HIGHPOINT SECURITY
TECHNOLOGIES Inc.

ADDRESSING SECURITY THREATS

ASSOCIATED WITH OPTICAL FIBER

HIGHPOINT DOCUMENT

2006

ADDRESSING SECURITY THREATS ASSOCIATED WITH OPTICAL FIBER

Executive summary

This report addresses the security threats to government and private institutions presented by the relatively new technology of optical fiber communications. It begins with a summary of fiber technology, highlighting its enormous capacity, long reach, good security, compact structure and commercial deployment status in the last mile access network. It identifies two prime scenarios, one where a fiber is covertly deployed for carrying surveillance information and the other where the surveillance information is covertly injected into a legitimately deployed fiber.

Means of finding a covertly deployed fiber are reviewed and the use of either X-ray or the new Tera Hertz probing technologies are recommended. The practical difficulties of carrying out a covert attack are asserted; simply breaking the illicit fiber is suggested as likely the best course of defensive action.

The use of a fiber splitter coupled at a connector location is recommended for tapping into a legitimately deployed fiber. Issues of power level, amplification and detection are briefly discussed. The optical spectrum analyzer and the high-speed analogue receiver with a sampling oscilloscope are tools required to discover and identify covert signals in the fiber and the optical time division reflectometer (OTDR) is required to discover and locate covert access points.

Finally a list of recommended countermeasures is presented. The report is a high level overview of the situation and further work is needed to develop a detailed plan of action for addressing specific scenarios.

INTRODUCTION

The protection of the knowledge assets of government and private institutions against the deliberate attempts by others to penetrate their security is a shifting technical battlefront pitting advances in the technology of covert surveillance and intrusion against advances in the technology of sweeping and detection.

The introduction of optical fiber for telecommunications networks during the past two decades clearly illustrates this contest. This technology has supplanted wire line, cable and satellite communications in many situations and is making incursions into the final mile or access network that connects customers at the edge of the network. As a consequence, new techniques for technical information collection have been enabled. These all involve the use of optical fiber to transport the illicit information from the premises of the target customer. Some also involve the use of fiber to carry power to the surveillance device and so remove any dependency on batteries or on electrical power stolen from the target.

This report addresses the challenge of defending premises against the new opportunities presented by optical fiber for covertly transporting such information from the target premises to the outside world.

FIBER OVERVIEW

The use of optical fiber for telecommunications was first proposed in 1966. The first low-loss fiber was demonstrated in 1970 and various experimental systems were developed during the seventies. Serious deployment in the network began during the eighties and ramped up enormously in harness with the development of the Internet in the nineties.

Today, it is the standard technology in all parts of the network except for the last mile where it is largely restricted to major institutions and apartment blocks. However, even this last bastion of the copper pair is now slowly succumbing to fiber as the demand for broadband audio and video Internet services increases.

As a consequence, whereas the covert use of fiber once always required that the attacking party had to covertly deploy and hide the fiber, now it is increasingly possible that the fiber is already in position, and the challenge for the attacker is to covertly feed the illicitly obtained information into the fiber on the target premises and remove it at some external location.

There are therefore two distinct tasks that need mastering by the sweeper. In the first case, it is to locate and possibly destroy the fiber and trace it to the end points. In the second case, the location of the fiber is known and the task is to determine and prevent any illicit use of the fiber without unduly disturbing the legitimate services being carried.

Several different types of fiber have been developed for various applications. Most fiber is made of high-silica glass although polymer (plastic) fiber is also available. Glass fiber is highly transparent (has low loss) over a broad spectral region extending from the visible region with wavelengths between 400 and 700 nm up to near-infrared wavelengths of 1800 nm. fiber used for telecommunications supports only one spatial mode; this is called single mode or mono mode fiber. fiber used for local area networks within premises usually supports many spatial modes and is called multi mode fiber.

Both types of fiber have been standardized resulting in an outer glass diameter of 125 um, about a 200^{th} of an inch. This diameter is increased by a polymer protective coating, typically doubling to 250 um and sometimes to 1 mm. Such a fiber would evidently be quite difficult to locate if deployed as such. However, for physical protection, fibers are normally further enclosed in an armored shell of Kevlar, polypropylene and/or metal, and the cable diameter is typically in the region of 3 mm to 10 mm. Typically, the larger cables will carry more than one fiber; an access fiber cable may contain six fibers, one for upstream, one for downstream and the remainder as spares for replacement and upgrade purposes. (This may seem wasteful, but the cost of the extra fibers is minor relative to the cost of the protective armour.)

Most telecommunications systems operate at a wavelength in the region of 1550 nm as this is the spectral region of lowest loss. However, access links may operate at the shorter wavelength band between 1300 and 1350 nm. In either case, vast amounts of available spectrum are unused.

Evidently, where the fiber cable is already deployed, the attacker may have the options of using one (or more) of the spare dark fibers and not have the challenge of having to share a live, lighted fiber. However, if sharing is required, there is plenty of spare spectrum to enable surveillance information to be added through the use of wavelength division multiplexing (WDM).

The low loss and high information transmission capacity of fiber result in the capability to send any conceivable amount of surveillance data over a distance of many kilometers. There is no requirement for the attacker to set up a data collection point close to the target point.

Standard commercial fiber systems use binary on-off keying (OOK) modulation. The ITU Sonet family from the telephony world uses data rates from 150 Mb/s to 40 Gb/s, with intermediate systems at multiples of four (600 Mb/s, 2.5 Gb/s, 10 Gb/s). The IEEE Ethernet family of the Internet Protocol (IP) world uses data rates of 10 Mb/s, 100 Mb/s, 1 GB/s and 10 Gb/s.

In the 1550 nm region, there are 150 standard ITU wavebands spaced 100 GHz apart between 180 THz (1667 nm) and 195 Hz (1538 nm). There is also a coarser ITU grid with 18 wavebands spaced 20 nm apart between 1270 nm and 1610 nm.

However, covert collection systems using fiber need not follow the standards. For example, the optical power could be analogue modulated with a baseband video signal directly from a camera. Alternatively, it could be phase modulated and show no apparent modulation of power. Moreover, the covert systems may use non-standard wavelengths such as those above 1610 nm or below 1270 nm.

FINDING A fiber

Finding a fiber that has been covertly deployed can be a considerable challenge. Not only is a fiber very small but it is also non-metallic. Fortunately, the necessity to protect the fiber forces the adoption of armour that considerably enlarges the cable cross-section making visible detection more feasible.

However, as this can also exclude metallic content, if the cable is buried, it is almost impossible to locate without intrusive physical exploration. If the armour includes metal, the cable can relatively easy be located using a metal detector; however, it would seem unlikely that an expensive attack operation would make such an elementary error as using cable with metallic armour.

While radar type techniques for remote sensing work best with metallic targets, unique reflections also occur from non-metallic targets wherever there is a change of dielectric constant or material scattering properties. Therefore, the use of tomographic and other techniques for recreating 3D imagery of buried structures must be considered as a means of non-intrusive probing.

Material such as brick, plaster and wood can be penetrated to some extent by X rays and by radio waves. X ray technology has excellent spatial resolution and the feasibility of

equipment that is conveniently compact and portable and operating at power levels that do not unduly hazard the operating personnel is growing,

Another technology that is currently on the cusp is that of sensing at Tera Hertz frequencies. This spectral band occupies the region between the far infrared and the microwave region, typically having frequencies between 100 GHz and 10 THz. Until recently, the technology has not existed to generate and detect power in this region. In principle, a probe frequency could be selected that excites something like a resonant reflection from a structure the size of a fiber. This would likely occur near 0.8 THz.

Sometimes, after a fiber has been found, it is desirable to find out where it leads in both directions. A useful tool in this activity is the optical time-domain reflectometer (OTDR) that can accurately determine the distance of transition points in the fiber such as connectors, splices, splitters and terminations.

If an OTDR trace shows an apparent splitter loss point where none is supposed to be, this would be a good indication of a location to search for an illicit splitter that may have been deployed by an attacking party to access the fiber to send back collection information.

TAPPING A fiber
Covert attack

It is often incorrectly thought that an optical fiber is incapable of being tapped. This is not the case. However, tapping a fiber is generally a much more complex and expensive operation than tapping a wire pair. The main reason for this is that the optical power within a fiber is well confined to the inner core region and does not normally escape to the fiber perimeter. Therefore, access to the power normally requires access to the fiber core: there is no equivalent to bringing a probe antenna near a wire.

The power confinement can be overcome. A condition for low loss transmission in a fiber is that the fiber be not bent into a small radius of curvature. If it is bent sufficiently, power escapes from the core and reaches the perimeter where it could be collected and sensed. The critical curvature is wavelength dependent; the guidance at longer wavelengths is much weaker than that at the shorter wavelengths. A relatively simple tap would therefore have the fiber make a sudden change in direction caused by a suitable clamping structure.

The design of the clamping structure is doubly important because the presence of a severe bend will result in severe stresses that could over the course of time result in a fracture if there was any initial surface imperfection. A suitable clamping design could probably contain the possibility of a fracture.

While the implementation of such a tap sounds quite straightforward, this presupposes that the fiber is readily accessible to carry out such an operation. Unfortunately, this is likely not the situation. Typically, the fiber will be encased within an armoured casing and it will be necessary to strip away a portion of this casing without damaging the fiber

at the center. This will likely need special equipment tailored to attack the particular cable structure.

Overt attack

The foregoing presupposes that a covert attack on the fiber is needed. However, this requirement is most likely the exception. As noted in the Overview section, if the fiber was covertly deployed, the requirement is generally to break it rather than tap it, whereas if the fiber was legitimately deployed, there are easier options for tapping it than carrying out a covert attack.

Specifically, in a standard fiber installation, access to the fiber can be gained at locations where it is connectorized. Such locations occur both on the premises of the client and of the fiber service provider, i.e., the telephone company. There may also be a connector location in the feeder plant. At a connector location, a connectorized fiber splitter can be easily inserted in a few seconds. Such a splitter could reliably tap off a fixed proportion of light traveling down the fiber. Two such splitters may be needed, one for each direction, unless there are good grounds for supposing that illicit information is only traveling in one direction – the expected situation.

A splitter could also be inserted at a splice location. This is a much longer operation that would take down the link for perhaps 30 minutes rather than a few seconds. It involves the breaking of the fiber at the splice point and the subsequent use of two splices to connect the splitter. Splice locations occur in the outside plant. Care is needed to stow the loose fiber and splitter away from harms reach.

Tap level

The question may be raised concerning how much power can be extracted from a fiber before the operation of the link is compromised. The answer depends on the link design. Standard commercial links are designed with considerable power margins to allow for component degradation, repair splice losses and thermal effects. Moreover, in an access (last mile) situation, they are rarely operating near their range limits. Consequently, considerable power can then be siphoned off without impairing the link performance.

However, it is possible that a system includes power level monitoring that may raise an alarm if the received power drops suddenly. This would need assessing on an individual basis.

Where the power tapped is at a low level, it is feasible to optically amplify it to a level where satisfactory detection is possible. Commercial Erbium Doped fiber Amplifiers (EDFAs) do this for the spectral band around 1550 nm and amplifier systems for other parts of the spectrum have been demonstrated experimentally.

COVERT SIGNAL DETECTION

This section considers the situation where the tap has been successfully deployed and a proportion of the light in the fiber is therefore accessible for analysis. Where the link was deployed by the local telephone company, the wavelength(s) of its transmitters will be known. The first objective will be to search for the presence of any power at unauthorized wavelengths. To do this, an optical spectrum analyzer will be needed. To include the possibility that a covert channel may be only 100 GHz away from a legitimate channel, the optical spectrum analyzer must have this degree of resolution, at least in the 1550 nm EDFA bands.

If a covert channel is discovered, the next stage is to establish the form of modulation being used. As a first stage, the signal should be detected with a broadband, erg, 10 GHz receiver and the electrical spectrum reviewed on an electrical spectrum analyzer. If a standard Ethernet or Sonet signal is being sent, this will be relatively easily identified. If a non-standard modulation format is being used, it will likely take considerable time to identify. A broadband sampling oscilloscope will likely be an important tool in this task.

COUNTERMEASURES

For those clients that are not connected to the network with a fiber, the only defense against a covert fiber deployment is vigilance and a periodic sweep operation.

However, for those that are already equipped with a fiber connection, there are options for maximizing security. These include:

- Deploying exclusively fiber systems with built in integrity surveillance facilities.
- Periodic OTDR checks of all fiber paths to identify any changes
- Insertion of narrow band optical filters at points along the fiber path to prevent any freeloading at unauthorized wavelengths
- Applying security and regular inspection around any fiber connection points.

CONCLUSIONS

This brief review of the security threats associated with optical fiber and the means of addressing them has identified two classes of situation, one where the fiber has been deployed covertly and needs to be found and removed, and the other where the existence and location of the fiber is known but the issue is to determine whether there is any unauthorized optical signal that has been added capable of carrying out knowledge assets.

The former presents the bigger challenge, both for the offensive and defensive parties. The use of THz imaging surveillance tools will likely become standard as that new technology advances.

For the latter, various measures are available in principle and practice to help find the unauthorized channel and determine its contents. The required test hardware is generally capital intensive. There are several countermeasures that can be used to minimize the threat.

Further work is required to build up a detailed plan of action within these various scenarios.

Biographical notes.

David Kahn has spent many years developing optical fiber technology in the UK and Canada. He designed the terminals for the first demonstration of video transmission over 1 km of fiber in 1972, was instrumental in introducing WDM to the public network in 1981, and demonstrated the first North American passive optical network (PON) targeted at fiber-to-the-home (FTTH) in 1987. He has initiated over thirty patents and was a post-graduate lecturer in fiber systems at Carleton U. (1981-1990) and Ottawa U. (2000-2003). He has also been closely involved in the development of collection technology for security services in the UK, the USA and Canada.