

# The darker side of the light

**Fibre-optic cable has been regarded as a 'secure' medium for a long time but, as Bill Ingram explains, this apparent security can be breached relatively easily unless preventative steps are taken**

Since the 1970's, it has been the perceived view among operators and users of fibre optic communication networks that optical fibre is secure from undetectable intrusions. Global information security guidelines and best practices recommend the installation of optical fibre for the electronic transfer of confidential material. In reality, it has been possible for outsiders to intrude into a network non-invasively without being detected by any of the methods that are currently deployed. Using compact and relatively simple devices that are now readily obtainable, an intrusion can be set up with a minimum of skill in a short period of time and managed remotely.

Some readers will be surprised to learn that such exploits, whilst probably uncommon, are not new. In May 2001, Neil King Jr., a staff reporter of The Wall Street Journal, wrote an extensive report on the military ramifications of fibre optic uses:

“Much of the information the agency (United States National Security Agency) once gleaned from the air waves now travels in the form of light beams through fiber-optic cables crisscrossing continents and ocean

floors. That shift has forced the NSA to seek new ways to gather intelligence – including tapping undersea cables, a technologically daunting, physically dangerous and potentially illegal task. In the mid-1990s, the NSA installed one such tap, say former intelligence officials familiar with the covert project. Using a special spy submarine, they say, agency personnel descended hundreds of feet into one of the oceans and sliced into a fiber-optic cable.”

Others, however, have claimed this successful intrusion began in the early 1980s.

In the 21st century, an intruder into a fibre optic network does not need a purpose built submarine and a room full of specialist devices. A mock telecom van or a maintenance worker's overalls will suffice to gain brief, unnoticed access to fibre optic cables at easy-to-access breakout points in manholes, communications rooms, server farms, and so forth.

Although commercial clip-on couplers were originally created as network test and maintenance gear to provide a quick and easy means to ascertain what fibres in a bundle were lit and which were dark, there are now

models available that are very precisely fabricated and easy to use. They are as compact as a medium sized office stapler and yet can cover the range of operating wavelengths in current use. A typical retail price is US\$1,600.

Using such a clip-on coupler, the intruder is able to gain access to the signal light path without the need to break or splice the optical fibre. The best of these couplers create a precisely calculated and controlled micro-bend in the target fibre optic cable. This causes a small amount of the total light to leak into a photo detector. The light is directed to an inexpensive media converter that enables connection to an Ethernet interface card on board a notebook computer. From there, the intruder has his choice of conventional communications routes to relay all the data he has captured from the optical path to his chosen destination. Since fibre optic network designs incorporate wide optical budgets and since the couplers only draw off a small fraction of the designed-in overhead, network performance monitoring will not detect an intrusion using this technique.

which are focused on the applications they are designed to protect. They do not prevent the physical aspect of the intrusion but merely attempt to contain the damage after an intrusion event has occurred.

The NeStronix Group, headquartered in Chantilly, Virginia, has developed a unique solution which can detect physical intrusion into a fibre optical network and execute a physical response to it within a very few milliseconds. The nature of the response will be defined in advance by the network administrative executives. They have developed and introduced the Opterna FiberSentinel System with WaveSense intrusion prevention technology.

WaveSense employs a rules-based, artificial intelligence inference engine, which combines with optical digital signature recognition analysis techniques to enable it to identify, differentiate and characterise eight distinct optical event types that may represent a threat to the integrity and functionality of a fibre optic communications network.

Since the FiberSentinel System works only on the phys-

## With the powerful computers in common use today, cracking encryption keys can be accomplished in a matter of hours

Although it is not the subject of this article, the reader should know that encryption is not sufficient to foil a sophisticated intrusion operation for the purpose of extracting data from an optical path. With the powerful computers in common use today, cracking encryption keys can be accomplished in a matter of hours.

There are several reasons why an intruder would want access to the target optical path. The purpose might be to gain access to secret information belonging to corporations, financial service institutions, telecommunications operators, or governmental agencies – especially military and diplomatic ones. On the other hand, the purpose might be a denial of service exploit. In that case, the intruder has two options: to create havoc on the network by injecting a mass of foreign data into the fibre optic cable or to inject a very powerful laser-generated optical pulse to bring the network down by catastrophically overloading expensive optical receivers.

Current network and processor protection is directed at the perceived historic threats from viruses, hackers and denial of service attacks. Firewalls, Anti-virus and Intrusion Detection Systems are all software devices,

ical level, it is not invasive of the network. FiberSentinel monitors only in the analogue domain and does not decode any data on the network. Hence it has no effect on the integrity of the network. This unique combination of optical analysis and the artificial intelligence inference engine has enabled Opterna's FiberSentinel System to define a new category of intrusion protection. It prevents intrusion rather than merely detecting it.

The eight distinct types of physical optical events which FiberSentinel will identify are: intrusions, injection of an optical signal, cable breaks, transients, receiver overloads, loss of data signal, low light levels at receiver and powering down of a FiberSentinel unit.

NeStronix has appointed Ingram's First Limited as agents to demonstrate and sell FiberSentinel Systems. Installations and maintenance will be delivered through Auriga (europe) PLC. ■

**Further details: the Fibre Optic button at the [www.ingramfirst.com](http://www.ingramfirst.com) web site. E-mail: [Bill.Ingram@ingramfirst.com](mailto:Bill.Ingram@ingramfirst.com) or tel: +44 1494 758258**