InfoGuard

and information becomes secure

Whitepaper

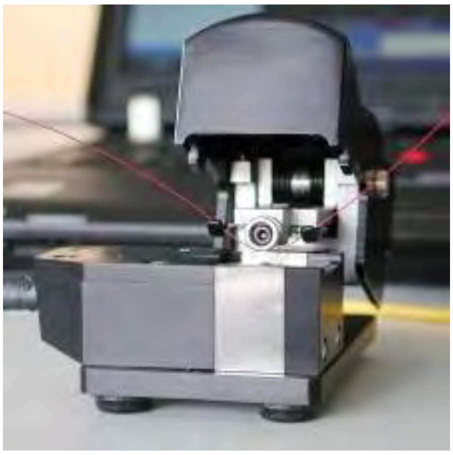
THE 7 Security Myths Surrounding Fibre Optic Networks

Version 1.0

1 Fibre optic networks – security myths and reality

State-of-the-art fibre optic networks are used to interconnect different sites in towns and cities (MAN), to link sites nationwide (WAN) and they also form the backbone for backup and disaster recovery infrastructures (Storage Area Network, SAN). And it is just here that they are easy prey for white collar criminals. In the latest study IDC (Fiber - Optic Networks: Is Safety Just an Optical Illusion?) is of the opinion that there is an urgent need to act in protecting data in fibre optic networks.
"For a long time fibre optic cable networks were deemed to be the most secure way to transport data between different networks … this reputation has turned out to be false", says IDC analyst Fouchereau. The study highlights several examples of tapping into fibre optic networks such as the attacks on Verizon or Deutsche Telekom networks. The largest North American industrial trade association – the National Association of Manufacturers (NAM) has also come to a similar risk assessment. According to NAM, tapping into fibre optic cables is a widespread method of industrial espionage; an opinion that is also shared by the German Federal Office for Information Security (BSI). In spite of all this, there are seven stubborn myths that simply won't go away.

1.1 Myth 1 – Data in fibre optic cables are safe from eavesdropping



An easy target are the network operators' distribution boxes, which are used for maintenance work and linking the individual fibre optic cables. If unauthorised persons gain access to these unprotected maintenance facilities it is very easy to record and analyse the unencrypted data stream using a bending coupler. Bending couplers are part of the standard equipment used by maintenance technicians to test the state and function of the optical fibre. As this method of attack has very little impact on network operations the attempt at eavesdropping generally goes unnoticed.
Other even more sophisticated techniques, which avoid direct contact with the data cable, cannot be detected at all. This method of attack exploits the fact that a minimum amount of light radiates naturally from every cable – even without having to bend the optical fibre. Sensitive photo-detectors capture this Rayleigh scattering and amplify it.

The interpretation of the data is accomplished by data and spectral analysers which, uses specific criteria to record, monitor and analyse the data in real time.
Detailed information on this subject can be found in our Whitepaper "Risks and Dangers of Fibre Optic Cables by visiting **www.infoguard.com/download**

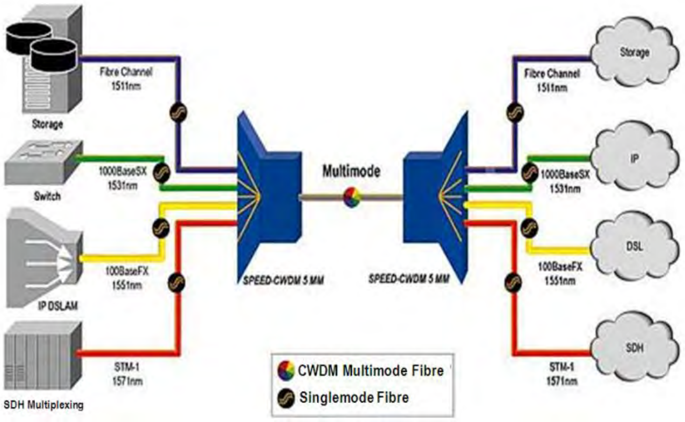
1.2 Myth 2 – The volume of data is too great for a targeted attack

Contrary to widespread opinion, large volumes of data alone provide no protection. In order to extract specific information from large amounts of data, corresponding IP numbers or keywords are sufficient.
Packet Sniffer programs are able to filter out the information required from the data streams which are then stored in real time. A packet sniffer is a program that records, monitors and analyses network data.

According to an AT&T paper published in 2002 and numerous well documented and publicized events, it is clear that systematic eavesdropping over fibre optic networks has become reality. In different cities across the USA, secret rooms have been set up allowing National Security Agents to monitor public as well as corporate networks administered by AT&T. The data analysis was undertaken using commercial products which, at the time, could analyse data traffic up to a transmission speed of 10Gbps – regardless of whether Ethernet, Fibre Channel / FICON or SDH / SONET traffic was involved.

1.3 Myth 3 Data in WDM networks cannot be analysed

A further myth is the reputed security of data in a WDM network (Wavelength Division Multiplexing). To optimise the transmission bandwidth the data streams in an optical fibre are transmitted in different spectral colours. This enables several channels to be transmitted simultaneously on a single optical fibre thus allowing the bandwidth capacity to be greatly increased and resulting in cost-effective use.

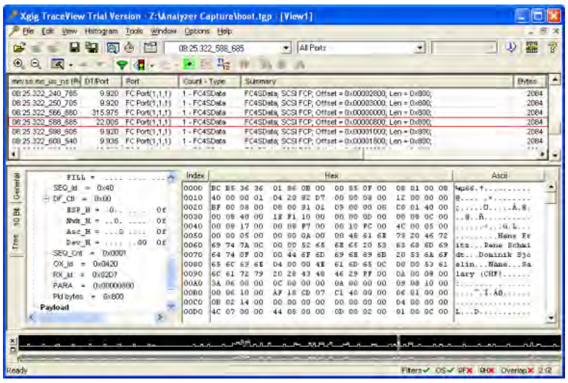


Thanks to this additional complexity and still larger volumes of data many users of WDM technology are lulled into a false sense of security. The truth is that the complexity, using multiplexers, is only marginally increased as the separation of these individual channels presents no problem to spectrum analyser and optical filters (tuneable or fixed). Subsequent data analysis, as mentioned previously, is easily achievable.

1.4 Myth 4 – The Fibre Channel protocol is too complex and thus secure

In order to manage and store the enormous flood of data companies take advantage of Storage Area Network (SAN) infrastructures. Based on disaster recovery considerations an infrastructure of this nature comprises two or more geographically separate SAN islands, which are interlinked to one another via a Fibre Channel network.

The widespread assumption that FC data contain no interpretable and readable information is mainly based on the complexity of the FC protocol and the block-based data transmission. To prove that successful eavesdropping over a SAN infrastructure presents no problem, InfoGuard in conjunction with the SAN specialist Brocade, undertook an exercise to tap into such a network.


Xgig TraceView Trial Version - Z:\Analyzer Capture\boot.tgp - [View1]
File Edit View Histogram Tools Window Options Help
08:25.322_588_685
All Ports
General
10 Bit
Tree
Ready
Filters✓ OS✓ SF✗ SH✗ Overlap✗ 2 G

```
mm:ss.ms_us_ns (R  DT/Port  Port            Count - Type  Summary                                                Bytes
08:25.322_240_785    9.920  FC Port(1,1,1)  1 - FC4SData  FC4SData; SCSI FCP; Offset = 0x00002800; Len = 0x800;  2084
08:25.322_250_705    9.920  FC Port(1,1,1)  1 - FC4SData  FC4SData; SCSI FCP; Offset = 0x00003000; Len = 0x800;  2084
08:25.322_566_680  315.975  FC Port(1,1,1)  1 - FC4SData  FC4SData; SCSI FCP; Offset = 0x00000000; Len = 0x800;  2084
08:25.322_588_685   22.005  FC Port(1,1,1)  1 - FC4SData  FC4SData; SCSI FCP; Offset = 0x00000800; Len = 0x800;  2084
08:25.322_598_605    9.920  FC Port(1,1,1)  1 - FC4SData  FC4SData; SCSI FCP; Offset = 0x00001000; Len = 0x800;  2084
08:25.322_608_540    9.935  FC Port(1,1,1)  1 - FC4SData  FC4SData; SCSI FCP; Offset = 0x00001800; Len = 0x800;  2084
```

```
    FILL = .... .... ...
  SEQ_Id = 0x40
⊟ DF_Ctl = 0x00
    ESP_H = .0.. .... 0f
    Nwk_H = ..0. .... 0f
    Asc_H = ...0 .... 0f
    Dev_H = .... ..00 0f
  SEQ_Cnt = 0x0001
  OX_Id = 0x0420
  RX_Id = 0x02D7
  PARA = 0x00000800
  Pld bytes = 0x800
Payload
```

```
Index  Hex                                                  Ascii
0000   BC B5 36 36  01 86 0B 00  00 85 0F 00  08 01 00 08   ¼µ66.†..........
0010   40 00 00 01  04 20 82 D7  00 00 08 00  12 00 00 00   @.... .×........
0020   BF 00 08 00  08 00 91 01  09 00 00 08  C0 01 40 00   ¿.....'.....À.@.
0030   00 08 40 00  1E F1 10 00  00 00 0D 00  00 08 0C 00   ..@..ñ..........
0040   00 08 17 00  00 08 F7 00  00 10 FC 00  4C 00 05 00   ......÷...ü.L...
0050   00 00 05 00  00 00 0A 00  00 48 61 6E  73 20 46 72   .........Hans Fr
0060   69 74 7A 0C  00 00 52 65  6E 65 20 53  63 68 6D 69   itz...Rene Schmi
0070   64 74 0F 00  00 44 6F 6D  69 6E 69 6B  20 53 6A 6F   dt...Dominik Sjo
0080   65 6C 69 6E  04 00 00 4E  61 6D 65 0C  00 00 53 61   elin...Name...Sa
0090   6C 61 72 79  20 28 43 48  46 29 FF 00  0A 00 08 00   lary (CHF)......
00A0   3A 06 00 00  0C 00 00 00  0A 00 00 00  09 00 10 00   :...............
00B0   00 06 10 00  AF 18 CD 07  C1 40 00 00  06 01 00 00   ....¯.Í.Á@......
00C0   0B 02 14 00  00 00 00 00  00 00 00 00  04 00 00 00   ................
00D0   4C 07 00 00  44 08 00 00  0D 00 02 00  01 00 0C 00   L...D...........
```

The attempt at tapping was carried out using a bending coupler on the fibre optic cable. The data packets were decoupled and recorded unnoticed with a fibre channel analyser. In addition the analyser logged and recorded all the read and write commands of the SCSI protocol without compromising the actual data stream. Even without additional analysis software readable information could be identified in plain text on the analyser within the intercepted FC frames. With the help of a simple script the recorded data could be converted to a complete virtual disk allowing us to make a full copy of the disk array.

The detailed findings can be found in our Whitepaper "Tapping Fibre Channel connections is much easier than believed", by visiting **www.infoguard.com/download**

1.5 Myth 5 – A dedicated dark fibre is secure

Many users of "dedicated" dark fibre links have the feeling that there is no risk of a tapping attack. They tend to forget that the term "dedicated" only applies to the transmitted data and not the infrastructure. In many cases dark fibre connections will run accross public domain and will therfore be provided and maintained by a third party provider and a that 'their' dark fibre link will also be physically routed via the ISP distribution box (see myth 1).

These communication links not only pose the same risks as a managed service but make it even easier for a hacker to obtain the desired information as the link only transmits data from a dedicated customer.

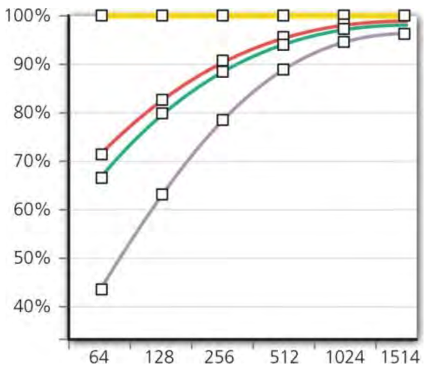
1.6 Myth 6 – By monitoring signal loss every attack can be identified

Monitoring the fibre optic cable in terms of characteristics, such as attenuation loss, is a common method for measuring the availability and quality of the communication line. Very often, there is the feeling that tapping into a fibre optic cable causes sufficient attenuation to make it identifiable by an optical monitoring tool. The conclusion is then drawn that monitoring the fibres offers sufficient and secure protection.

But how great is this degradation in reality? Optical monitoring tools have a tolerance of between 0.5 and 1dBm, so that they are resistant to laser disparity, temperature variations and other outside influences. As long as the disturbance lies within the tolerance the attack will certainly not be noticed. If, for example, a Y-bridge or a bending coupler is installed in the network the loss will be added to the reference value and will not attract attention. Moreover, professional bending couplers, which are used for espionage purposes, clearly display attenuation of less than 0.5dB. Not to be forgotten are the state-of-the-art tapping methods based on "non-touching" technology that insert no additional line loss whatsoever.
Taking these aspects into account and although it is certainly advisable to optically monitor the fibre optic cable which provides a permanent record of their quality and status, **no guarantee for the confidentiality of the data can be assumed.**

1.7 Myth 7 – Encryption causes performance and latency problems

In order to secure the exchange of digital information, IPSec was the most popular form of transmission technology up until a few years ago. IPSec transmissions run over network layer 3 of the OSI model which, unfortunately, has a negative impact on performance and throughput.



The IPSec protocol inflates small data packets to almost twice their size and thus causes an increased amount of traffic in the encrypted data tunnel. An IP packet having an original size of 64 bytes is enlarged by an additional overhead of 57 bytes. Even in the most favourable scenario IPSec-based encryption of larger packets only uses 90 percent of the available bandwidth. The negative effect has a huge impact because 65 percent of worldwide IP traffic consists of small 64 and 128 byte data packets. As a result of the fragmentation and greater computing effort the latency also increases. Data transmission in virtual real-time and without loss of bandwidth is nevertheless possible when the data packets are encrypted at the data link layer (layer 2) of the OSI model. In contrast to layer 3 encryption the coded single packets do not require an additional header for layer 2 encryption so that unnecessary data ballast, and the resulting performance and latency problems, can be avoided. This enables the available bandwidth to be almost fully utilised (> 99.9 %!).

In addition, layer 2 encryption reduces the level of complexity and thus cuts down considerably on the operating and administrative effort.
Thus the myth surrounding performance and latency degradation for layer 3 encryption is true – **but does not apply to the layer 2 approach!**

2 Reliable protection thanks to Layer 2 encryption

For all these reasons the protection of information, even when using optical networks, is vital and can be undertaken without restriction. InfoGuard is the leading manufacturer of layer 2 encryption solutions. These offer all-round and secure information exchange in MAN, WAN and SAN networks with 100% encryption throughput and minimum latency. Thus they are suitable for use in heavily utilized links and for time-critical applications. Data encryption is undertaken by the Advanced Encryption Standard (AES) with a key length of 256 bits.

As a Swiss company, InfoGuard stands for the highest quality of its products and complete independence in the implementation of its security functions. For this reason, we develop and manufacture all our products in-house in Switzerland.

Ethernet Layer 2 Multipoint Encryption

InfoGuard EGM / EG1M / EG10M

- Layer-2 Ethernet Encryption with AES 256 Bit
- 100% encryption performance from 20 Mbps / 100 Mbps, 200 Mbps / 1 Gbps to 2 Gbps / 10 Gbps
- Minimal latency in microsecond range
- Easy to integrate (bump-in-the-wire) in point-to-point, point-to-multipoint and multipoint-to-multipoint Ethernet networks
- Encrypts unicast, multicast and broadcast and supports class of service
- Separate encryption key for each peer unit
- Secure investment thanks to optional upgrades

Ethernet Layer 2 Link Encryption

InfoGuard EG1 / EG10

- Point-to-point Layer-2 Ethernet Encryption with AES 256 Bit
- 100% encryption performance for up to 10Gbps
- Minimal latency in microsecond range
- Easy network integration (bump-in-the-wire)

Multilink / Multiprotocol Encryption

InfoGuard MG10 / MG4 / MG10S

- Flexible and cost-efficient data encryption using AES 256 Bit for Ethernet, Fibre Channel, FICON und E1 connections
- 100% encryption performance for up to 10Gbps
- Minimal latency in microsecond range
- Transmits up to ten different signals via CWDM, DWDM, Dark Fibre or SDH networks
- Supports Gigabit Ethernet, 1/2/4/8 Gbps Fibre Channel and FICON

SONET/SDH Encryption

InfoGuard SG3 / SG12 / SG48 / SG192

- Point-to-point Layer 1 SONET/SDH data encryption using AES 256 Bit
- 100% encryption performance for up to 10Gbps
- Minimal latency in microsecond range
- Easy network integration into existing STM SONET/SDH networks

All InfoGuard encryption devices are developed and manufactured in Switzerland

As a member of the Swiss "The Crypto Group", one of the largest and renowned ICT security companies in Europe with over 300 employees, customers in 130 countries worldwide benefit from more than 55 years of experience and continuity in information security.