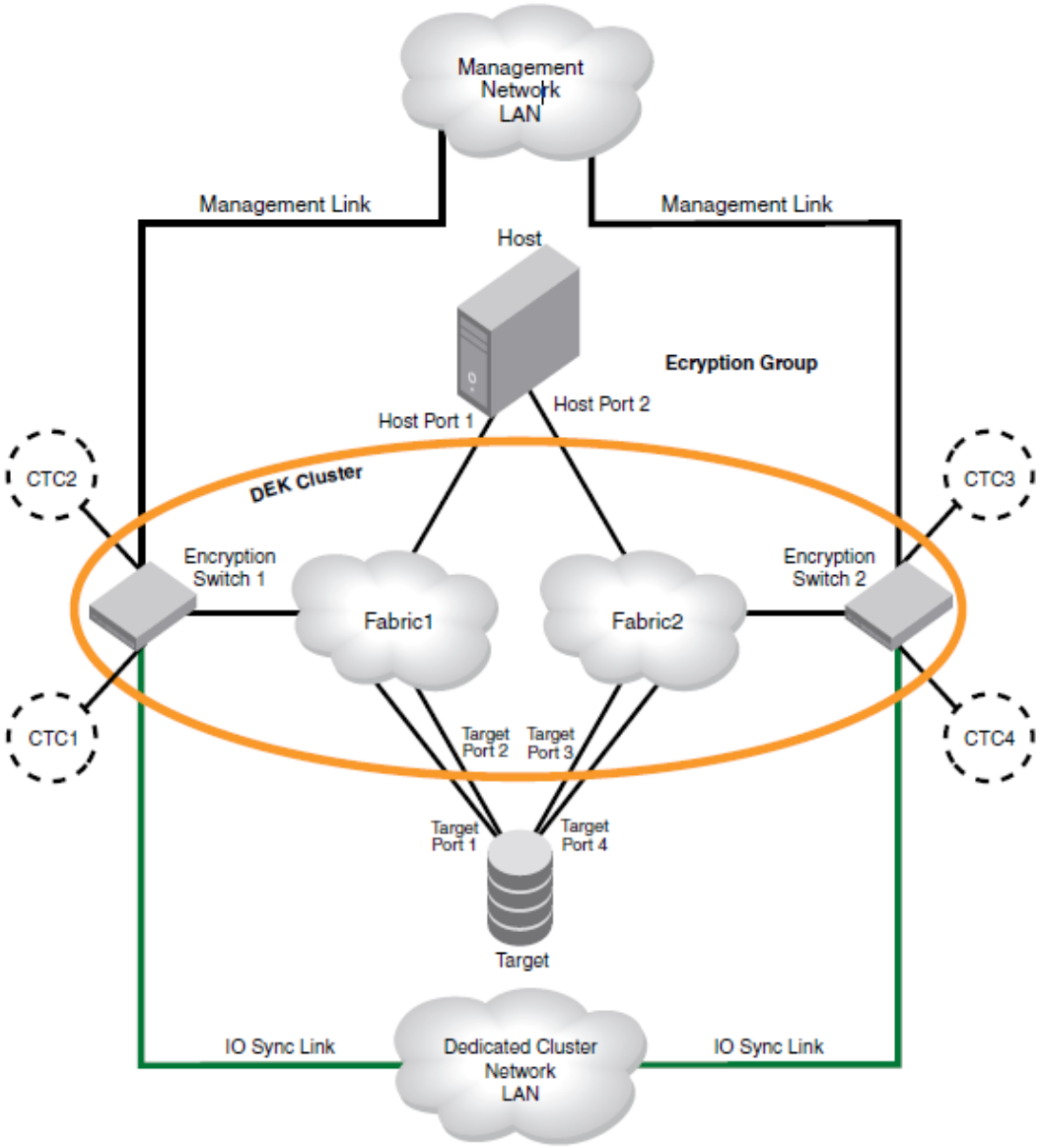


FIGURE 11. Multiple path, Data Encryption Key group (Brocade 2011, 172)

Once the encryption group is formed as in Figure 11, all encryption operations are managed as a group, and all the commands are issued from the present group leader. The group leader can change, but it is by default the switch that issued the create encryption group command. (Brocade 2011, 9-11.)

## 7.2 Key Management System (KMS) and key lifecycle management

Data is encrypted and decrypted by using the same data encryption key, so a DEK must be preserved for as long as the data is needed. Losing the DEK is similar to

data loss. Key management systems provide life cycle management for encryption keys by storing the keys for years or decades, if necessary. In the Brocade encryption switch environment, there are four stages in the life on an encryption key. The first stage in the key lifecycle is creation of the key by an encryption engine and encrypting the data with it. The second phase is key distribution to other encryption engines, if there are any, and storing the key into a key management system, referred to as key vault. The third stage is its lifetime, while the key is used to encrypt and decrypt data. The fourth and last stage is key expiration, termination and destroying. The last stage of the key's lifecycle is reached either manually by specifying the key to expire for just in case or if the encryption key is compromised. Key expiration may also happen automatically if there is maximum lifetime configured for the key to prevent it from becoming compromised. (Brocade 2011, 9-11; Bouchard 2012, 87-90.)

During the second phase of the key lifecycle, when the key is stored to a key vault, it is first encrypted before being moved away from the BES FIPS 140-2 Layer 3 security boundary. The term FIPS 140-2 Layer 3 boundary is used for the secure physical chassis of Brocade Encryption Switch, defined and approved by the United States federal government. By encrypting the data encryption key (DEK) before it is sent out from the FIPS boundary, it is protected from compromising in the process.

The encryption key used to encrypt DEK is called key encryption key (KEK). Key management systems compatible with BES are divided into two categories: opaque key vault and trusted key exchange. An example of trusted and opaque key exchange is shown in Figure 12. In trusted key exchange, key vault and BES authenticate each other for example with a SSL certificate. This may vary between vendors. Most vendors also use a linked key, which is a symmetric key that is used to encrypt DEK before moving it over trusted exchange. In trusted key exchange, KEK refers to a link key that is the orange key in the upper section of Figure 12. In trusted key exchange, key vault is able to see the data encryption key as cleartext.

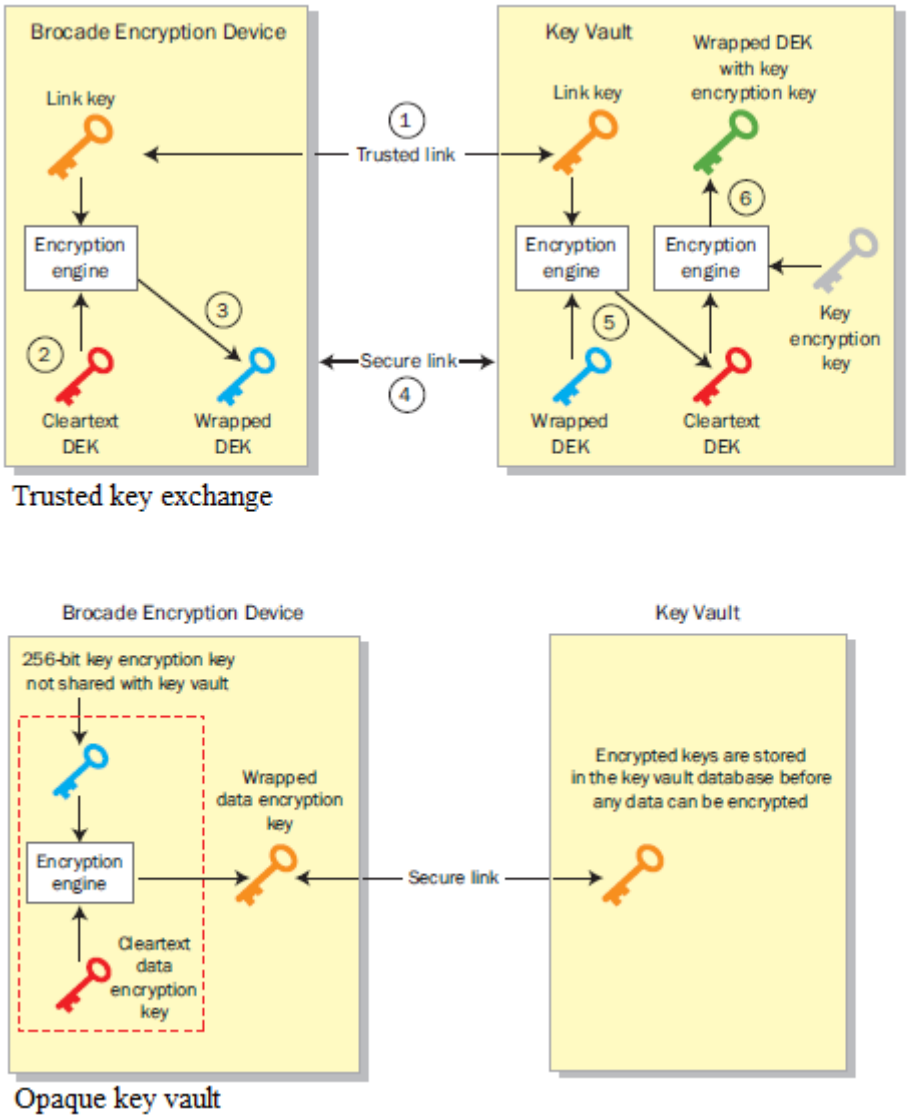


FIGURE 12. Trusted vs Opaque key exchange (Bouchard 2012, 89-90)

In opaque key vault, key management never has access to the cleartext data encryption keys. Also, opaque key vault does not contain information on how the DEK was encrypted. The Brocade Encryption switch forces generating a Master Key (MK), which is used to encrypt DEKs before sending them out to the opaque key vault. Brocade Encryption Switch allows backing up the Master Key to a file or to a opaque key vault by encrypting it with a passphrase. It is also possible to back up the Master Key to a set of smart cards. (Bouchard 2012, 87-90; Erma 2013.)

# 8 SAMPLE ENVIRONMENT

A sample environment was build in order to test eavesdropping in practice. The sample environment included one server computer with Fibre Channel HBA, one storage array subsystem, one Brocade Encryption Switch, one key management system and a Fibre Channel 8 Gbps capable sniffer device. Red Hat Enterprise Linux was installed to the server computer, with one logical unit (LUN 0) assigned from storage array as a root volume. The server computer does not have local disks and it boots from SAN storage. Ideally the sample environment represents a modern datacenter with SAN fabric.

## 8.1 First test scenario, man in the middle

Figure 13 displays the first test set made, connecting the server and storage together with a single optical path through the Brocade Encryption switch. At this phase the BES is acting as a normal, non-encrypting SAN switch allowing the server and array to communicate with each other in cleartext. The upper part of Figure 13 represents how the server and storage array see their physical connection, as well as how it would be normally cabled. The lower part of Figure 13 represents cabling and sniffer device installation during the test case. The sniffer device in the sample environment was manufactured by JDSU and its model is Xgig.

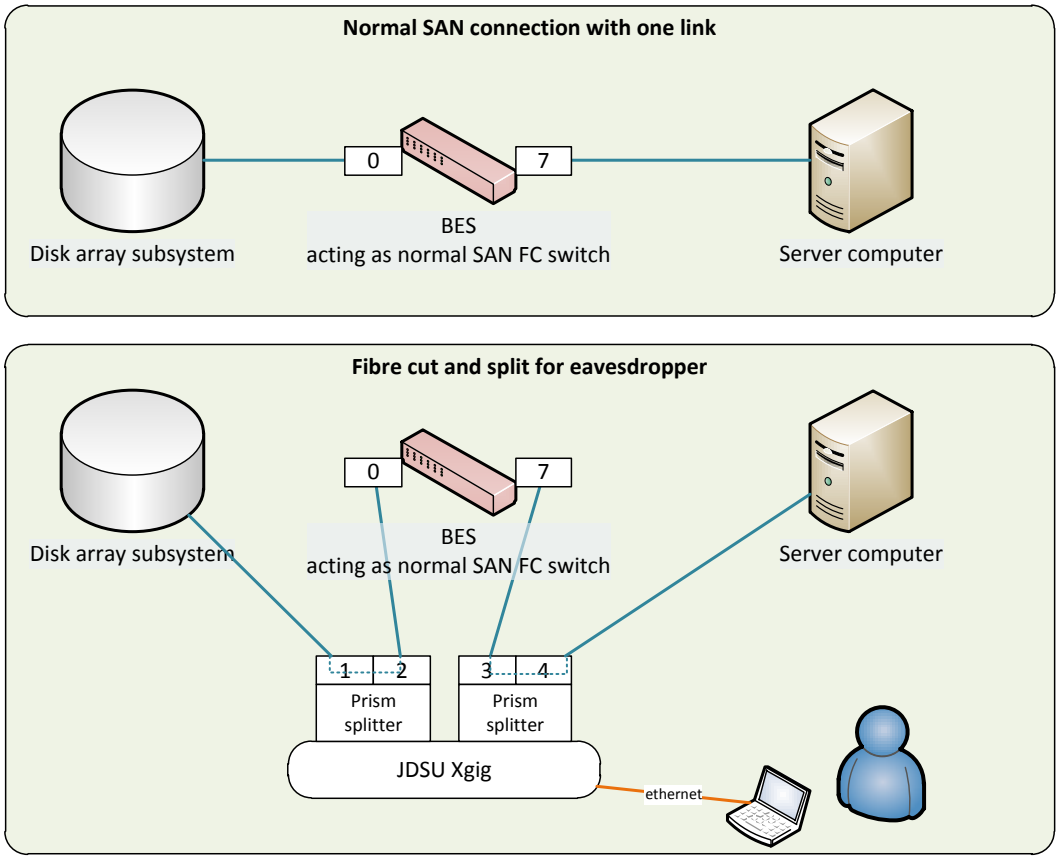


FIGURE 13. Test phase one

As there is no encryption in this phase of the test, sniffered payload is the same from both prisms seen in Figure 13. In order to achieve such scenario in real life for eavesdropping purposes, one would need to break the optical circuit and connect both ends through a splitter, which would be likely to create an alert to the party responsible for the SAN fabric. During the first eavesdropping test the operating system was installed to the server computer. The server computer has one logical unit allocated from the storage array, mapped as LUN 0 and size of 30 GB.

As a side note, in all modern operating systems password brute forcing does not work well to the server directly, as there is probably a limited number of attempts before the account will be locked.

During the first eavesdropping test, the hashed root password was captured by the JDSU Xgig when written to files called /etc/passwd and /etc/shadow. Gaining this

information, an attacker is able to brute force the root password without the account being locked in the process. Also, because eavesdropping revelead also the operating system version, hash mechanism can be easily searched and so-called rainbow tables can be used to obtain cleartext root password faster. Gaining hashed passwords is not only limited for the installation of the operating system, but also every time when the server computer reads the hashed password to its memory when a user is logging in.

## 8.2 Trying sniffering with clipon coupler

Similarly to how the optical signal was split to the eavesdropper device in Figure 13, the second test scenario in this sample environment was to achieve the same without need to break the optical circuit, thus being undetected. There are several manufacturers for clip-on fiber couplers on the market and such a coupler costs from USD 500 to up to USD 10 000, depending on quality and deamplification the device will create to the actual link. In figure 14, there is an example of a clip on device designed for single-mode fiber optic, running signal on light wavelenghts of 1300 ~1500 nm, with insertion loss of less than 7 dB.

FIGURE 14. Kingfisher's OPT130 Clip-on coupler (Kingfisher international 2013)

It seems that most clip on couplers are for single-mode cables only, but there are some for multi-mode cables as well. Because it was hard to find one for the multi-mode cable, a single-mode clip on coupler was used for the next test.

Long distance inter switch links in Fibre Channel SAN are very commonly implemented by single-mode cables. Another SAN switch was obtained to the sample environment and set up as described in Figure 15. The single-mode cable connecting the two switches was not more than 3 meters long and fiber optic modules on both switches were extended long wavelenght SFPs, running on 1330 nm.

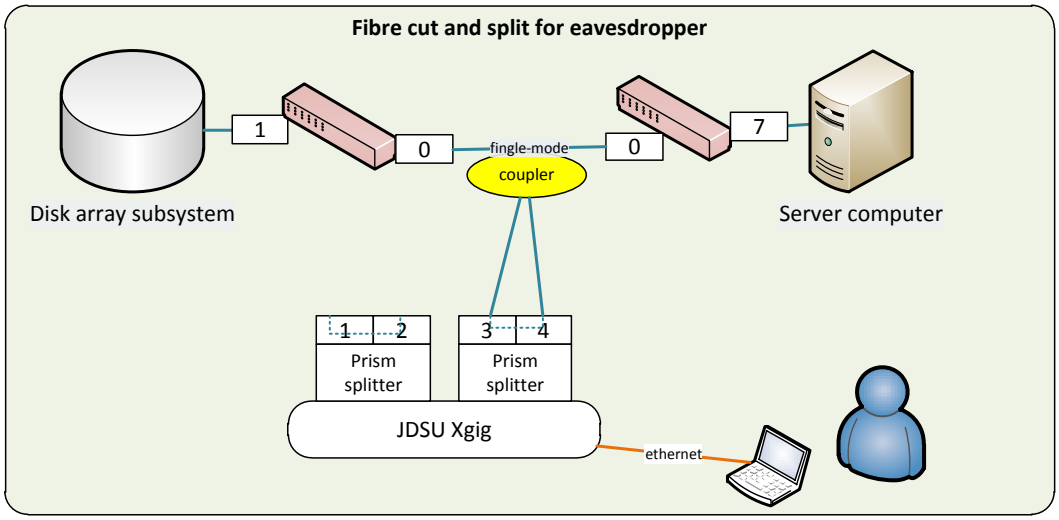


FIGURE 15. Test phase two

Fiber optic modules were broken during the test because receivers got too much input power, as the modules were sized to connect up to 40 kilometer paths, while the fiber in between was only a few meters long.

The decision was made to abort the test, as it had already been seen it is possible to steal data payloads being transferred. It seems relatively easy to use a clip-on coupler for the working single-mode link as the coupler does not badly harm the coating of the cable.

## 8.3 BES encryption enabled

After the unsuccessful clip-on coupling test, the sample environment was returned to the similar state as in Figure 13, but now Encryption Engine was enabled and LUN 0 encrypted by BES. As mentioned in Chapter 7 and Figure 9 on page 21, the encryption engine redirects all frames through virtual initiator and virtual target ports that belong to the encryption engine itself. After crypto-target-container was created for the disk array target port and the server's HBA and LUN configuration brought in to the CTC, Brocade Encryption Switch created redirection zones for the encryption engine. Each device logged in to the SAN fabric has FCID, and so has the encryption engine. Figure 16 displays cabling and physical and virtual ports for this scenario with the following FCIDs assigned to each port:

- switch port - FCID
- port 0 - 0x010000
- port 7 - 0x010700
- virtual initiator - 0x012401
- virtual target - 0x012001

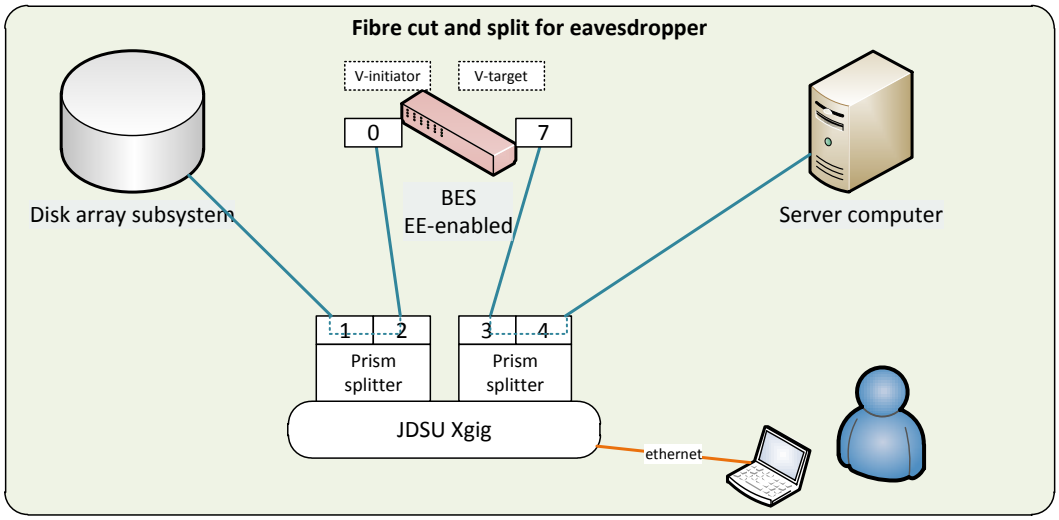


FIGURE 16. Third test scenario with encryption enabled

Without encryption and redirection zones, when the server sends an I/O request to storage array, it would send it from source FCID address of 0x010700, to destination address of 0x010000. After encryption is enabled and CTC configured, when the server sends an I/O request, it is actually going to virtual target in destination address of 0x012001.

In order to make sure encryption is actually there in place, one more LU was allocated to the server: LUN 1, size of 50 MB. The logical unit was formatted and mounted as ext4 filesystem /testi/ to Linux. After mounting the filesystem, the following command was issued to write a string to a file:

- 'echo "HELLO LAMK" > /testi/hellolamk.txt'

In Figure 17, there is a print screen from the analyzer software that used to capture these FCP frames, highlighting FCID for source and destination during each exchange. First the server issues an SCSI write command to the LUN 1, to a specific Logical Block Address (LBA), destinated to virtual target with exchange ID (OX_ID) of 0x01A4. Payload and acknowledgement frames with the same OX_ID are all between the physical server initiator port and virtual target port. As seen on the right-hand side of Figure 17, payload is plain text.

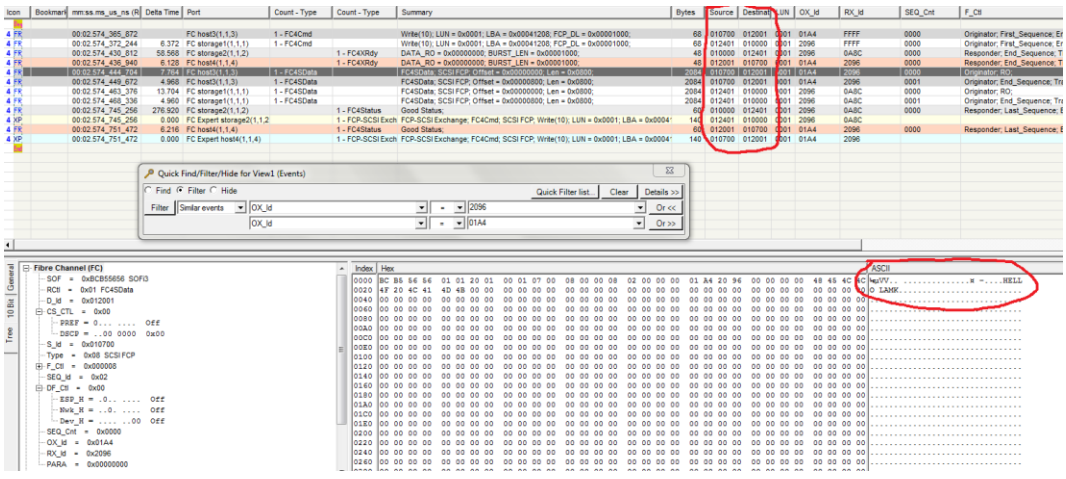

FIGURE 17. Captured frames with plain text exchange ID (0x01A4)

Payload of these ASCII characters fit in to one 2112 byte payload slot, but there is one more payload (FC4SData) frame transmitted, ending the specific sequence.

Furthermore, we can see in Figure 18 that the encryption engine encrypts the payload and sends it over from virtual initiator to physical target in sequence 0x2096. Again real source and destination FCIDs are visible in captured data, and we can also see that the same payload as we were previously able to read containing 'HELLO LAMK' -string, is now encrypted ciphertext.

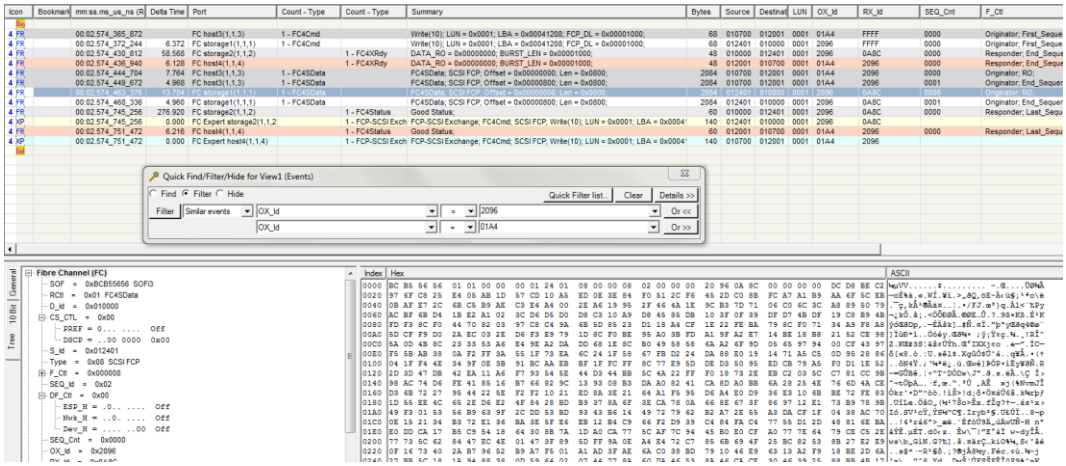

FIGURE 18. Captured frames with encrypted exchange ID (0x2096)

This test scenario proves that the frame is indeed not plaintext after the encryption engine, but whether it proves it is properly encrypted following AES256-XTS encryption algorithm is a good question and this thesis will not be able to answer this question.

## 8.4 Metadata of an encrypted Logical Unit

One more test to be done was to clone an encrypted LUN and map it to another server, outside the encryption engine context. The expected result would be that there is 32 bytes of metadata on each LBA in range 1 to 16, and LBA 0 is plaintext. The server used to read the cloned LUN data was Linux and hexdump was used to read the LUN. The crypto-target-container configuration for the LUN is displayed in the upper part of Figure 19, displaying key identification for the DEK (KEY ID) used to encrypt this specific LUN. The lower part of Figure 19 displays the results of hexdump output at around beginning of LBA1. Block size being 512 bytes, LBA 0 represents bytes 0…511 (0x000…0x1FF), LBA 1

represents bytes 512…1023 (0x200…0x3FF) and so on. So there definately is the key ID, but Brocade never revealed what the other part of the metadata actually contains. They said that it is company secret. However, as the documentation says, there is metadata on each LBA in range of 1 to 16.

```
LUN number:              0x1
LUN type:                disk
LUN serial number:       ETAPP   LUN P3/KZoBxaKB-
       60A9800050332F4B5A6F4278614B422D6F4278614B422D000A980050332F4B5A
Encryption mode:         encrypt
Encryption format:       native
Encrypt existing data:   enabled
Rekey:                   disabled
Internal EE LUN state:   Encryption enabled
Encryption algorithm:    AES256-XTS
Key ID state:            Read write
New LUN:                 No
Key ID:                  7d:55:71:88:00:32:4e:6b:2f:b2:7c:a6:36:91:dd:2a
Key creation time:       Fri Jan 18 19:54:50 2013
```

```
000001e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
00000200  6a 74 ba be 01 00 00 0e  7d 55 71 88 00 32 4e 6b  |jt......}Uq..2Nk|
00000210  2f b2 7c a6 36 91 dd 2a  fa ce 00 00 00 00 00 00  |/.|.6..*........|
00000220  d0 35 14 c3 b1 02 fc db  85 5e d9 ab 93 79 93 c5  |.5.......^...y..|
```

FIGURE 19. LU metadata on LBA 1

The last two bytes of LBA0 in Figure 19 represents boot signature in master boot sector, thus verifying that what Brocade has documented about LBA0 being always plaintext, is true.

## 8.5 WWN spoofing

There is a known exploit using FC-GS-4 spec query commands to obtain Fabric zoneset from HBA initiator. This allows the attacker to list WorldWideNames for the initiators in each zone and may allow the attacker to change its own WWN to match other server computer's WWN, thus allowing the attacker to access Logical Units visible to original WWN.

Spoofing was tried with Linux and Emulex HBA. There is a utility pack for linux called fcoe-utils, which can be used to query the zoneset. It was found out that by default SAN switch settings, Brocade did not allow queries, but Cisco MDS switches did. At the time of testing, Cisco did not have a fix for this exploit, but at

the time of writing this, the issue is fixed in Cisco NX-OS release 5.0(4b)E3 and later (Cisco support 2013).

Emulex firmware was modified to spoof WWN and tried to access LUN mapped to the server with the same WWN. On both Cisco and Brocade fabrics, the result was the same; fabric name server rejected fabric login for the attacker HBA, because the same WWN is already logged in from another FCID address. If the original server is rebooted and then the attacker tries to login to the fabric, it will be successful and the attacker is able to read data from the LUN.

QLogic HBA drivers for Linux are open-source and allow to issue fabric disconnect (FDISC) command with false source FCID to the fabric nameserver. This would make it possible to force logout from the original server and allow attacker HBA to login and capture the data from the original LUN. In the sample environment this was never tested, but it was discussed in theory. Such attack vector may exist that an attacker purchases space and SAN storage from a service provider for the attacker's own server computer that is cabable of querying SAN fabric zonesets and spoofing WWN, as well as force logout for the original server from the fabric.

# 9 SUMMARY

This thesis studied the possibility to eavesdrop a Fibre Channel Storage Area Network. In theory and practice this is fairly easy with proper equipment and access to facilities containing fibre optic cables. It is a bit more difficult when eavesdropping the traffic without breaking the optical link, but this definitely seems to be possible even though the thesis failed to prove it in practice. Real life unveilings on Verizon and NSA also speak for this, with illegal eavesdropping device found from Verizon and NSA being able to capture traffic from undersea cables.

During the eavesdropping tests it was found that a huge amount of information is revelead through SAN if an operating system is installed to a SAN attached storage. The thesis revelead the hashed root password for the installed Linux operating system, allowing brute forcing the password to cleartext without the account being locked for too many attempts. Other information, such as IP addresses, services and firewall rules are also stored with the operating system and such information may allow the attacker to find another route in and to hijack the server computer.

Spoofing the World Wide Name of a server adapter was also tested. Spoofing the WWN may allow the attacker to read data from storage logical units belonging to other server computers in the SAN. A spoofing attack seems to be possible if there is another way around to force the original server to log out from the SAN fabric, but if the original server is online and logged in to the SAN fabric, it seems all SAN switches reject the fabric login from the attacker's server adapter. Also, it is likely that a syslog event is seen by monitoring and the attacker is quickly caught.

Brocade Encryption Switch was able to encrypt data sent over the Fibre Channel network, making it impossible for the attacker to read data in cleartext. However, the first link between the server computer and BES is always cleartext, but at least the data is not sent over a long distance as plaintext.

The thesis was able to solve the question whether it is possible to eavesdrop Fibre Channel Storage Area Network; the answer is yes. Organizations that need to protect their data from being exposed to unauthorized persons should definitely encrypt all data and payloads sent over any network, including Fibre Channel SAN. The thesis was capable of proving eavesdropping on this level, one can only imagine what NSA is capable of doing with their underwater eavesdropper in a submarine.

SOURCES

Barker, R. & Massiglia, P. 2002. Storage Area Network Essentials. John Wiley & Sons Inc.

Bogdanov, A., Khovratovich D. & Rechberger, C. Biclique Cryptanalysis of the Full AES. [Ref. 13 Jan 2013]. Available: http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf

Bouchard, R. 2012. Securing fibre channel fabrics, 2nd edition. [Ref. 28 Sept 2013]. Available http://www.brocade.com/downloads/documents/books/securing-fibre-channel-fabrics-bk.pdf

Brocade. 2011. Fabric OS Administrator's Guide Support Thales Encryption Manager for Storage (TEMS) Environments. Publication #53-1002161-02.

Butler, R. 2007. Fibre Channel World Wide Names. [Ref. 5 Oct 2013]. Available: https://community.emc.com/servlet/JiveServlet/previewBody/5136-102-1-18154/WWN_Notes_v1.3.pdf

Cisco Support. 2013. [Ref. 6 Mar 2013]. Available: https://supportforums.cisco.com/thread/2143285

Donald, L. 2003. MCSA/MCSE 2003 JumpStart Computer and Network Basics. Glasgow: SYBEX

Erma, Timo 2013. RE: BES [email message]. Recipient Harri Hänninen. Sent 2 Oct 2013 [Ref. 2 Oct 2013].

Farley, M. 2001. Building Storage Networks. Osborne/McGraw-Hill.

Federal Information Processing Standards Publication, 2001, Advanced Encryption Standard. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Kingfisher international. 2013. Product catalog.

Leyden, J. 2007. Optical link hacking unsheathed. [Ref. 25 Sept 2013]. Available: http://www.theregister.co.uk/2007/04/25/optical_hacking/

Neal D. 2011, AES encryption is cracked [Ref. 12 Jan 2013]. Available: http://www.theinquirer.net/inquirer/news/2102435/aes-encryption-cracked

Tate, J., Lucchese, F. & Moore, R. 2006. Introduction to Storage Area Networks.4th edition. IBM Corp.

The New York Times. 2005. New Nuclear Sub Is Said to Have Special Eavesdropping Ability. [Ref. 20 Feb 2013]. Available: http://www.nytimes.com/2005/02/20/politics/20submarine.html?_r=0

Wikipedia. 2013. Key management [Ref. 12 Jan 2013]. Available: http://en.wikipedia.org/wiki/Key_management

Wollnik, M. 2013. Extending Data Deduplication to new workloads in Windows Server 2012 R2. [Ref. 9 Nov 2013]. Available: http://blogs.technet.com/b/filecab/archive/2013/07/31/extending-data-deduplication-to-new-workloads-in-windows-server-2012-r2.aspx

Zorpette, G. 2001. Making Intelligence Smarter, IEEE Xplore digital library. [Ref 28.09.2013]. Available: http://ieeexplore.ieee.org/ielx5/6/21038/975021/975021.html