InfoGuard
and information becomes secure

White Paper

Tapping Fibre Channel connections is much easier than commonly believed!

Version 1.0

Table of Contents

1 Tapping SAN infrastructure much easier than commonly believed

Storage area networks (SANs) are crucial for the confidentiality of company information. An experiment involving the tapping of a SAN proves that the Fibre Channel Protocol is vulnerable, too, and anything but secure, regardless of prevailing opinions to the contrary. There are simple means of obtaining sensitive information in SAN data traffic.

Huge volumes of electronic information are generated at companies year after year. Companies utilise a Storage Area Network (SAN) infrastructure to manage and store this enormous flow of data. Instead of being confined to just one location, a SAN is typically set up as two or more geographically remote SAN islands to facilitate disaster recovery. Data is generally transported between these SAN islands over high-performance fibre channels (FCs) known as interswitch links (ISL) to meet the tough quality requirements of SAN infrastructures.

1.1 A big potential risk from the data highway

Many companies in the financial, insurance, pharmaceuticals, chemistry or industrial sector encrypt their information when it is transmitted over public terrain. The same is true of public administrative agencies. But they do not do so if they mirror this data in a data centre. It is only logical that this data stream contains highly sensitive information. A company may face an existential risk unless it can absolutely guarantee the integrity, confidentiality and authenticity of this information.

It commonly known that information passing through fibre optic connections can also be tapped quite easily. Optical data theft is considered a very real danger by the Association of Manufacturers (NAM), the largest manufacturers organisation in North America. NAM even suspects the tapping of fibre optic lines to be a common method of economic espionage. According to information from the German Federal Office for Information Security (BSI), Fibre Channels are not actually tap-proof. InfoGuard shows in an impressive demonstration just how easy tapping is (refer to the information box to the right).

Nevertheless, many SAN operators classify the danger of data espionage in Fibre Channel connections as slight and consider it only a hypothetical risk. This widespread view stems mainly from the complexity of the FC protocol and from the block-based data transmission involved.

This conclusion is wrong and fatal, as InfoGuard shows in its following report on tapping Fibre Channel connections.

Known method for tapping fibre optic connections
There are various methods for obtaining information from fibre optic networks. One way is to gain access through the Y-bridges, the permanently integrated access points to a fibre optic network used by providers for trouble shooting. Data recording at these points do not influence any attenuation increase and are therefore not verifiable.
Another elegant method is to use a bending coupler. If optical fibres are bent slightly, a small percentage of the light is decoupled without damage to the fibre. Although small in percent, this light allows the entire signal to be regenerated. The fibre optic network can be accessed through the splices that are present at periodic intervals in the transition link and inadequately protected from unauthorized access.

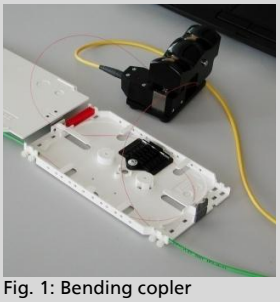


Fig. 1: Bending copler

For further information on tapping methods in fibre optic networks, please refer to the White Paper issued by InfoGuard AG. You will find it at **www.infoguard.com/download**

2 Test structure for tapping a SAN infrastructure

To show just how easy it is to launch a successful tapping attack on a SAN infrastructure, InfoGuard teamed up with storage specialist Brocade and set up a storage application scenario typical of those used at companies.

The corporate head office is connected to the remote SAN island over a dark fibre, the actual interswitch link. Data is transferred over two Fibre Channel switches. The mirrored information is stored in a far-off data centre in a disk array system comprising two SAN disks.

The tapping attack is launched against the Fibre Optic conductor by de-coupling the data packets and recording them unnoticed using a fibre channel analyzer. The analyzer is also capable of interpreting the FC protocol and concurrently logging all read and write commands from the SCSI protocol without interrupting the actual data flow.

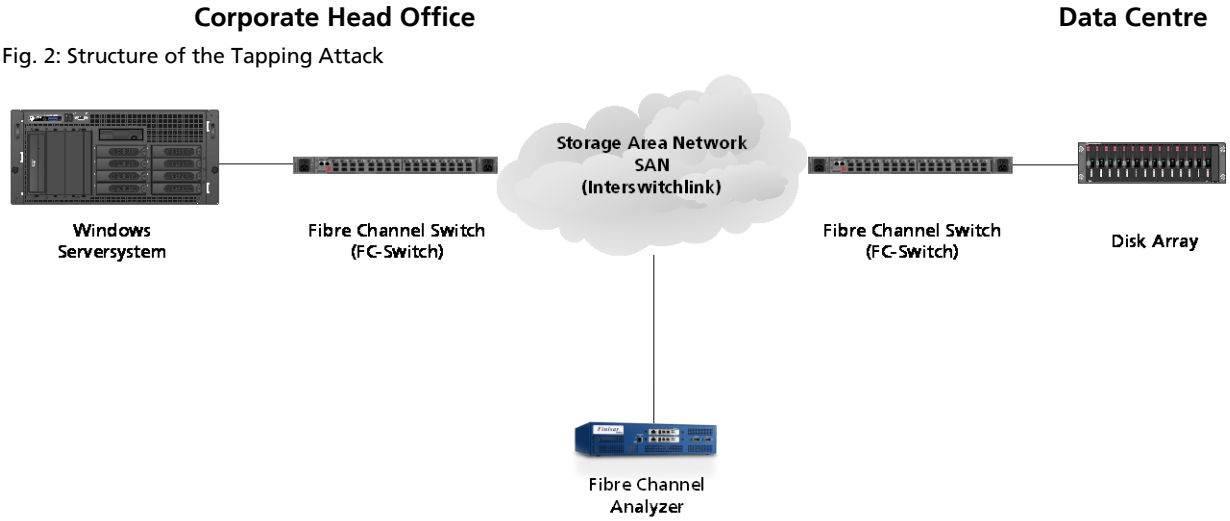


Fig. 2: Structure of the Tapping Attack

Server System

2.1 Recording Fibre Channel protocols is child's play

To record initialisation commands between the server at the head office and the external SAN disks, the recording function of the FC analyzer is started prior to the boot of the server at the head office. We created a file with confidential salary information and personal data on the data server at the head office and saved it on the external SAN disk in order to simulate the actual data theft. Data being transferred is concurrently recorded by the FC analyzer. Consequently, all relevant information is recorded and available for analysis.

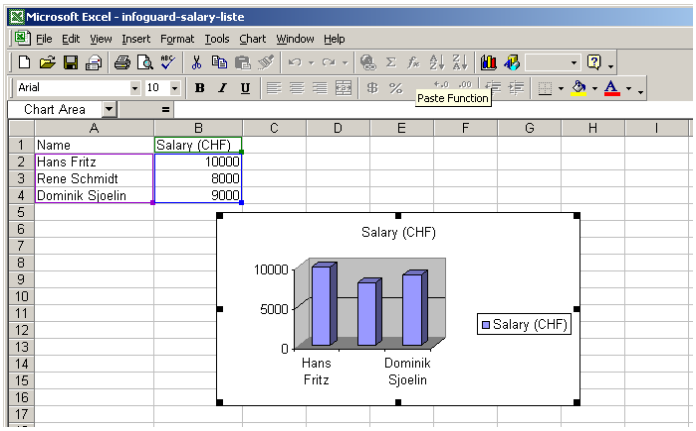


Fig. 3: Original file with salary information and personal data

Data becomes information

The recorded data flow between the head office and the SAN island contains all read and written data blocks as well as all SCSI commands with references to logical block addresses. Even without additional analysis software, readable information in plain text is recognisable on the analyzer within the FC frames. Along with the file name, this information includes, inter alia, text-based portions such as a person's name and salary from the content of the file itself.

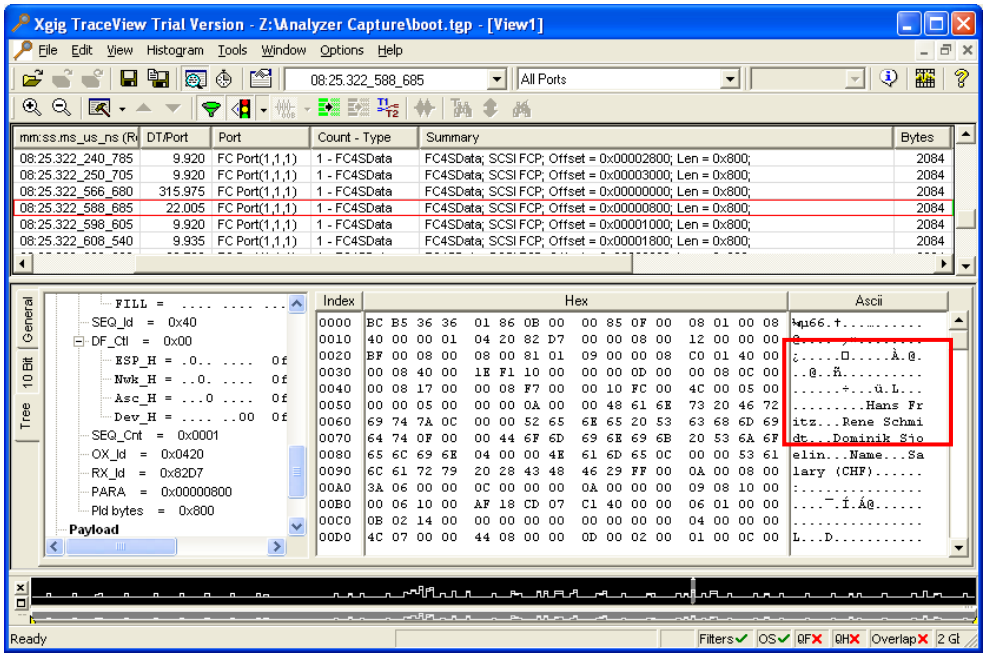
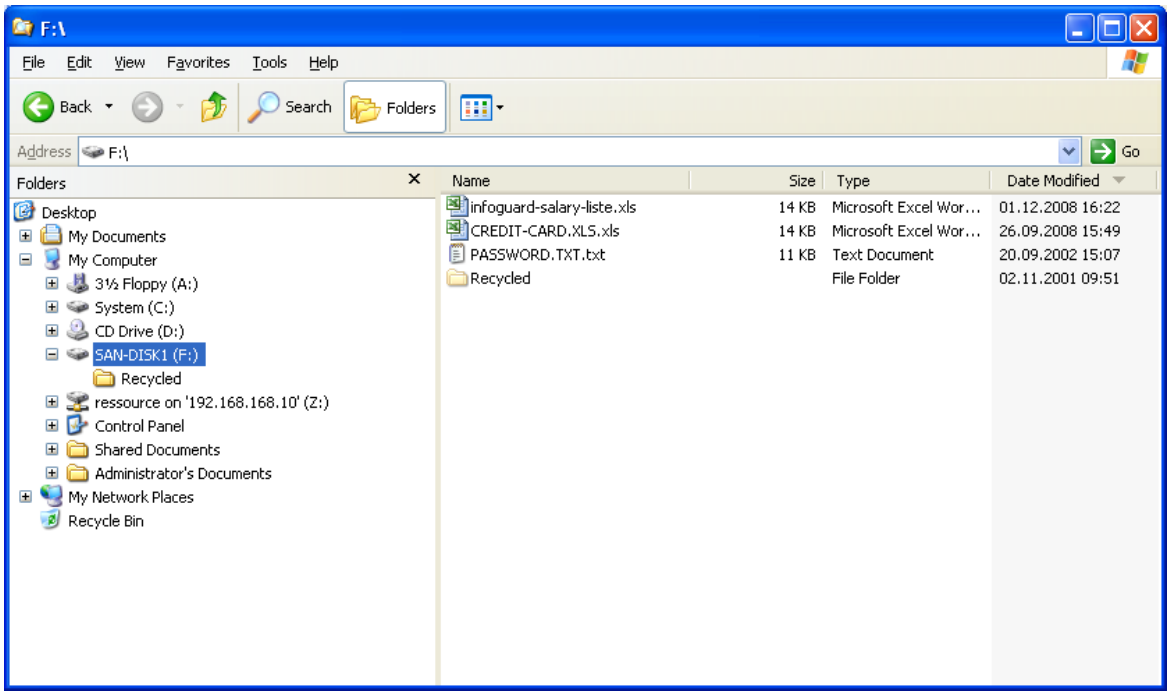


Fig. 4: Tapped and Recorded Fibre Channel Data

To convert the recorded data into a completely readable file, the data is exported from the FC analyzer to a CSV file and converted to a binary file using a simple, self-written Perl script. When recording the data traffic, we also logged all read accesses to the external SAN disk. Drawing on this information, we were then able to create a virtual replication of the SAN disk on a standard commercial laptop with ease, a replication comparable to the kind of image used for computer installation. Reproduction of the original SAN disk was born!
A double-click on the replicated file on our "hacker PC" confirmed that the entire content was concurrently recorded, including all sensitive information.

Fig. 5: Reproduction of the original SAN disk on the "hacker PC"



This simple tapping demonstration shows that the Fibre Channel protocol is also vulnerable to tapping, not just the commonly used Ethernet Protocol. Account numbers, credit-card numbers and other highly sensitive information is rendered readable merely through an analysis of FC frames, without even resorting to any special evaluation software.

Moreover, entire SAN infrastructures can be reconstructed as described above with the suitable tools and IT skills. This demonstration is powerful proof that **the confidentiality of data transmitted over public terrain in SAN networks is by no means assured.**

3 Encryption as a means of protecting SAN infrastructures

Companies sending sensitive data over fibre optic connections must be aware of this risk and provide reliable protection against it. SOX, PCI-DSS, Basel II, data protection and a number of other sets of regulations demand that such action be taken. Compliance with legal requirements is important and indispensable. There is no question: Encrypting data with special high-performance encryption solutions is ultimately the only way to provide secure, reliable protection for each SAN infrastructure.

InfoGuard is the leading manufacturer of Layer 2 encryption solutions. Our company belongs to the Swiss-based Crypto Group, one of Europe's largest and most esteemed ICT security companies, with over 300 employees. Consequently, our customers benefit in 130 countries worldwide from more than 55 years of experience and continuity in ICT security. Encryption solutions from InfoGuard afford fully secure information exchange in MAN, WAN and SAN networks with 100% encryption throughput and minimal latency times in the microsecond range. They are therefore ideal for use in SAN infrastructures. Data is encrypted using the Advanced Encryption Standard (AES) with a key length of 256 bits. As a Swiss company, InfoGuard is synonymous with top product quality and with absolute independence in the implementation of your security functions. For this reason, we develop and produce all products in-house in our Swiss facilities.

InfoGuard Multilink Encryption – InfoGuard MG10 – is the world's first multilink and multiprotocol unit to allow high-performance encryption with minimal latency time for the secure transmission of business-critical information. Up to ten different Ethernet, Fibre Channel and FICON connections can be transmitted over a single link. Different connections and protocols can be combined to attain a transmission speed of 10 Gbps, making the platform a universally applicable encryption solution that is both scalable and flexible.

Fig. 6: InfoGuard MG10

- Flexible, cost-efficient encryption for Ethernet, Fibre Channel and FICON connections
- Transmits up to ten different signals over an STM-64/OC-192 connection
- Supports Gigabit Ethernet, 1/2/4 Gbps Fibre Channel and 1/2/4 Gbps FICON
- Key generation with random generator hardware and distribution utilising security card or inter-unit management
- Automatic key change after configurable time interval without link interruption
- Audit and event logging
- MTBF > 50,000 hours, with dual hot-pluggable power supply and cooling system