IDQ
FROM VISION TO TECHNOLOGY

REDEFINING SECURITY

ID Quantique White Paper

FIBRE OPTIC NETWORKS: YOUR WEAKEST LINK?

Version 1.0

March 2011

ID Quantique SA
Chemin de la Marbrerie 3

1227 Carouge/Geneva
Switzerland

T +41 22 301 83 71
F +41 22 301 83 79

info@idquantique.com
www.idquantique.com

Table of contents

ID Quantique SA
Ch. de la Marbrerie, 3
1227 Carouge
Switzerland

Tel: +41 (0)22 301 83 71
Fax: +41 (0)22 301 83 79
www.idquantique.com
info@idquantique.com

1. Introduction

Information lies at the heart of every organisation – be it banks dealing with credit cards and personal records, governments dealing with state information or simply companies with their own trade secrets and intellectual property. Since information is so vital for the growth and survival of a company, it comes with the added responsibility of ensuring its confidentiality, integrity and availability.

The risk a company faces due to loss of information is often underestimated. Not only does it mean loss of revenue and damage to the company brand, but also additional legal liabilities, loss of customer trust and loss of shareholder confidence.

According to the Ponemon Institute/ Symantec[1], the cost to US corporations of a data breach has grown to $214 per compromised record, or an average of $7.2 million per breach. In 2010, for the first time, malicious or criminal attacks were the most expensive cause of data breaches. The world-wide average in 2009 was $3.43 million per breach or $142 per compromised record. Analysts believe that the global costs will increase to US levels as data protection laws in more countries mandate public disclosure of data breaches. In addition, the 2010 Global Fraud Report by Kroll[2] states that for the first time in 2010 the theft of information and electronic data overtook physical theft as the most frequently reported fraud (27% of respondents).

However, today many organizations still have a false sense of security about the data on their network. Here are some of the myths that are still prevalent:

- Fibre optic is inherently secure
- Dark fibres provided by carriers are secure
- Data is protected by volume
- WDM networks cannot be tapped

This paper discusses the vulnerabilities of networks, including those of fibre optic technology, and proposes simple and cost-effective solutions to counter these threats.

2. Vulnerability of Fibre Optic Networks

2.1 Understanding the Evolving Threat Landscape

For years it has been public knowledge that ethernet networks using copper cables are easy to tap or probe without even physically accessing the wires. The electro-magnetic field associated with the signal extends outside the cable, which allows easy data interception without disrupting the communication. The US Navy and National Security Agency (NSA) were already employing this method to tap communications in Operation Ivy Bells during the cold war[3].

However, optical fibres are still considered inherently secure by many organizations as the light transporting the data remains within the cable. They believe that it is difficult to access fibre optic cables as they are located within a protective covering below ground, and that any tap would create enough disturbances to be noticed by the network administrator. This false belief has been aggravated by major telecom companies which in many cases still sell dark fibre at a premium as a security option.

As early as 2003 John Pescatore, VP of Security at the Gartner Group and a former NSA analyst, stated in an interview to Computerworld:

“Tapping a fibre-optic cable without being detected, and making sense of the information you collect isn’t trivial but has certainly been done by intelligence agencies for the past seven or eight years… These days, it is within the range of a well-funded attacker,

[1] Ponemon/Symantec *2010 Annual Study: US Cost of a Data Breach*

[2] Kroll 2010 *Global Fraud Report (Economist Intelligence Unit Survey Results)*

[3] http://en.wikipedia.org/wiki/Operation_Ivy_Bells

probably even a really curious college physics major with access to a fibre-optics lab and lots of time on his hands" [4].

Nowadays it takes equipment costing under €500, about 10 minutes for the tap installation and some persistence in finding the optical fibre in the right manhole.

2.2 How Optical Fibre Networks work

Before discussing the technical details of attacks on optical fibre networks, it is important to understand the basics of the technology and how it works.

An optical fibre is a fine thread of glass used to guide light in order to transmit signals. It consists of a central region, also known as the core, surrounded by a cylindrical region called the cladding. Impurities are deliberately added in the glass that forms the core of the fibre, in order to increase its index of refraction and to ensure that light injected into the fibre remains within the fibre and is guided along its axis. This phenomenon is called total internal reflection. A plastic coating that protects the fibre from damage and moisture normally surrounds the cladding.

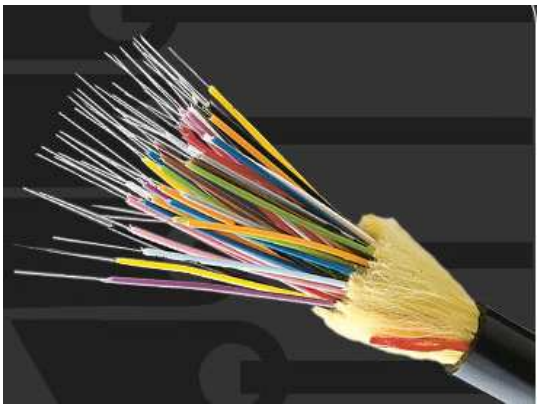


Figure 1: Fibre optic cable section

[4] The US have built submarines with the capability of tapping and splicing undersea fibre optic cables, such as USS Jimmy Carter (SSN-23), commissioned in 2005.

An optical fibre can carry many independent channels, each using a different wavelength (or color) of light. This approach is known as wavelength-division multiplexing (WDM) and increases the bandwidth supported by the fibre.

With the ever-increasing demands on enterprise networks today, fibre optic technology is in great demand. The technical resourcefulness of fibre optic networks is unsurpassed by any other telecommunication technology. They support higher bandwidths, provide better performance, can be deployed over longer distances, are cost effective and are easy to upgrade.

2.3 Optical Fibre Network Tapping Techniques

However, optical fibre has no inherent protection – in fact it is an ideal target for an assailant, as it normally carries a large volume of data - often highly sensitive - between the company and its adjoining buildings or disaster recovery center. And since optical taps are cheap and detecting interception is extremely difficult, it gives a high return on investment for any hacker.

Optical fibre network tapping techniques are:

Passive: They do not raise suspicions that the end party is being attacked.

Safe: They do not leave any traces pointing to the assailant.

Cheap: Tools to tap optical fibre networks are available at very affordable rates.

2.3.1 Coupler Splice-In

This is the simplest and most primitive method of tapping into a fibre optic cable. Here, the fibre optic cable is cut and a coupler is spliced in such a way that the signal continues to the intended party whilst being eavesdropped by the attacker.

A coupler is a standard optical component, which can be purchased online and which splits the optical signal transmitted on an optical fibre to two output fibres. They exist with different splitting ratios. Typical values are 50/50, 10/90 and 1/99. Adjustable ratio couplers

also exist. Couplers with high asymmetry (eg: 1/99) are also called “optical taps” and are sometimes installed by telecom operators to monitor their links by measuring a small fraction of the signal, without affecting the performance of their customer network.

Coupler :
1 fibre in
2 fibres out

Figure 2: Coupler Splice-in

It should be noted that the Coupler Splice-In method causes the link to go down momentarily, which would normally trigger an alarm. However, a well-trained technician could splice a coupler in a fibre link in less than a minute, causing only a brief interruption which may be attributed to environmental phenomena or a normal network glitch. Moreover, since most carriers have pre-installed splice points on their networks for maintenance purposes these would be the natural point of attack.

2.3.2 Fibre Bending Coupling

A fibre optic cable guides light correctly as long as it is not bent with a radius under 5-10 millimeters. Bending the fibre to a smaller radius would ensure that light leaks out, as the total internal reflection condition is no longer fulfilled. This light can then be captured and converted to an electrical signal.

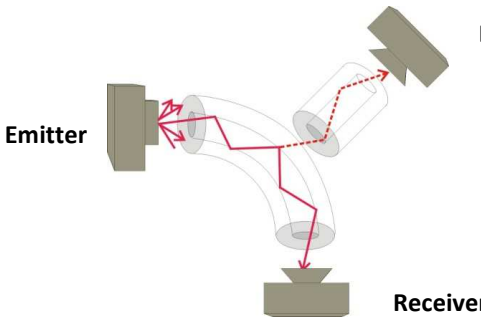


Figure 3: Fibre Bending Coupling Concept

Devices developed for this purpose are called clip-on couplers, and can be purchased easily and cheaply. The clip-on coupler is clamped onto the fibre and the signal extracted is passed to another fibre. It is not even necessary to remove the outer protective covering of the fibre. Operators normally use such devices to check fibre connectivity, but nothing prevents a malevolent party from using them for data interception.

This kind of tap requires only trivial manipulation taking less than 10 minutes, and it generally goes unnoticed, as there is no link interruption, and very moderate insertion loss. Through capturing only a small percentage of the light, a hacker can obtain 100% of the information.

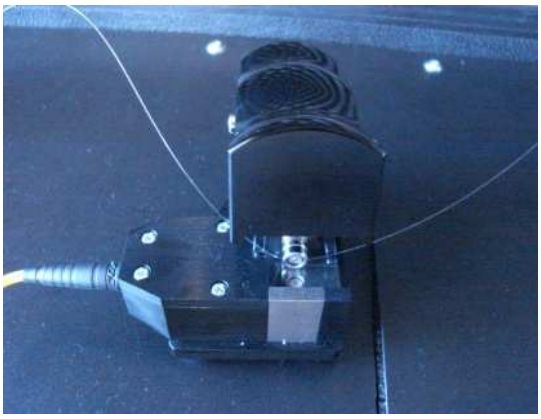


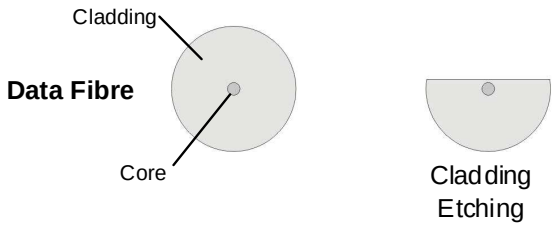
Figure 4: Fibre Bending Coupling

2.3.3 Evanescent Coupling

Earlier in this paper we discussed how optical fibres seemed secure as the light is confined within the fibre. This is true, but although most of the signal lies in the core of the fibre, a fraction of the light is also extended into the cladding. This fraction of light is called the evanescent field. Removing the fibre coating and a part of the cladding without touching the core would enable an attacker to access the evanescent field and eavesdrop on the line. For a skilled technician, the whole process would take approximately one hour to complete.

There are several ways for the removal of the cladding on the fibre. Chemical etching with hydrofluoric acid or mechanical polishing of the fibre are but a few of the known techniques. Once the fibre has been etched off, a second fibre that is similarly etched is placed above the first fibre, to pick up the evanescent field necessary for signal collection. The coupling ratio here would depend upon the distance between the two cores. Apart from being totally undetectable, evanescent coupling has many other advantages such as:

- No link interruption
- Adjustable coupling ratio
- Very low excess loss[5]



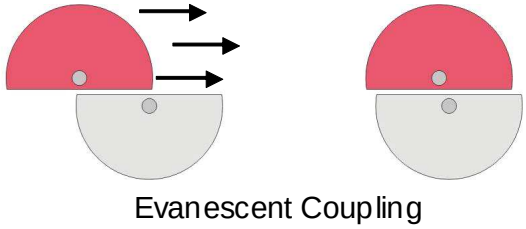


Figure 5: Evanescent Coupling

3. Network Security Myths

Many of the security myths listed below are still actively propagated by telecom carriers and manufacturers of WDM equipment. In some cases ambiguity is deliberately enhanced with phrases concerning "security" or "protection" of the infrastructure, without specifying what this actually means.

Myth 1: Optical fibre networks or dark fibres are inherently safe

As indicated above, optical fibres can be intercepted with relative ease once they are accessed, and there is no inherent security for data travelling inside a fibre. However, dark fibres are often still left unencrypted or otherwise unprotected in the belief that they are safe or physically protected.

Fibres are bundled in cables, which sometimes include a metal covering to give physical resistance and prevent access to the fibre strands. However, these cables are rolled on a large reel during production, and the reels cannot accommodate more than a few kilometers of the bulky cable. This means that the sections of cables must be spliced together in the field. The splices are then located in chambers and cabinets placed in manholes along the roadside or train tracks.

[5] Excess loss is the amount of light extracted from first fibre but not coupled into second fibre

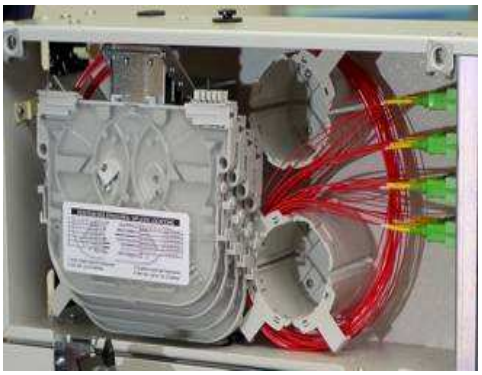


Figure 6: Splice Box

The spliced fibres are readily found in manholes where the naked fibre can easily be intercepted. ID Quantique tested the ease of accessing optical fibres in manholes in Geneva, Switzerland, in March 2011. With the aid of a fluorescent jacket & hard-hat (purchased for under €20) ID Quantique employees posed as workmen, and were able to locate and open manholes containing crucial optical fibres after only 30 minutes search in the center of town[6]. There are reported cases of vandals attacking fibre network cables through manholes[7], and the list of network data breaches is too long to enumerate[8]. These numbers will only increase with the adoption of mandatory disclosure laws in more countries.

The telecom station is another area where the fibre networks are easily accessible. Optical fibres typically do not run directly from one facility to another, but via a local telecom station and from there to one or several telecom stations before reaching the end facility. While telecoms stations are normally well protected through physical access controls, recent trends of outsourcing network installation and deregulation, where incumbent telecom operators are forced to open up their stations to external companies, mean that it is increasingly difficult to secure and track access. Assailants are able to gain access to stations – sometimes they are even insiders[9]. At any rate, the data owner has no control and no visibility on who has access to the telecom station.

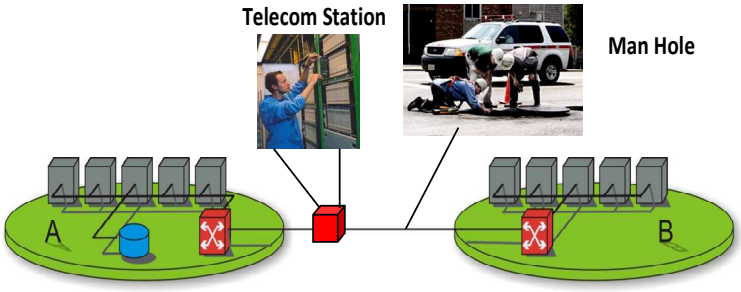


Figure 7: Physical Security of Optical Fibre Networks: A Myth

Myth 2: Data is protected by volume

It is often assumed that the bit rate of a modern telecommunication network is so high that it is practically impossible to intercept and analyse live traffic, that valuable information is masked by the quantity of irrelevant traffic.

This is a misconception – mainstream network analysers have the capability to capture and process

[6] The video of locating fibres in manholes and the process of fibre optic tapping is provided upon request from info@idquantique.com

[7] "Vandals chop fibre-optic cables & killed landlines, cell phones & Internet service for tens of thousands of people" (9th April 2009) http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/04/09/BAP816VTE6.DTL&tsp=1

[8] Data breaches are now tracked on sites such as www.datalossdb.org, www.privacyrights.org www.databreaches.net, and numerous others. The lists extend to hundreds of pages.

[9] "Terry Childs, the system administrator in jail awaiting trial for holding San Francisco's fibre-optic WAN hostage in July 2007, continues to darken the lives of members of the city's IT dept": http://www.internetnews.com/government/article.php/3771256/Rogue+Sys+Admin+Still+Haunts+San+Francisco.htm

traffic up to maximum bandwidth. Intercepted traffic can also be stored in bulk for offline analysis.

Myth 3: WDM networks cannot be tapped

Wavelength Division Multiplexing (WDM) is a technique that increases the bandwidth of an optical fibre by multiplexing several wavelengths, such that each wavelength would correspond to a separate channel carrying different signals. The traditional assumption is that an eavesdropper would not be able to separate the channel of interest.

Figure 8: Spectral filters and analysers used to demultiplex the signal

This again is a myth, as nothing prevents an eavesdropper from having the same equipment to demultiplex the signal as the intended recipient of the information. Also, the tapping methods discussed above have the capability to extract all the channels from an optical fibre. Advanced filters are also available in the market (at about €100) to block all but one channel, enabling an eavesdropper to select the right wavelength for convenient interception.

4. Security Solutions

4.1. Attenuation Monitoring

Optical signals suffer from minor degradations as they travel through the fibre. This is usually caused by scattering and absorption of light across the length of the fibre and is known as attenuation. Devices to check the attenuation of signal in an optical fibre are available and can be used to check if there are alterations in the predetermined intensity of the signal. Any alteration in the attenuation could then be detected.

While some disturbances in the network could potentially be detected by such a system, such as the placing of a tap with a clip-on coupler, it also has many limitations:

- It would be unable to detect an evanescent coupling tap.
- It would be unable to detect a coupler that has already been placed on the optical fibre network before its commissioning.
- To detect most types of interception the signal attenuation limits would have to be set at paranoid levels. This would result in frequent false positives, to the extent that a routine technical check would be sufficient to trigger an alarm.
- In reality it is common practice that, once a line is established and working, the network engineer does not bother to actively monitor it as there are other priorities to attend to.

4.2. Securing Networks through Encryption

The only certain method for protecting sensitive data on the network is through encryption. Encryption encodes plain text, such as credit card details, with an

encryption key to transform it into ciphertext. This ensures that only the authorised receiver with the key is able to decode the information. The leading standard for data encryption is the Advanced Encryption Standard (AES) which supports key sizes of 128 to 256 bits. State of the art encryption recommends a 256-bit key length.

Today the encryption of sensitive or personal information is mandated in several industries, and compliance with these regulations is subject to frequent audits. Regulations such as the Payment Card Industry Data Security Standard (PCI DSS), The Health Insurance Portability and Accountability Act (HIPAA), EU Data Privacy Directive, and others are the primary drivers for new encryption budgets. According to a Trust Catalyst Report[10], 53% of all respondents already encrypt their network links. In the financial services industry this number rises to 70%.

Employing the right encryption technology will help corporations ensure that performance is not sacrificed for security. Encrypting data at layer 2 (data link layer) can ensure high throughput and low latency (less than 10 microseconds. In contrast to layer 3 encryption (eg. IPSec), there is no encryption tax at layer 2 on the size of the data packets. Encryption can therefore be performed at wire speed (maximum data transmission rate) for even the most demanding 10Gbps links.

5. Conclusion

While companies spend millions of dollars on traditional network security applications, such as firewalls, anti-virus or intrusion prevention systems, many still fail to take adequate steps to protect the data in transit over their fibre optic networks.

Timely data protection through encryption costs significantly less than the financial impact of a data breach, not to mention the collateral damage to the company's reputation and customer confidence. Moreover, a passive data loss or breach may continue for a long period of time before it is detected, or before the company realizes that it has already taken place – this seriously aggravates the potential damage and subsequent liability.

As malicious and criminal attacks spread, companies need to exercise due caution to protect their data. Encryption is the only method to ensure real data security. This should be implemented as part of a coherent risk management and data protection strategy. Whether companies plan to connect data centers, campus networks or foreign branches they need encryption – without encryption there is no compliance, no confidentiality and ultimately no security.

[10] Trust Catalyst *2009 Encryption and Key Management Industry Benchmark Report*