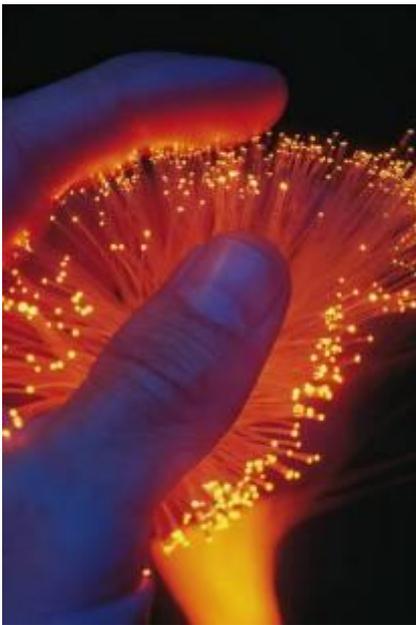**Background Paper Fibre Optic Networks**

Risks and Dangers of Fibre Optic Cables

Today, the world of business would be inconceivable without fibre optic cables. However, what is often forgotten or even denied is the fact that it is very easy to tap into fibre optic networks. The security risk, therefore, should not be underestimated.

Fibre optic cables are data communication lines that have previously displayed unrivalled advantages. There is no other means of transporting such huge volumes of information so fast and so reliably. State-of-the-art fibre optic networks are employed by many banks, insurance companies, enterprises and public authorities as the backbone, which just happens to be the place where industrial espionage is child's play. According to numerous, international studies, digital eavesdropping has multiplied tenfold in the past two years in companies around the globe. The commercial damage resulting from attacks of this nature is enormous. The F.B.I. estimates the annual potential for damage as a result of industrial espionage to be in the order of USD 20 billion – solely for attacks taking place within the United States.

1 Fibre optic cable – the transmission medium of the future

Fibre optic cables are gaining increasing popularity for transmitting data with estimates putting the length of cable installed around the globe at more than 300 million kilometres. The cables offer high data transmission rates and are thus particularly suited for the transmission of data, images and voice. In carrier networks, Gigabit Ethernet is the access technology whilst fibre optics provides the transmission medium.

In day-to-day business, the transfer of information and data has become indispensable, and there is no let up in the volumes that are being transmitted. Bandwidths of 1 Gbps or higher are the order of the day for connecting different metropolitan locations (MAN), for networks throughout Switzerland (WAN) as well as for backup and disaster recovery infrastructures (Storage Area Network, SAN). Even large volumes of data can be mirrored and safeguarded at locations far away from their origins. The terror attacks on the World Trade Centre lost no time in bringing home the importance of remote data backups. The significant advantages of fibre

optics for networks of this type – speed, capacity, economy – have led to a situation where the demand has increased dramatically.

The widespread notion that fibre optic cables are particularly secure when compared with the traditional copper wire is not quite accurate since there are various methods, so-called "Optical Tapping Methods", to extract data from fibre optic networks. The risk of being detected is very slight, if not non-existent. Anybody looking for the necessary tools can find them easily on the internet. The majority of telecommunications providers, however, fail to draw attention to this growing danger or are blatantly ignorant of the fact.

2 The vulnerability of fibre optic cables

Eavesdropping on fibre optic cables is a great deal simpler than was previously thought. Which fibre optics are being used by whom is relatively easy to determine as the individual cables in a cable loom are marked for maintenance purposes. Thus it is sufficient to identify the cable emerging from a building and tap into it from a freely accessible point. In fibre optic networks in Switzerland alone, several thousand amplifiers are installed in housings that, as a rule, can be opened with a square locking key. These amplifiers are equipped with service connectors for maintenance work and thus provide the easiest point of intrusion.

In principle "optical tapping" methods can be subdivided into three categories:

- Splice methods
- Splitter/Coupler methods
- Non-touching methods

The risk is real. Secret Services in the United States have detected espionage equipment illegally hooked into Verizon's fibre optic network close to a company – just before the quarterly results were about to be published. The investigating authorities believed that terrorists wanted to bolster their finances by profiting from the gain in the price of shares.

2.1 Optical Tapping - "Splice Methods"

In the simplest method of tapping, a break is made in the optical fibre and appropriate equipment is inserted. During the time this equipment is being hooked in communication is interrupted and this can be detected without great difficulty. However, if the downtime is short, most providers will attribute the disturbance to a network glitch and allow data transit to continue unaware that a tap has been placed.

Most off-the-shelf tapping equipment today makes it unnecessary to interrupt the signal and thus the splicing method has lost its significance in recent years.

## 2.2 Optical Tapping - "Splitter/Coupler Methods"
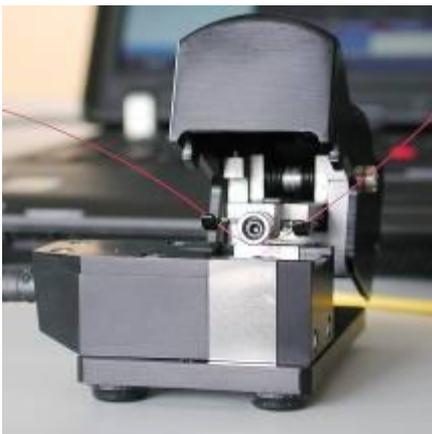
If a glass fibre is bent to a certain radius, however, the light tends to follow the bend and some will escape from the fibre – a phenomena known from physics classes. With today's modern receivers, it is sufficient to capture just a small percentage of the light (1-2% of the optical rating is sufficient), to obtain the full signal and convert it into digital form. Either the fibre can be bent using a clip-on coupling device that receives the light signal at the same time – a bend coupler[1] FCD-10B from the Canadian EXFO company, for example.

---
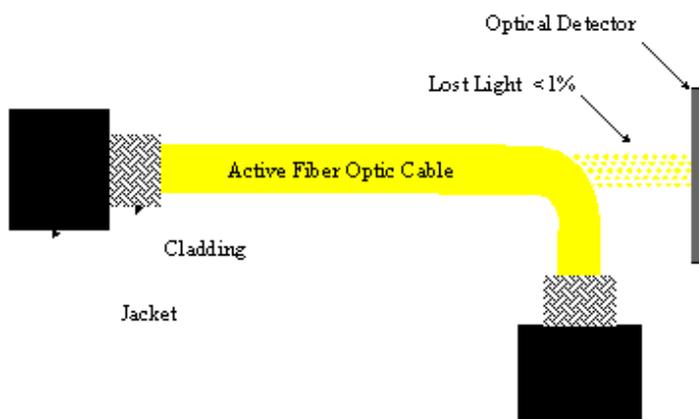
[1] Bend coupler; due to the reflections and the differing refractive index between the core glass and cladding glass of an optical fibre, centrifugal light can escape and be captured if an optical fibre is bent and the coating removed. If decoupling is to be permanent, the fibre to be bent and the fibre to be connected should be rubbed down to the core and spliced together. This also facilitates coupling and puts the notion that optical fibres are impervious to passive attacks into perspective.

Or one can insert a number of spikes at individual points to deform the optical fibre in such a way that light emerges.
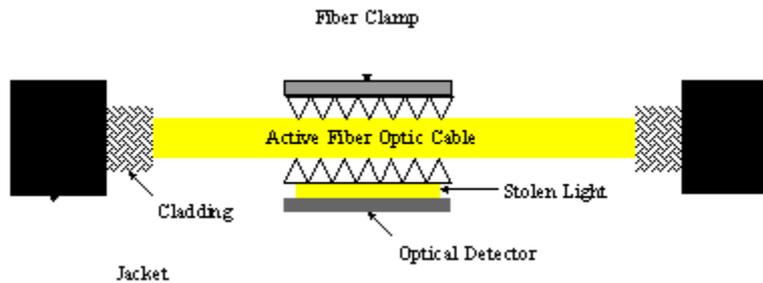
The technical device needed for coupling purposes is part of the equipment of every maintenance technician who tests the state and function of the optical fibre, and can be readily purchased. The Canadian manufacturer Canadian Instrumentation & Research, Ltd. offers the equipment on the internet for around USD 1000. Signal extraction using a bend coupler is technically simple and easy to implement but, because of the unavoidable attenuation (up to 1dB), it is not difficult to detect.
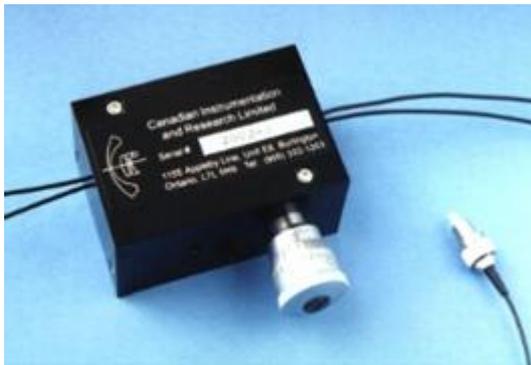

Abb. Polarization Maintaining Variable Ratio Evanescent Wave Coupler from Canadian Instrumentation & Research, Ltd. is suitable for launching tapping intrusions on single mode and WDM connections using the so-called polarization phenomena.

In principle, the "coupler" method can be considered as a passive intrusion although there are bend couplers that can also be employed for active intrusions. The main objective here is not to extract the light signal but to supply the existing flow of information with incorrect data (external signal) or interrupt it.

2.3 Optical Tapping – «Non-touching methods»

On the basis of current technology, crude manipulation of the cable network, as mentioned above, is outdated. Deutsche Telekom AG, in Bonn, has already registered a more subtle method with the European and American Patent Offices (EP 0 915 356 A1, and US 6,265,710 B1). The principle: Sensitive photodetectors capture the minimum amounts of light emerging laterally from the glass fibre. As a result of this so-called Rayleigh scattering, the light pulses have to be constantly amplified on their way through the cable network so that when they reach the geographical end point a sufficiently strong optical signal can still be received. This Rayleigh scattering can be amplified by means of focussing elements at the photodetector until a usable intensity has been achieved, or it can be directed to the input face of another glass fibre. One advantage of this method that criminals can use it to their benefit; neither the cable nor the signal is attenuated to the degree where it can be measured. Put in a nutshell: using this procedure, Deutsche Telekom has patented a tapping option that works without the glass fibre having to be touched and cannot be evidenced by measurement (undetectable eavesdropping). The "non-touching" method, too, can be characterised as a passive or active intrusion.
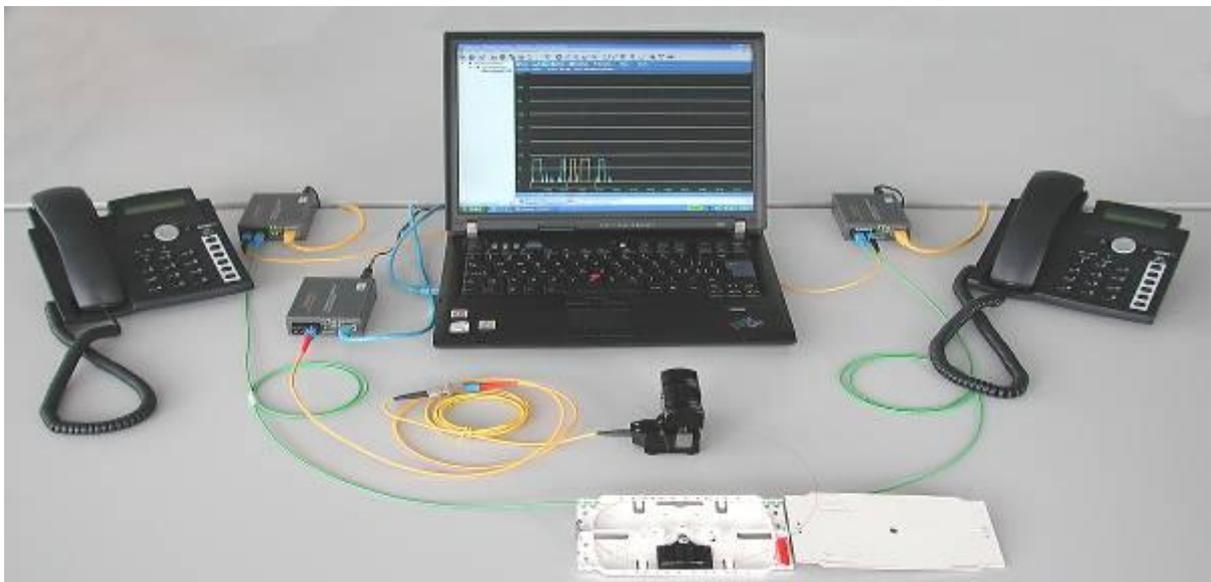
Examples of Optical Tapping Methods

Thus the report for the European Parliament on the international surveillance network "Echelon" stating that fibre optic cables could only be tapped at the end nodes of a connection is no longer valid.

Based on the findings of an internal AT&T paper in 2002, it is evident that systematic tapping of fibre optic cables, in the USA, e.g. eavesdropping on the very popular and frequently used by companies, WorldNet, is reality. In various cities in the USA, so-called "secret rooms" have been

constructed on the instructions of the government (under the cloak of fighting terrorism), in order to analyze communications traffic. In the cases mentioned, splitters were already installed in the fibre optic cables when the infrastructure was put in place. For analysis purposes the "Narus STA-6400" product from the American company of the same name was used.

The management of this company includes William P. Crowell – a former and experienced person who was Deputy Director of the National Security Agency in 1994. William Crowell is a consultant specialising in Information Technology, Security and Intelligence Systems and following his term of office with the NSA held the position of CEO at the American Security Specialists Cylink before moving to the Federal Advisory Board after Cylink was acquired by SafeNet. Since 9/11, he has also been working in the "Market Foundation Task Force on National Security" and has published a number of studies on Homeland Security.

2.4 Analysis of extracted data using packet sniffers

Contrary to widespread thinking large volumes of data on its own provides no protection. In order to extract specific information from large amounts of data corresponding IP numbers or key expressions are sufficient. Using the digits, packet sniffer programs are able to filter out the information required from the data streams and store it in real time. A packet sniffer is a program that records, monitors and analyses network data. In addition, a sniffer can also be used for legitimate as well as subversive purposes as a means of monitoring complete networks and their users. Corresponding read-out instruments and software can be readily obtained.

One example is the solution previously mentioned from Narus, with headquarters in Mountain View, CA (USA). As a matter of fact, solutions of this nature are offered to ISPs as a means of implementing new calculation models for data traffic and it should come as no surprise that these tools can also be used to analyse the contents of data traffic (from OSI Layer 3 and higher, including VoIP applications).

On the technical side, Narus works together with renowned partners and supplies virtual analyzer plug-ins for practically all off-the-shelf network components. To date, the so-called Internet Business Infrastructure (IBI) is able to analyze data traffic up to a speed of 10Gbps, or OC192. As customers, Narus lists, among others, the following telecommunications companies on its own website: AT&T, Brazil Telecom, Korea Telecom, KDDI, Telecom Egypt, Saudi Telecom, France Telecom, T-Mobile and U.S. Cellular.

3 Protective measures

It is hardly possible to monitor the entire fibre optic infrastructure but, at the same time, it is very difficult to estimate the seriousness of the gaps in security. Whilst network equipment vendors and network providers in Switzerland solely subscribe to a hypothetical risk, the largest North American National Association of Manufacturers (NAM) views the "theft of optical data" as a very real danger. At NAM, it is even conjectured that tapping into fibre optic cables is a widespread method of industrial espionage. According to information provided by the German Federal Office for Security in Information Technology (BSI), fibre optic transmission paths really do pose a threat in terms of security. Data encryption is thus an absolute must. However, only the armaments' industry is equipped with legal regulations. Nothing has been done to address the security issues that affect enterprises and government authorities with their data communication paths in remote data processing centres.

3.1 Encryption – the secure solution for fibre optic network

When data is being transmitted over fibre optic networks sensitive information is almost always involved, whether from financial institutes, insurance companies, pharmaceutical and chemical industries or public administrations. If the integrity, confidentiality and authenticity of this information is not 100% guaranteed, the user of this technology may be exposed to a risk of immeasurable proportions. The only sensible and really secure course of action to guard against intrusions of this nature is to encrypt information using high performance encryption solutions prior to connecting to the public networks.

3.2 Gigabit Ethernet Encryption

InfoGuard AG offers a new security solution in the name of "EtherGuard1" and "EtherGuard10". It is based on the successful and tried and tested concept that has been employed by renowned banks and leading enterprises and has established itself as "Best Practice".

The system encrypts at OSI-Layer 2, provides 100% data throughput up to a transmission speed of 1 & 10Gbps and runs on the network with full transparency regardless of the protocol being used. The maximum performance (100% encryption throughput) as well as the extremely small latency time (<5us) makes it possible to deploy the devices even in time-critical applications and heavily

loaded links. The encryption devices provide 100% security against eavesdropping for point-to-point transmission paths, whether in the form of dark fibres or in multiplexed topologies using CWDM/DWDM.

Security is based on a unique security architecture and fulfils the highest requirements as demanded by sensitive-critical environments. Our security solutions have been developed in accordance with the Common Criteria standards. Data is encrypted using the strong, public Advanced Encryption Standard (AES) supporting key sizes of 256 or 128 bits.

The EtherGuard products are explicitly configured for sustained operations and require very little in the way of maintenance. For transmitting the data over fibre optic networks, off-the-shelf module transceivers of the type SFP or XFP are used. These can be configured for varying distances and wavelengths.

As a Swiss company we stand for the highest quality of our products and complete independence in the implementation of our security functions. To underline this, all security-relevant modules have been developed and produced by our qualified security specialists in Switzerland.

Source:

FCW.com, "Lights out", 12. June 2006, Brian Robinson

Securitysolutions.com, „Hacking at the Speed of Light", 1. April 2006, Sandra Kay Miller

Virgo Publishing, "Big Brother Is Watching", 3. January 2006, Charlotte Wolter

"AT&T Deploys Government Spy Gear on WorldNet Network", 16. January 2004

Computerworld, „Intelligence ops in Baghdad show need for security back home", 8. April 2003, Dan Verton

Wolf Report, „Das Schweigekartell I & II", March 2003, Wolfgang Müller-Scholz

White Paper on Optical Taps, 9. February 2003, Oyster Optics, Inc.

Frankfurter Rundschau, „Glasfaser mit Durchblick", 4. September 2002, Herr Gábor Papp

Frankfurter Allgemeine Zeitung, „Hört, hört - Wie einfach Glasfasern angezapft werden können", 13. March 2003, Herr Heinz Stüwe

Die Welt, „Glasfaserkabel sind nicht abhörsicher", 3. February 2002, Herr Gábor Papp

White Paper on Optical Taps, 1. August 2002, Oyster Optics, Inc.

United States Patent, US 6,265,710 B1, 24. July 2001, Deutsche Telekom AG

Europäisches Parlament, Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation, 11. July 2001

Europäische Patentanmeldung, EP 0 915 356 A1, 18. September 1998, Deutsche Telekom AG